Grant Thornton

# Assurance report

# Paychex Europe Denmark

ISAE 3402 type 2 assurance report on IT general controls for the period from 1 January 2025 to 31 December 2025 related to provision and operation of SaaS solutions

January 2026

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

# Table of contents

# Section 1: Paychex Europe Denmark’ statement

The accompanying description has been prepared for customers who have used Paychex Europe Denmark’s provision and operation of SaaS solutions, 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.

Throughout this document, "Paychex Europe Denmark" collectively refers to the following subsidiaries:

- Danske Lønsystemer ApS (VAT: 15 61 14 72)
- Lessor ApS (VAT: 24 24 00 10)
- Emply International ApS (VAT: 37 04 86 58)

The following systems are part of the provision and operation of SaaS solutions in scope for the audit:

- Lessor Løn
- Lessor Portal
- Lessor Workforce
- Danløn
- Emply

Paychex Europe Denmark is using the subservice organisations Netic A/S, NetNordic Denmark A/S, PostNord Strålfors A/S, Post Danmark A/S, Contractbook ApS, Bogholdergruppen.DK ApS, Compaya A/S, Trifork Security A/S and Netminds ApS.

This assurance report is prepared in accordance with the carve-out method and Paychex Europe Denmark’ description does not include control objectives and controls within Netic A/S, NetNordic Denmark A/S, PostNord Strålfors A/S, Post Danmark A/S, Contractbook ApS, Bogholdergruppen.DK ApS, Compaya A/S, Trifork Security A/S and Netminds ApS. Certain control objectives in the description can only be achieved, if the subservice organisation’s controls, assumed in the design of our controls, are suitably designed and operationally effective. The description does not include control activities performed by subservice organisations.

Some of the control areas, stated in Paychex Europe Denmark’ description in Section 3 of IT general controls, can only be achieved if the complementary user entity controls with the customers are suitably designed and operationally effective with Paychex Europe Denmark’ controls. This assurance report does not include the appropriateness of the design and operating effectiveness of these complementary controls.

Paychex Europe Denmark confirms that:

(a) The accompanying description in Section 3 fairly presents the IT general controls related to Paychex Europe Denmark’ provision and operation of SaaS solutions processing of customer transactions throughout the period from 1 January 2025 to 31 December 2025. The criteria used in making this statement were that the accompanying description:

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

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

(ii) Contains relevant information about changes in the IT general controls, performed during the period from 1 January 2025 to 31 December 2025

(iii) Does not omit or distort information relevant to the scope of Paychex Europe Denmark ApS, while acknowledging that the description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in their own particular environment

(b) The controls related to the control objectives stated in the accompanying description were suitably designed and functioning during the period from 1 January 2025 to 31 December 2025 if relevant controls with the subservice organisation were operationally effective and the customers have performed the complementary controls, assumed in the design of Paychex Europe Denmark's controls during the entire period from 1 January 2025 to 31 December 2025.

The criteria used in making this statement were that:

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

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

(iii) The controls were used consistently as drawn up, including the fact that manual controls were performed by people of adequate competence and authorisation, during the period from 1 January 2025 to 31 December 2025

Allerød, 19 January 2026
Paychex Europe Denmark ApS

Henrik Møller
Chief Executive Officer

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

To Paychex Europe Denmark, their customers and their auditors.

## Scope

We have been engaged to report on Paychex Europe Denmark's description in Section 3 of its system for delivery of Paychex Europe Denmark's provision and operation of SaaS solutions throughout the period 1 January 2025 to 31 December 2025 and about the design and operational effectiveness of controls related to the control objectives stated in the description. Paychex Europe Denmark is using the subservice organisations Netic A/S, NetNordic Denmark A/S, PostNord Strålfors A/S, Post Danmark A/S, Contractbook ApS, Bogholdergruppen.DK ApS, Compaya A/S, Trifork Security A/S and Netminds ApS.

This assurance report is prepared in accordance with the carve-out method and Paychex Europe Denmark's description does not include control objectives and controls within Netic A/S, NetNordic Denmark A/S, PostNord Strålfors A/S, Post Danmark A/S, Contractbook ApS, Bogholdergruppen.DK ApS, Compaya A/S, Trifork Security A/S and Netminds ApS. 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 Paychex Europe Denmark's description in Section 3 of IT general controls, can only be achieved if the complementary user entity controls with the customers have been appropriately designed and works effectively with the controls with Paychex Europe Denmark. The report does not include the appropriateness of the design and operating effectiveness of these complementary controls.

