Trifork Security A/S

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 March 2024 to 31 December 2024 in relation to Trifork Security A/S's security and observability services to customers

February 2025

Contents

1. Management's assertion

The accompanying description has been prepared by Trifork Security A/S (Trifork Security) for customers who have used the security and observability services and their auditors who have a sufficient understanding to consider the description, along with other information, including information about controls operated by the customers themselves, when assessing the risks of material misstatements in their financial statements.

Netic A/S is a service organisation that provides HR services to Trifork Security. This report uses the inclusive method, and Trifork Security's description includes a description of Netic A/S's HR services used by Trifork Security to perform HR tasks, as well as relevant control objectives and controls of Netic A/S.

Trifork Security uses Netic A/S for its hosting and backup services. This report uses the carve-out method, and the description in section 3 includes only the controls and related control objectives of Trifork Security and excludes the control objectives and related controls of Netic A/S. Our evaluation did not extend to controls of Netic A/S.

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

Trifork Security confirms that:

a) The accompanying description in section 3 fairly presents the security and observability services that have processed customers' transactions throughout the period from 1 March 2024 to 31 December 2024. The criteria used in making this statement were that the accompanying description:

   (i) Presents how IT general controls in relation to the security and observability services were designed and implemented, including:

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

   (ii) Includes relevant details of changes to IT general controls in relation to the security and observability services during the period from 1 March 2024 to 31 December 2024

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

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 March 2024 to 31 December 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;

(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; and

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 March 2024 to 31 December 2024.

Aalborg, 24 February 2025
Trifork Security A/S

Mads Vigh
CEO

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

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 March 2024 to 31 December 2024 in relation to Trifork Security's security and observability services to customers

To: Trifork Security, its customers and their auditors

Scope

We have been engaged to report on Trifork Security's description in section 3 of IT general controls in relation to the security and observability services which have processed customers' transactions throughout the period from 1 March 2024 to 31 December 2024 (the description) and on the suitability of the design and operating effectiveness of controls related to the control objectives stated in the description.

Netic A/S is a service organisation that provides HR services to Trifork Security. This report uses the inclusive method, and Trifork Security's description includes a description of Netic A/S's HR services used by Trifork Security to perform HR tasks, as well as relevant control objectives and controls of Netic A/S.

Trifork Security uses Netic A/S for its hosting and backup services. This report uses the carve-out method, and the description in section 3 includes only the controls and related control objectives of Trifork Security and excludes the control objectives and related controls of Netic A/S. Our evaluation did not extend to controls of Netic A/S.

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

Trifork Security's responsibilities

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

Service auditor's independence and quality control

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

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

Service auditor's responsibilities

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

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

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

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

Inherent limitations

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

Opinion

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

a) The description fairly presents how IT general controls in relation to the security and observability services were designed and implemented throughout the period from 1 March 2024 to 31 December 2024;

b) The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls operated effectively throughout the period from 1 March 2024 to 31 December 2024 and user entities applied the complementary customer controls referred to in section 3; and

c) The controls tested, which together with the complementary customer controls referred to in section 3, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 March 2024 to 31 December 2024.

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

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

We permit the disclosure of this report in full only, including the description of tests of controls and results thereof by Trifork Security, at its discretion, to customers who have used Trifork Security's security and observability services during some or all of the period of 1 March 2024 to 31 December 2024 and their auditors, who have a sufficient understanding to consider it, along with other information about controls operated by customers themselves when assessing the risks of material misstatements of customers' financial statements, without assuming or accepting any responsibility or liability to customers or their auditors on our part.

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

Aarhus, 24 February 2025
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

Rico Lundager
Senior Manager

3. System description

3.1. Introduction

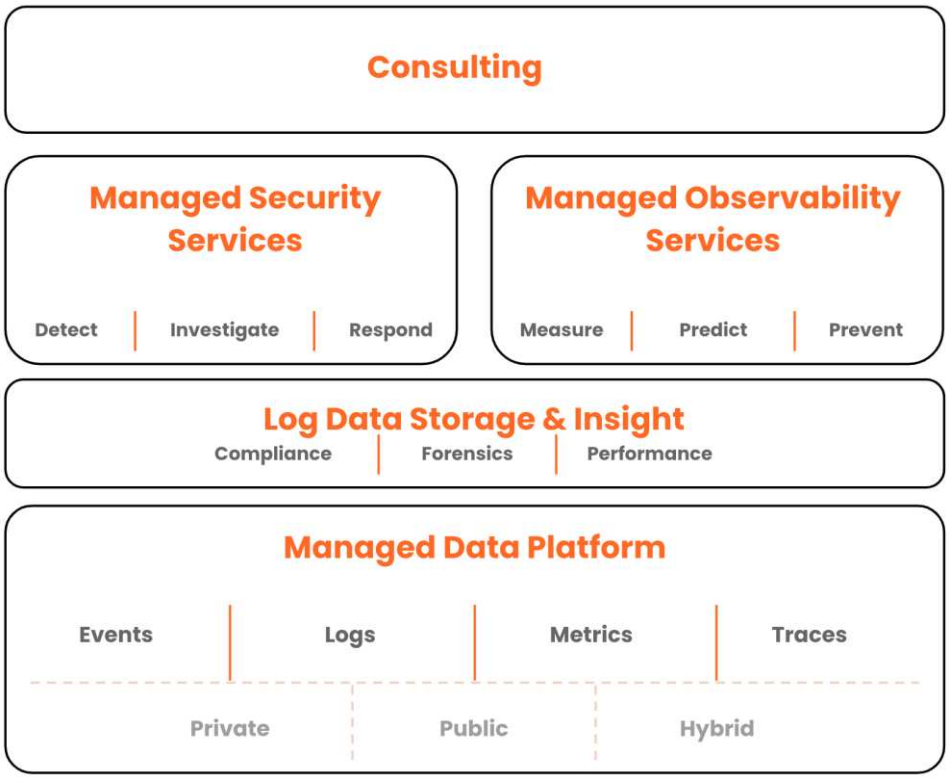
Trifork Security is a Danish company with more than 20 years of IT experience. Our goal is to solve the key challenges for public and private organisations focusing on cybersecurity, data management and observability, decreasing threats by doing our core services while increasing awareness on regulatory and compliance requirements.

In close collaboration with our originator Netic A/S, which consists of more than 150 IT operations specialists and which has extensive experience in secure and stable IT operations, we operate and secure some of the most critical infrastructure in Denmark.

Trifork Security has a diverse and dedicated team of around 50 consultants that provide managed and consulting services within operations, data observability and cybersecurity, all located in Denmark.

3.2. Description of services

Trifork Security is a supplier within managed services including managed EDR, 24/7 SOC and log management:



- Managed Security Services covering leading SIEM and EDR solutions is operated and monitored 24/7 by our Danish-based SOC and supported 24/7 by senior experts to handle major security incidents
- Managed Observability Services is mainly support and consulting covering implementation, operation and utilisation of business use cases
- Log Data Storage covers the discipline of ensuring the right data sources, data maintenance and retention times to support compliance, security use cases and observability data
- Managed Data Platform is the 24/7 operation of the actual platform optimising capacity and performance.

In addition to the managed services, we provide consultancy services, covering cybersecurity, observability, strategy, compliance, governance and assessments relating to the maturity of a customer.

This assurance report only covers these services: Managed Security Services and Managed Observability Services.

3.3. Control environment

Trifork Security is committed to maintaining a robust control environment that prioritises integrity, ethical values and a commitment to competence. This commitment is embedded in our company culture and is reinforced by a comprehensive framework of policies, procedures and practices. Our dedication to information security is demonstrated by our ISO 27001 certification, which ensures we have implemented internationally recognised best practices for managing and protecting sensitive information. Furthermore, we are dedicated to achieving and maintaining compliance with the NIS2 Directive, further solidifying our commitment to cybersecurity at all levels.

Management commitment:

- Our senior management team actively promotes a culture of ethical conduct, compliance with laws and regulations (including NIS2) and the importance of effective internal controls
- We have a code of conduct that clearly articulates our ethical principles and expectations for all employees
- Management and all employees receive regular communication and security training reinforcing the importance of these principles and providing guidance on ethical decision-making and compliance with relevant regulations
- Management is committed to attracting, developing and retaining competent individuals, and provides ongoing training and development to ensure individuals have the necessary skills and knowledge to perform their duties effectively.

Human resources practices:

- Our human resources practices are designed to support a strong control environment
- We conduct performance evaluations to assess employee performance and identify areas for improvement
- We have a whistleblower hotline that allows employees to report concerns confidentially without fear of retaliation.

Information security (ISO 27001 certified):

- We have implemented a comprehensive information security management system (ISMS) in accordance with ISO 27001 standards. This certification demonstrates our commitment to maintaining the confidentiality, integrity and availability of information.
- Our ISMS includes a wide range of controls, including:
    - Technical measures: Firewalls, intrusion detection systems, access controls, encryption and data loss prevention tools
    - Organisational measures: Data classification policies, data backup procedures, incident response plans, well-defined organisational structure with clear lines of authority and responsibility and regular security awareness training for all employees
    - Physical security measures: Access controls to our facilities and secure data centres.

- Our ISO 27001 framework serves as a strong foundation for meeting the technical and organisational security requirements of NIS2.

Monitoring and continuous improvement:

- We regularly monitor the effectiveness of our control environment through internal audits, management reviews and other monitoring activities, including regular reviews of our ISO 27001 compliance and progress towards NIS2 compliance
- We have a process for identifying and addressing non-conformities and opportunities for improvement and implementing corrective actions
- We are committed to continuous improvement and regularly review our control environment to ensure it remains effective and aligned with our business objectives and regulatory requirements.

3.4. Subservice organisations

Netic A/S supports and provides a range of services to Trifork Security.

Netic A/S provides the following services:

- HR and administration services to Trifork Security, HR advisory and handling of employee contracts, obtaining criminal records and verifying them
- Facility services like housing, physical security incl. access control, alarms and video surveillance
- Financial administration like bookkeeping, invoicing etc.
- Legal services like legal advisory in regard to current or new legislation and matters relating to customers, vendors, employees, etc.
- IT and hosting services like data centres, server housing, storage, backup and core and office network.

3.5. Risk management

Trifork Security has a systematic approach to risk management, where we have established a methodology and procedure regarding risk management. Multiple times a year, risk workshops are held, and in the assessments of the risks both senior management and employees with technical knowledge and experience are involved.

During the quarterly Information Security Board (ISB) meetings, where senior management and a representative from the Governance, Risk and Compliance (GRC) team participate, the biggest risks and their possible treatments are discussed. This ensures that senior management is kept informed, while also discussing and agreeing on treatments of the risks.

Risk management is a focus area at Trifork Security. Therefore, one of the objectives in our ISMS is Risk Identification & Assessment, supporting our continuous focus and work with risk management.

3.6. Control objectives and control activities

As an ISO/IEC 27001:2022 certified company, Trifork Security has implemented an ISMS, which includes an information security policy and controls, which are continuously improved.

In the following, we will elaborate the areas and provide an overview of the primary implemented controls.

Information security policies

Based on ISO 27001, Trifork Security has developed an information security policy, framing our approach to information security, as well as relevant topic-specific policies.