## Paychex Europe Denmark's responsibility

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

## Grant Thornton's independence and quality control

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

## Auditor's responsibility

Our responsibility is to express an opinion on Paychex Europe Denmark's description (Section 3) as well as on the design and operation of the controls related to the control objectives stated in that description based on our procedures. We conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organisation", issued by International Auditing and Assurance Standards Board.

This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively. An assurance engagement to report on the description, design, and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its system, and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgement, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved.

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

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

## Limitations of controls at a service organisation

Paychex Europe Denmark'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 Paychex Europe Denmark's statement in Section 1 and based on this, it is our opinion that:

(a) the description fairly presents how the IT general controls in relation to Paychex Europe Denmark's provision and operation of SaaS solutions were designed and implemented throughout the period from 1 January 2025 to 31 December 2025.

(b) the controls related to the control objectives stated in the description were suitably designed and implemented throughout the period from 1 January 2025 to 31 December 2025 in all material respects, and

(c) the controls tested, which were the controls necessary for providing reasonable assurance that the control objectives in the description were achieved in all material respects, operated effectively throughout the period from 1 January 2025 to 31 December 2025.

## Description of tests of controls

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

## Intended users and purpose

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

Copenhagen, 19 January 2026

**Grant Thornton**
Godkendt Revisionspartnerselskab

| | |
|---|---|
| Kristian Randløv Lydolph<br>State Authorised Public Accountant | Andreas Moos<br>Partner, CISA, CISM |

# Section 3: Description of Paychex Europe Denmark's services in connection with provision and operation of SaaS solutions, and related IT general controls

## Introduction

This document serves to provide comprehensive IT security compliance insights into Paychex Europe Denmark ApS (VAT: 37 54 56 94) subsidiaries SaaS solutions for customers and relevant stakeholders (including auditors). The intent is to ensure transparency for customers and their auditors regarding the IT security control measures implemented within the organisation.

These solutions encompass payroll and HR administration, shop floor management, time tracking, and workforce management.  The infrastructure in scope of the description is datacentre with Linux and Windows servers.

Throughout this document, "Paychex Europe Denmark" collectively refers to the following subsidiaries:

- Danske Lønsystemer ApS (VAT: 15 61 14 72)
- Lessor ApS (VAT: 24 24 00 10)
- Emply International ApS (VAT: 37 04 86 58)

The following systems are part of the provision and operation of SaaS solutions in scope for the audit:

- Lessor Løn
- Lessor Portal
- Lessor Workforce
- Danløn
- Emply

## Organisational structure and responsibilities

Paychex Europe Denmark employs about 400 staff members across various departments, including Administration, Finance, Development, Support, IT Security, IT Operations, and Product Departments.

The employees of Paychex Europe Denmark are thus responsible for the support of our own products as well as the hosting infrastructure. The support teams handle all incoming questions. They either solve the problems or pass on the task to the Operations Department for further processing.

Thus, the Operations Department acts as second line support and monitors existing operating solutions and other tasks associated with the day-to-day management of our hosting environment.

**Paychex Europe Denmark’s services**
Paychex Europe Denmark provides a comprehensive suite of solutions encompassing payroll and HR administration, shop floor management, time recording, and workforce management. These services are designed to enhance operational efficiency and compliance for customers.

## Paychex Europe Denmark’s organisation and responsibility

Paychex Europe Denmark has a clear and transparent corporate structure and employs over 500 employees.

The organisational structure of the Paychex Europe Denmark includes the departments Administration, Finance, Development, Support, IT-security and IT Operations as well as various product departments.

The employees of Paychex Europe Denmark are thus responsible for the support of our own products as well as the hosting infrastructure. The support teams handle all incoming questions. They either solve the problems or pass on the task to the Operations Department for further processing.

Thus, the Operations Department acts as second line support and monitors existing operating solutions and other tasks associated with the day-to-day management of our hosting environment.

**IT security compliance**
We work with IT security in our Information Security Management System (ISMS) that is used to protect and manage an organisation's information security in a systematic and efficient way. Its purpose is to identify, assess, and mitigate risks related to data and IT systems while ensuring the confidentiality, integrity, and availability of information.