Organisation of information security

The management team responsible for the day-to-day operation of Trifork Security consists of Mads Vigh, CEO; Karsten Thygesen, CTO; Stig Andersen, CPO; and Philip Lyngø, CISO and Manager.

Trifork Security has established an ISB. The ISB has board meetings every three months concerning risks, recommendations and news from stakeholders, events and incidents, as well as other relevant topics. The IBS consists of the management team and relevant employees such as representatives from the GRC team. The IBS is responsible for Trifork Security's information security.

Employee security

All employees (full-time and part-time included) sign an employment contract, including a confidentiality section. Interns sign a non-disclosure agreement. This confidentiality is maintained during and after employment.

Trifork Security requires all employees to have a clean criminal record, and criminal records are obtained annually.

As part of the onboarding process, all employees must participate in an "introduction to information security" meeting, where topics such as information security guidelines, GDPR and incident reporting are reviewed by either the CISO or a GRC consultant. During onboarding, all employees read and accept all guidelines regarding information security, and these guidelines must be read and accepted annually.

Trifork Security does continuous awareness training, including social engineering simulations, quizzes and more.

Access management

Trifork Security's general policy on access to systems is that access is only allowed if it serves a legitimate purpose and on a need-to-know basis. This applies to physical as well as logical access. Where technically feasible, all access to systems must be logged with accurate information on time and identification of the user who accessed the system.

During onboarding, access is given to employees based on RBAC. If the need arises, access to systems can be given later in one's employment if this serves a legitimate purpose. This process is managed through our ITSM system.

All access rights are removed as part of the offboarding process.

Access rights are reviewed for systems every three months to ensure any errors or changes are corrected.

Customers only have access to their own systems.

Managing assets and systems

New assets, such as software, servers, computers, etc., are registered in the CMDB. This process is as automatic as systemically possible. At the end of an asset's lifecycle, the asset gets decommissioned.

All assets are kept in good security condition through e.g. upgrade of software, ongoing patch management and vulnerability management.

Cryptography

All data connections transmitting confidential, personal or sensitive data must be encrypted with up-to-date technology.

Data extracts containing sensitive data transmitted between Trifork Security and our customers and/or business partners must be encrypted, e.g. by use of PGP, only allowing the intended party to open them.

Data extracts include all types of sensitive data on all types of media – for example CDs, USB sticks, emails and digital uploads.

Physical and environmental security

Customer data is stored and protected in our suppliers'/partners' data centres, depending on the services delivered.

Operations security

Operations security is an important part of Trifork Security's daily operations and we make an effort to document our operations procedure.

Trifork Security has set up log monitoring. Alarms are raised by e.g. specific log patterns and errors. Audit events are logged and used centrally in our log management platform.

All our endpoints are protected against malware, and continuous vulnerability scanning is being carried out. Patching takes place continuously and follows a determined patch management plan.

Backup of Trifork Security systems is done by our hosting partner.

All systems and services are monitored 24/7 by our SOC.

Authentication and authorisation are centrally handled, and different roles are given minimum privileges to systems and services internally at Trifork Security.

Trifork Security makes network segmentation via firewalls and microsegmentation.

Trifork Security regularly performs vulnerability scans.

All production systems are redundant, where possible.

All mobile devices and laptops are managed by MDM.

Change management

Trifork Security has a process for change management, covering standard, normal and emergency changes based on ITIL. The process includes adequately documenting e.g. the change risk, rollback plan and test plan. An approval phase and CAB phase as well as a verification phase are also part of the process. The changes are documented in our ITSM system, and this is done to ensure that any possible consequences can be linked back to the change.

Supplier relationships

Trifork Security has established a supplier and partner management process for both selection and evaluation of suppliers/partners. The selection process consists e.g. of classifying the supplier/partner and based on classification, there are information security requirements the supplier/partner must comply with.

Annually we evaluate the supplier/partner to ensure that they still comply with the requirements indicated in the partner management process.

Incident management

Trifork Security has implemented an information security incident management process. The processes consist of reporting, assessing, handling and learning from information security incidents. Reporting of information security incidents is communicated to the employees and is an easy procedure where employees send a specific template to an ISB mailbox.

Furthermore, Trifork Security has implemented an operational incident process that can be escalated to a major incident process, e.g. containing communication plans.

Information security aspects of business continuity management

An emergency response plan is implemented with clear roles and responsibilities, RPO and RTO, as well as action cards. The plan has been developed to ensure business continuity and to maintain a high level of information security.

The emergency response plan is tested annually and is continuously improved.

Also refer to section 4 for a description of the specific control activities.

3.7. Changes to Trifork Security's system during the period

During the period from 1 March 2024 to 31 December 2024, Trifork Security has obtained an ISO 27001:2022 certification. The certificate demonstrates our great information security focus and dedication to strengthen our internal processes, ensuring a reliable and secure service to our customers. The certificate is valid during the period 18 October 2024 to 17 October 2027 with annual external audits.

No material changes to services or control activities were made during the period.

3.8. Complementary controls at the customers

As part of the delivery of services, the customers must implement certain controls that are important to achieve the control objectives specified in the description. This includes:

- Setting up and administering own users of the solution in the production environment (identity and access management)
- Setting up and administering users from Trifork Security who have access to the customer's environment (identity and access management)
- Ensuring that sensitive personal information is not included in support cases sent to Trifork Security via tickets etc.
- Complying with password policies based on the best practices set up by Trifork Security in software-as-a-service solutions.

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

4.1. Purpose and scope

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

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

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

4.2. Test actions

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

Inspection	Reading of documents and reports containing specifications regarding the execution of the control. This includes reading and consideration of reports and other documentation in order to assess whether specific controls are designed so they may be expected to become effective if implemented. Furthermore, it is assessed whether controls are being monitored and checked sufficiently and at appropriate intervals. We have tested the specific system set-up on the technical platforms, databases and network components in order to verify whether controls are implemented and have functioned during the period from 1 March 2024 to 31 December 2024. Among other things, this includes assessment of patching level, permitted services, segmentation, password complexity, etc. as well as inspection of equipment and locations.
Inquiries	Inquiry of appropriate personnel. Inquiries included how the controls are performed.
Observation	We observed the execution of the control.
Reperformance of the control	Repetition of the relevant control. We repeated the execution of the control to verify whether the control functions as assumed.

Trifork Security uses Netic A/S as a subservice supplier of HR services. This report uses the inclusive method and comprises controls that Netic A/S performs for Trifork Security.

Incorporation of subservice organisation

For the part of HR services that are outsourced to Netic A/S, we have tested the following related controls at Netic A/S: 6.1, 6.2 and 6.6.

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

Control objective 5: Organisational controls

- Procedures and controls ensure management supports information security in line with business needs and legal requirements, including a framework for implementing and operating security measures.
- Procedures and controls ensure that access to information and systems are managed and monitored based on business needs and user roles, ensuring only authorised access and promptly addressing unauthorised attempts.
- Procedures and controls ensure that the organisation is prepared to effectively manage information security incidents, assess security events and maintain information security during disruptions.
- Procedures and controls ensure that an agreed level of information security in supplier relationships is maintained and correct and secure operation of information processing facilities.

No.	Trifork Security's control activity	Tests performed by PwC	Result of PwC's tests
5.1	**Policies for information security** Information security policies and topic-specific policies must be defined, approved by management, published, communicated to and acknowledged by relevant employees and stakeholders, and reviewed at planned intervals or when significant changes occur.	We made inquiries of Management about the procedures/control activities performed. We inspected that a Management-approved and updated security policy is in place. We inspected that the information security policies are communicated to employees and relevant parties.	No exceptions noted.
5.2	**Information security roles and responsibilities** Roles and responsibilities for information security must be defined and allocated according to the organisation's needs.	We made inquiries of Management about the procedures/control activities performed. We have inspected that the organisational responsibilities are defined and allocated to relevant persons.	No exceptions noted.
5.3	**Segregation of duties** Conflicting duties and conflicting responsibilities must be separated.	We made inquiries of Management about the procedures/control activities performed. We have inspected by sampling that appropriate separation between critical operational functions has been established and that separation between primary data and backup has been established.	No exceptions noted.

Control objective 5: Organisational controls

- Procedures and controls ensure management supports information security in line with business needs and legal requirements, including a framework for implementing and operating security measures.
- Procedures and controls ensure that access to information and systems are managed and monitored based on business needs and user roles, ensuring only authorised access and promptly addressing unauthorised attempts.
- Procedures and controls ensure that the organisation is prepared to effectively manage information security incidents, assess security events and maintain information security during disruptions.
- Procedures and controls ensure that an agreed level of information security in supplier relationships is maintained and correct and secure operation of information processing facilities.

No.	Trifork Security's control activity	Tests performed by PwC	Result of PwC's tests
5.4	**Management responsibilities** Management must require all employees to comply with information security in accordance with the organisation's established information security policy, topic-specific policies and procedures.	We made inquiries of Management about the procedures/control activities performed. We have inspected that Management is aware of information security initiatives.	No exceptions noted.
5.9	**Inventory of information and other associated assets** An inventory of information and other associated assets, including owners, should be developed and maintained.	We made inquiries of Management about the procedures/control activities performed.	No exceptions noted.
5.10	**Acceptable use of information and other associated assets** Rules for acceptable use and procedures for handling information and supporting assets should be identified, documented and implemented.	We made inquiries of Management about the procedures/control activities performed. We have inspected that acceptable use of assets has been defined and communicated.	No exceptions noted.
5.11	**Return of assets** Employees and other stakeholders must return all organisational assets in their possession when their employment, contract or agreement ends or changes.	We made inquiries of Management about the procedures/control activities performed. We have observed that a procedure is in place to ensure that assets are returned upon termination. We have inspected by sampling that there is documentation for the return of all assets upon termination for terminated employees.	No exceptions noted.

Control objective 5: Organisational controls

- Procedures and controls ensure management supports information security in line with business needs and legal requirements, including a framework for implementing and operating security measures.
- Procedures and controls ensure that access to information and systems are managed and monitored based on business needs and user roles, ensuring only authorised access and promptly addressing unauthorised attempts.
- Procedures and controls ensure that the organisation is prepared to effectively manage information security incidents, assess security events and maintain information security during disruptions.
- Procedures and controls ensure that an agreed level of information security in supplier relationships is maintained and correct and secure operation of information processing facilities.

No.	Trifork Security's control activity	Tests performed by PwC	Result of PwC's tests
5.12	**Classification of information** Information must be classified according to the organisation's information security needs based on confidentiality, integrity, availability and relevant stakeholder requirements.	We made inquiries of Management about the procedures/control activities performed. We have inspected that a data classification scheme for classifying information has been established.	No exceptions noted.
5.15	**Access control** Rules for managing physical and logical access to information and supporting assets are established and implemented based on business and information security requirements.	We made inquiries of Management about the procedures/control activities performed. We have inspected that access control guidelines have been implemented, reviewed and approved.	No exceptions noted.
5.17	**Authentication information** The allocation and management of authentication information should be governed by a management process, including advising staff on the appropriate handling of authentication information.	We made inquiries of Management about the procedures/control activities performed. We have inspected that the procedure ensures that authentication information is handled securely.	No exceptions noted.