## Organisation of information security

Delegation of responsibility for information security: Our organisation is divided into different areas of responsibility. We have prepared a number of detailed responsibility and role descriptions for employees on all levels. Confidentiality has been established for all parties involved in our business. The confidentiality is ensured via employment contracts.

Separation of functions: Through on-going documentation and processes, we try to eliminate or minimise the dependence on key management personnel. Tasks are assigned and defined via procedures for managing the operational services.

Contact with special interest groups: The operating staff subscribes to newsletters from e.g., DK-CERT and other sources to keep informed about the emerging security threat landscape.

## Information Security & Compliance Forum (ISF)

Paychex Europe Denmark has established an Information Security & Compliance Forum (ISF), consisting of key internal stakeholders from IT Operations, IT Security, and Legal & Compliance.

The purpose of ISF is to discuss and decide on matters related to IT security, including data protection and cybersecurity. ISF holds monthly meetings and reports directly to Executive Management.

## IT security policy

We have defined our quality standards system based on the general objective of providing our customers with a stable and secure service.

To comply with the objectives, we have implemented policies and procedures which ensure that our supplies are uniform and transparent. Our IT security policy is produced in accordance with ISO/IEC 27002:2022 and our information security management systems (ISMS) is based on ISO/IEC 27001:2022 that applies to all employees and all deliveries.

Our methodology for the implementation of controls is defined with reference to ISO 27002:2022 (guidelines for information security management) and is thus divided into the following control areas:

- Information security policies
- Organisation of information security
- Employee safety
- Asset management
- Conditional access
- Cryptography
- Physical security and environmental safeguards
- Operational safety
- Communication security
- Purchase, development, and maintenance of systems
- Supplier relationships
- Information security breach management
- Information security aspects related to emergency and restoration management
- Compliance

We continue to improve both policies, procedures, and operations.

## Security risk management

Paychex Europe Denmark conducts an annual risk assessment or as necessitated by significant operational changes. This evaluation considers both internal and external factors to mitigate risks associated with service delivery to an acceptable level.

IT risk analysis: Paychex Europe Denmark produced a risk analysis. On an annual basis or in case of significant changes, the group carries out a risk assessment of the assets of Paychex Europe Denmark. Both internal and external factors are taken into consideration.

The risk analysis provides an assessment of all risks identified. The risk analysis is updated on a yearly basis or in case of significant changes to ensure that the risks associated with the services provided are minimised to an acceptable level.

The responsibility for IT security lies with the CIO supported by the CISO of the company who also approves the risk analysis.

A structured risk management framework has been implemented, incorporating a scoring system for service-related risks. Each identified risk is quantitatively assessed based on probability and impact, with a predefined acceptable risk threshold of 20%. Continuous evaluations and remedial actions are undertaken to mitigate risks.

We have implemented a scoring system for risks associated with the delivery of our services.

We assess the risks which we believe we are facing point by point. We make use of a simple calculation method for this purpose: "probability %" * "impact %".

The acceptable level goes to 20 %. We continuously assess if we can reduce the risks and take initiatives to address these risks.

We update the IT security policy regularly and at least once a year. The IT security policy is approved by the CEO.

## Mobile equipment and teleworking

Mobile equipment and communication: We have made it possible for our employees to work from home via a VPN connection with two factor authentication. Portable units are protected by HDD passwords, log-in information, and HDD encryption. Mobile devices (smart phones, tablets etc.) can be used for the synchronisation of emails and the calendar.

Remote access: Only authorised persons are granted access to our network, systems and data. Access to corporate resources is protected with two factor authentication.

## Human resource security

**Prior to employment**
Screening: We have implemented procedures for the recruitment of staff and thoroughly examine the curriculum vitae (CV) of the applicant to ensure that we employ the right candidate regarding background and skills. Furthermore, we ensure that employees have clean criminal records.

Conditions of employment: The general terms of employment, e.g., confidentiality related to the customers and personal circumstances, are specified in the employment contracts/job descriptions of all employees in which, among other things, the termination of employment and sanctions following security breaches are also described.

**During employment**
Management’s responsibility: All new employees sign a contract prior to commencement of their employment.

The contract provides that the employee must comply with the policies and procedures existing at any time. The contract/job description clearly defines the responsibility and role of the employee.

Awareness of and training activities related to information security: Our assets are first of all our employees. We encourage our operating staff to maintain their qualifications, educations, and certifications through training courses, lectures, and other relevant activities to ensure that the employees concerned can be kept up to date with security and be aware of new threats.