Control objective 5: Organisational controls

- Procedures and controls ensure management supports information security in line with business needs and legal requirements, including a framework for implementing and operating security measures.
- Procedures and controls ensure that access to information and systems are managed and monitored based on business needs and user roles, ensuring only authorised access and promptly addressing unauthorised attempts.
- Procedures and controls ensure that the organisation is prepared to effectively manage information security incidents, assess security events and maintain information security during disruptions.
- Procedures and controls ensure that an agreed level of information security in supplier relationships is maintained and correct and secure operation of information processing facilities.

No.	Trifork Security's control activity	Tests performed by PwC	Result of PwC's tests
5.18	**Access rights** Access rights to information and supporting assets are provided, reviewed, changed and removed in accordance with the organisation's topic-specific policy and rules for access management.	We made inquiries of Management about the procedures/control activities performed. By inspection, we observed that formalised procedures are established for access rights. By using random samples, we investigated whether: • according to guidelines, rights are granted based on a work-related need • all accesses are revoked when an employee leaves. By inspection, we observed that user access rights are reassessed once every six months.	No exceptions noted.
5.19	**Use of supplier's products and services** Processes and procedures are defined and implemented to manage the information security risks associated with the use of supplier's products or services.	We made inquiries of Management about the procedures/control activities performed. We have inspected that there is a formal and documented procedure ensuring that new or renegotiated application or supplier contracts are validated against a list of established information security requirements. We have inspected by sampling that risk assessments are conducted at appropriate intervals on critical suppliers. We have inspected that main suppliers are regularly reviewed based on agreed information security requirements.	No exceptions noted.

Control objective 5: Organisational controls

- Procedures and controls ensure management supports information security in line with business needs and legal requirements, including a framework for implementing and operating security measures.
- Procedures and controls ensure that access to information and systems are managed and monitored based on business needs and user roles, ensuring only authorised access and promptly addressing unauthorised attempts.
- Procedures and controls ensure that the organisation is prepared to effectively manage information security incidents, assess security events and maintain information security during disruptions.
- Procedures and controls ensure that an agreed level of information security in supplier relationships is maintained and correct and secure operation of information processing facilities.

No.	Trifork Security's control activity	Tests performed by PwC	Result of PwC's tests
5.20	**Managing information security in supplier agreements** Relevant information security requirements must be established and agreed upon with each supplier based on the type of supply relationship.	We made inquiries of Management about the procedures/control activities performed. We have inspected that a formal and documented procedure is in place to ensure that new or renegotiated application or service supplier contracts are validated against a list of defined information security requirements.	No exceptions noted.
5.22	**Monitoring, evaluation and change management of supplier services** The organisation must regularly monitor, evaluate, assess and manage changes in the supplier's information security practices and service delivery.	We made inquiries of Management about the procedures/control activities performed. We have inspected that there is a formal, documented procedure ensuring that new or renegotiated supplier contracts are validated against a list of established information security requirements. We have inspected by sampling signed contracts in which the information security requirements are contractually agreed upon.	No exceptions noted.

Control objective 5: Organisational controls

- Procedures and controls ensure management supports information security in line with business needs and legal requirements, including a framework for implementing and operating security measures.
- Procedures and controls ensure that access to information and systems are managed and monitored based on business needs and user roles, ensuring only authorised access and promptly addressing unauthorised attempts.
- Procedures and controls ensure that the organisation is prepared to effectively manage information security incidents, assess security events and maintain information security during disruptions.
- Procedures and controls ensure that an agreed level of information security in supplier relationships is maintained and correct and secure operation of information processing facilities.

No.	Trifork Security's control activity	Tests performed by PwC	Result of PwC's tests
5.24	**Information security incident management planning and preparation** Trifork Security has planned and prepared for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	We made inquiries of Management about the procedures/control activities performed. We observed that a formal and documented incident management process related to information security events and breaches has been implemented. We observed that the incident management processes have been communicated to employees. We observed that all incidents have been registered, that necessary actions have been performed and that the solutions have been documented in an incident management system and reported through the ISB.	No exceptions noted.
5.26	**Response to information security incidents** Information security incidents are handled in accordance with documented procedures.	We made inquiries of Management about the procedures/control activities performed. We have inspected that a formal and documented incident handling process has been implemented. We have inspected that all incidents are recorded, necessary actions are taken and solutions are documented in an incident management system.	No exceptions noted.
5.29	**Information security during disruption** There is a plan for how to maintain information security at an appropriate level during disruption.	We made inquiries of Management about the procedures/control activities performed. We have inspected that a formal and documented contingency plan is maintained, reviewed and approved annually. We have inspected that the underlying procedures for the contingency plan are reviewed with relevant personnel.	No exceptions noted.

Control objective 5: Organisational controls

- Procedures and controls ensure management supports information security in line with business needs and legal requirements, including a framework for implementing and operating security measures.
- Procedures and controls ensure that access to information and systems are managed and monitored based on business needs and user roles, ensuring only authorised access and promptly addressing unauthorised attempts.
- Procedures and controls ensure that the organisation is prepared to effectively manage information security incidents, assess security events and maintain information security during disruptions.
- Procedures and controls ensure that an agreed level of information security in supplier relationships is maintained and correct and secure operation of information processing facilities.

No.	Trifork Security's control activity	Tests performed by PwC	Result of PwC's tests
5.37	**Documented operating procedures** Operating procedures for information processing facilities are documented and made available to personnel who need them.	We made inquiries of Management about the procedures/control activities performed. We have inspected that operational procedures are established and updated at least annually. We have inspected that operational procedures are available to all relevant employees.	No exceptions noted.

Control objective 6: People controls

- Procedures and controls ensure that background checks are conducted, security requirements are included in contracts, training is provided, disciplinary actions are enforced and security responsibilities are managed post-employment.
- Procedures and controls ensure the use of confidentiality agreements, secure remote work arrangements and prompt reporting of security events.

No.	Trifork Security's control activity	Tests performed by PwC	Result of PwC's tests
6.1	**Screening** Before recruiting employees, the following background check is made: • A personal reference • The applicant's CV • Education and professional qualifications identity control • Criminal record.	We have inquired of Management about background checks and checks of criminal records. We have inspected that the procedure for appointment covers relevant areas. By inspection of a sample of employees, we have ascertained that background checks are performed.	No exceptions noted.
6.2	**Terms and conditions of employment** As part of the agreement with both permanent and temporary employees, a contract is signed which describes the company's and employee's responsibilities and obligations regarding information security.	We have inquired of Management about terms and conditions of employment We have observed that new employees are introduced to information security.	No exceptions noted.
6.3	**Information security awareness, education and training** Awareness and training in information security policies and procedures are continuously provided to employees.	We have inspected that information security topics are addressed at department meetings. We have inspected that employees are required to complete mandatory awareness training.	No exceptions noted.
6.5	**Responsibilities after termination or change of employment** In connection with termination of the employment relationship, it is ensured that confidentiality is maintained, assets are returned and access rights are removed.	We have inquired of Management about procedures and controls at employees' termination. We have inspected controls for employees terminated in 2024.	No exceptions noted.

Control objective 6: People controls

- Procedures and controls ensure that background checks are conducted, security requirements are included in contracts, training is provided, disciplinary actions are enforced and security responsibilities are managed post-employment.
- Procedures and controls ensure the use of confidentiality agreements, secure remote work arrangements and prompt reporting of security events.

No.	Trifork Security's control activity	Tests performed by PwC	Result of PwC's tests
6.6	**Confidentiality or non-disclosure agreements** Confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	We have inquired about procedures for obtaining non-disclosure agreements with Management. We have inspected that employees' contracts include a non-disclosure agreement.	No exceptions noted.
6.8	**Information security event reporting** All employees, collaborators and other users of systems and services are obliged to note and report any observed weaknesses or suspected weaknesses in systems and services. Security incidents are reported to Management as soon as possible.	We have inquired of a sample of employees about how security weaknesses are reported. We have inquired about how information and evidence regarding security weakness are obtained and managed. We have inquired about how the process for monitoring security breaches is managed.	No exceptions noted.

Control objective 7: Physical controls

- Procedures and controls ensure the establishing and maintaining of secure physical perimeters and entry controls to protect sensitive areas from unauthorised access, damage and interference.
- Procedures and controls ensure the protection of information and assets from physical and environmental threats, and maintain the integrity and availability of supporting utilities and equipment.

No.	Trifork Security's control activity	Tests performed by PwC	Result of PwC's tests
7.1	**Physical security perimeters** Security perimeters are defined and used to protect areas that contain information and other associated assets. IT equipment (servers, SAN, switches, primary backup, etc.) is located at hosting provider and is protected.	We made inquiries of Management about the procedures/control activities performed. We inspected that assurance reports are obtained from hosting providers and that they are reviewed to ensure that requirements are met.	No exceptions noted.
7.2	**Physical entry** Secure areas are protected by appropriate entry controls and access points.	We made inquiries of Management about the procedures/control activities performed. We inspected that assurance reports are obtained from hosting providers and that they are reviewed to ensure that requirements are met.	No exceptions noted.
7.5	**Protecting against physical and environmental threats** Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure, is designed and implemented.	We made inquiries of Management about the procedures/control activities performed. We inspected that assurance reports are obtained from hosting providers and that they are reviewed to ensure that requirements are met.	No exceptions noted.
7.8	**Equipment siting and protection** Equipment should be sited securely and protected. IT equipment located at service providers (servers, SAN, switches, primary backup, etc.) is protected.	We made inquiries of Management about the procedures/control activities performed. We inspected that assurance reports are obtained from hosting providers and that they are reviewed to ensure that requirements are met.	No exceptions noted.
7.9	**Security of assets off-premises** Procedures and safeguards are in place to protect off-site assets.	We made inquiries of Management about the procedures/control activities performed. We inspected that assurance reports are obtained from hosting providers and that they are reviewed to ensure that requirements are met.	No exceptions noted.

Control objective 7: Physical controls

- Procedures and controls ensure the establishing and maintaining of secure physical perimeters and entry controls to protect sensitive areas from unauthorised access, damage and interference.
- Procedures and controls ensure the protection of information and assets from physical and environmental threats, and maintain the integrity and availability of supporting utilities and equipment.

No.	Trifork Security's control activity	Tests performed by PwC	Result of PwC's tests
7.11	**Supporting utilities** Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities. IT equipment located at service providers (servers, SAN, switches, primary backup, etc.) is protected.	We made inquiries of Management about the procedures/control activities performed. We inspected that assurance reports are obtained from hosting providers and that they are reviewed to ensure that requirements are met.	No exceptions noted.
7.12	**Cabling security** Cables carrying power, data or supporting information services should be protected from interception, interference or damage. IT equipment located at service providers (servers, SAN, switches, primary backup, etc.) is protected.	We made inquiries of Management about the procedures/control activities performed. We inspected that assurance reports are obtained from hosting providers and that they are reviewed to ensure that requirements are met.	No exceptions noted.
7.13	**Equipment maintenance** Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information. IT equipment located at service providers (servers, SAN, switches, primary backup, etc.) is protected.	We made inquiries of Management about the procedures/control activities performed. We inspected that assurance reports are obtained from hosting providers and that they are reviewed to ensure that requirements are met.	No exceptions noted.
7.14	**Secure disposal or re-use of equipment** Items of equipment containing storage media are verified to ensure that any sensitive data and licenced software have been removed or securely overwritten prior to disposal or re-use.	We made inquiries of Management about the procedures/control activities performed. We inspected that assurance reports are obtained from hosting providers and that they are reviewed to ensure that requirements are met.	No exceptions noted.

Control objective 8: Technological controls

- Procedures and controls ensure the protection of information and network infrastructure through appropriate classification, secure authentication, robust network security measures and the application of secure system engineering principles.
- Procedures and controls ensure the protection of information systems against malware, enable recovery from data loss or system failures, and maintain redundancy to ensure continuous operation and resilience.
- Procedures and controls ensure the secure management of system configurations, the separation of development, test, and production environments, and the implementation of change management procedures to prevent vulnerabilities and maintain system integrity.
- Procedures and controls ensure the logging and monitoring of activities within information systems to detect and respond to anomalous behaviour and potential security incidents, thereby maintaining the integrity and security of the organisation's information systems.

No.	Trifork Security's control activity	Tests performed by PwC	Result of PwC's tests
8.2	**Privileged access rights** A policy for allocation and restriction of users with privileged access. All users with privileged access have a dedicated user for the privileged access. All access to operating systems, networks, databases and data files made available to new and existing users is audited in order to ensure compliance with the company policy. Steps are also taken to ensure that access permissions are dependent on the requirements of the job function and are approved and set up correctly in the systems.	We made inquiries of Management about the procedures/control activities performed. We inspected that formalised procedures are established for user administration and rights management and that these also apply to users with privileged rights. We inspected that authorisation granted to employees is accompanied by a justification of the level of access requested and an approval from the immediate superior.	No exceptions noted.
8.3	**Information access restriction** Access to information and other associated assets are restricted in accordance with the established topic-specific policy on access control.	We made inquiries of Management about the procedures/control activities performed. We have inspected that a policy for restricting access to systems and applications to employees with a work-related need has been implemented.	No exceptions noted.
8.5	**Secure authentication** Secure authentication technologies and procedures are implemented based on information access restrictions and the topic-specific policy on access control. Secure authentication technologies to sensitive information, which, among other things, include multi-factor authentication.	We made inquiries of Management about the procedures/control activities performed. We inspected that a formal policy for access control that defines allowed technical solutions for authentication is maintained. We inspected that access to the customer environment requires the use of multi-factor authentication.	No exceptions noted.

Control objective 8: Technological controls

- Procedures and controls ensure the protection of information and network infrastructure through appropriate classification, secure authentication, robust network security measures and the application of secure system engineering principles.
- Procedures and controls ensure the protection of information systems against malware, enable recovery from data loss or system failures, and maintain redundancy to ensure continuous operation and resilience.
- Procedures and controls ensure the secure management of system configurations, the separation of development, test, and production environments, and the implementation of change management procedures to prevent vulnerabilities and maintain system integrity.
- Procedures and controls ensure the logging and monitoring of activities within information systems to detect and respond to anomalous behaviour and potential security incidents, thereby maintaining the integrity and security of the organisation's information systems.

No.	Trifork Security's control activity	Tests performed by PwC	Result of PwC's tests
8.7	**Protection against malware** Protection against malware shall be implemented and supported by appropriate user awareness. Procedures for ensuring working antivirus software on all applicable systems. The antivirus software is monitored.	We made inquiries of Management about the procedures/control activities performed. We inspected by using samples that the employees' computers and servers are protected by antivirus.	No exceptions noted.
8.8	**Management of technical vulnerabilities** Information about technical vulnerabilities of information systems in use is obtained, the organisation's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.	We made inquiries of Management about the procedures/control activities performed. We have inspected relevant procedures.	No exceptions noted.
8.13	**Information backup** Backup copies of information, software and systems are maintained and regularly tested in accordance with the agreed topic-specific policy on backup. Backup are scheduled to run on a regular basis. Logs of the backup are monitored on a daily basis. Restore tests are conducted to verify that data are properly backed up and are recoverable.	We made inquiries of Management about the procedures/control activities performed. We inspected that monitoring has been implemented to ensure that continual and correct backup is performed. We have inspected that backup requirements have been established. We have inspected backup policies and that backup jobs are monitored. We have inspected that a full recovery test of IT environments has been conducted.	No exceptions noted.

Control objective 8: Technological controls

- Procedures and controls ensure the protection of information and network infrastructure through appropriate classification, secure authentication, robust network security measures and the application of secure system engineering principles.
- Procedures and controls ensure the protection of information systems against malware, enable recovery from data loss or system failures, and maintain redundancy to ensure continuous operation and resilience.
- Procedures and controls ensure the secure management of system configurations, the separation of development, test, and production environments, and the implementation of change management procedures to prevent vulnerabilities and maintain system integrity.
- Procedures and controls ensure the logging and monitoring of activities within information systems to detect and respond to anomalous behaviour and potential security incidents, thereby maintaining the integrity and security of the organisation's information systems.

No.	Trifork Security's control activity	Tests performed by PwC	Result of PwC's tests
8.15	**Logging** Logs that record activities, exceptions, faults and other relevant events are produced, stored, protected and analysed. Logs from critical systems are kept in a central log consolidation tool. Access rights are reduced to allow only one person to delete logs.	We made inquiries of Management about the procedures/control activities performed. We inspected that event logging of user activities, exceptions, faults and information security events has been configured.	No exceptions noted.
8.17	**Clock synchronisation** The clocks of information processing systems used by the organisation are synchronised to approved time sources.	We made inquiries of Management about the procedures/control activities performed. We have inspected that the clocks of servers and network devices are synchronised.	No exceptions noted.
8.18	**Use of privileged utility programs** The use of utility programs that are capable of overriding system and application controls are restricted and tightly controlled.	We made inquiries of Management about the procedures/control activities performed. We have observed procedures and scrips for creating new servers.	No exceptions noted.
8.19	**Installation of software on operational systems** Procedures and measures should be implemented to securely manage software installation on operational systems.	We made inquiries of Management about the procedures/control activities performed. We have observed patch procedures for servers and mobile devices. We have inspected that servers are patched according to procedures.	No exceptions noted.

Control objective 8: Technological controls

- Procedures and controls ensure the protection of information and network infrastructure through appropriate classification, secure authentication, robust network security measures and the application of secure system engineering principles.
- Procedures and controls ensure the protection of information systems against malware, enable recovery from data loss or system failures, and maintain redundancy to ensure continuous operation and resilience.
- Procedures and controls ensure the secure management of system configurations, the separation of development, test, and production environments, and the implementation of change management procedures to prevent vulnerabilities and maintain system integrity.
- Procedures and controls ensure the logging and monitoring of activities within information systems to detect and respond to anomalous behaviour and potential security incidents, thereby maintaining the integrity and security of the organisation's information systems.

No.	Trifork Security's control activity	Tests performed by PwC	Result of PwC's tests
8.20	**Network security management** Networks and network devices are secured, managed and controlled to protect information in systems and applications. Policies are implemented to ensure a secure communication and that tampering of data is minimised. Access to network devices is limited to employees with a work-related need.	We made inquiries of Management about the procedures/control activities performed. By inspection, we investigated whether, in accordance with guidelines, an appropriate security architecture has been established in the network, including whether: • network diagrams are maintained • remote access is granted through two-factor authentication • changes to the network environment, chosen for our random samples, are carried out in a controlled manner as described in the change management procedure.	No exceptions noted.

Control objective 8: Technological controls

- Procedures and controls ensure the protection of information and network infrastructure through appropriate classification, secure authentication, robust network security measures and the application of secure system engineering principles.
- Procedures and controls ensure the protection of information systems against malware, enable recovery from data loss or system failures, and maintain redundancy to ensure continuous operation and resilience.
- Procedures and controls ensure the secure management of system configurations, the separation of development, test, and production environments, and the implementation of change management procedures to prevent vulnerabilities and maintain system integrity.
- Procedures and controls ensure the logging and monitoring of activities within information systems to detect and respond to anomalous behaviour and potential security incidents, thereby maintaining the integrity and security of the organisation's information systems.

No.	Trifork Security's control activity	Tests performed by PwC	Result of PwC's tests
8.22	**Segregation of network** Groups of information services, users and information systems are segregated in the organisation's networks.	We made inquiries of Management about the procedures/control activities performed. We observed that networks have been segregated into secure zones. We have reviewed the technical security architecture and inspected whether an appropriate security level has been established according to the guidelines, including whether the network is divided into zones. We have observed, whether access to the network is divided into relevant user groups based on a work-related need. We observed that jump-hosts are utilised for layered security.	No exceptions noted.
8.31	**Separation of development, test and production environments** Separate IT environments for testing and production have been established.	We made inquiries of Management about the procedures/control activities performed. We observed whether, in accordance with guidelines, separate environments have been established for testing and operation.	No exceptions noted.
8.32	**Change management** Changes to information processing facilities and information systems are subject to change management procedures. The change control procedures require the initiation of tickets for all service requests. Ticket tracking includes	We made inquiries of Management about the procedures/control activities performed. We inspected the adequacy of change management procedures and inspected that an appropriate change management system has been established supported by a technical infrastructure.	No exceptions noted.

Control objective 8: Technological controls

- Procedures and controls ensure the protection of information and network infrastructure through appropriate classification, secure authentication, robust network security measures and the application of secure system engineering principles.
- Procedures and controls ensure the protection of information systems against malware, enable recovery from data loss or system failures, and maintain redundancy to ensure continuous operation and resilience.
- Procedures and controls ensure the secure management of system configurations, the separation of development, test, and production environments, and the implementation of change management procedures to prevent vulnerabilities and maintain system integrity.
- Procedures and controls ensure the logging and monitoring of activities within information systems to detect and respond to anomalous behaviour and potential security incidents, thereby maintaining the integrity and security of the organisation's information systems.

No.	Trifork Security's control activity	Tests performed by PwC	Result of PwC's tests
	source of request, change description, failback plan and risk indication and employees who are responsible. All changes must be approved. A request for change form is entered into the ticket by the ticket processor. The change processor executes risk assessment and classification.	Using random samples from the system used for documenting changes, we inspected whether, in accordance with guidelines, changes to the operating environment are carried out utilising a controlled process, including that: • Changes have an approval • Changes are assessed according to risk • Test and backout plan are described.	

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."

Mads Vigh
CEO
På vegne af: Trifork Security A/S
Serienummer: 9e48e84c-fcc8-4da7-9673-58e68ad0c0d7
IP: 83.151.xxx.xxx
2025-02-24 07:26:22 UTC

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
På vegne af: PricewaterhouseCoopers Statsautoriseret…
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 87.49.xxx.xxx
2025-02-24 07:40:33 UTC

Rico Lundager
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Senior manager
På vegne af: PricewaterhouseCoopers Statsautoriseret…
Serienummer: 2e75390a-f48a-4123-b26c-3fd3e97823aa
IP: 208.127.xxx.xxx
2025-02-24 08:11:16 UTC