Sanctions: The general terms of employment, e.g., confidentiality related to the customers' and personal circumstances, are specified in the employment contracts of all employees in which, among other things, the termination of employment and sanctions following security breaches are also described.

Responsibility related to the termination of employment: When an employee terminates, a procedure will be initiated to ensure that the employee returns all relevant assets, e.g., portable devices etc. and that the access to buildings, systems and data are withdrawn. The overall responsibility to ensure all control procedures upon termination of employment lies with the CEO of the company. The documentation related to the termination of employment is available in electronic form in the human resources department.

## Asset management

**Responsibility for assets**
List of assets: Servers and network equipment including configuration are registered to be used for documentation purposes and to gain an overview of equipment etc. To secure against unauthorised access and to ensure the transparency of the structure, we have prepared some documents describing the internal network including units, naming of units, logical division of the network etc.

The documentation for equipment is updated on a regular basis and reviewed at least once a year by our operating staff.

Ownership of assets: Central network units, servers, peripheral units & systems are owned by operating staff members of Paychex Europe Denmark.

Acceptable use of assets: This subject is described in the employee handbook.

Return of assets: When an employee terminates, a procedure will be initiated to ensure that the employee returns all relevant assets and that the access to buildings, systems and data is being withdrawn. The overall responsibility to ensure all control procedures upon termination of employment lies with the CEO of the company.

The documentation related to the termination of employment is available in electronic form in the human resources department.

**Classification of information**
We ensure appropriate protection of information of importance to the organisation and our customers. We make sure that all data are labelled and classified and is only processed based on documented processes.

## Access control

**Access control requirements**
Conditional access policies: The way the granting of access is handled is described in a policy document. The policy is part of our IT security policy.

**User access administration**
Procedures for creation and deletion of user profiles:

The user profiles of our customers are created solely due to the wishes of our customers. In some of the systems, the end-customer himself creates his user profile without interference from Paychex Europe Denmark's employees. Our own users are created as super users to ensure that our support teams can provide professional service. All user profiles must be personally identifiable. The access to passwords for accounts which only are used by systems (service users) are limited to few authorised persons.

Grant of rights: The granting of privileges is controlled in accordance with the regular user administration process. Privileges are only granted on a need-to-basis.

Handling of confidential login information: Personal login information is known only by the employee and subject to a password policy to ensure the complexity.

Evaluation of user access rights: Periodically, i.e., once a year, we review the internal systems of the company including user profiles and access levels to ensure that the procedure related to the termination of employment is followed and that the customers' data cannot be accessed by former employees of Paychex Europe Denmark.

**User responsibility**
Use of confidential password: The IT security policy provides that all employee passwords must be personal and that only the user knows the password. Passwords for service accounts etc. which cannot be used for logging in, and which are not changed for systemic reasons are stored in a separate system. Only a limited number of employees can access this system.

**Control of access to systems and data**
Limited access to data: The access for our employees is differentiated. Only systems, servers and data which are relevant to the area of work of each single employee are accessible.

System for the administration of passwords: All employees are subject to restrictions as regards the passwords to customer systems as well as the customers' own systems. All users have passwords which are subject to restrictions related to the creation of the passwords.

Some of our systems require the password to be complex and changed regularly. In other systems, the customer decides how often the password should be changed and how complex it should be.

## IT security

**Secure areas**
All customer facing services are hosted at a datacenter provider who has processes to ensure only accredited personnel has access.

**Cryptography**
We ensure the proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information. We have policies on how we manage encryption keys and encryption techniques.

**Operational safety**
Change management: All changes follow an implemented change management process and are documented in Jira.

Capacity management: We have established a monitoring system for monitoring capacity constraints. All incidents follow an implemented incident management process.

**Protection against malware**
Measures against malware: We use a number of sophisticated security tools and have a SOC/SIEM implemented.

**Backup**
We ensure that we will be able to recreate systems and data in an appropriate and correct manner in accordance with the agreements concluded with our customers. We have, for that purpose, developed a test to re-establish systems and data.

Backups of our customers' data take place with us. Backup copies are saved in electronic form on a physical location other than the data centre.

**Logging and monitoring**
Incident logging: Network traffic and server logs are monitored and logged. Security logs are forwarded to our SIEM solution.

Administrator and operator logs: The administrator logging process is performed simultaneously with the ordinary logging process.

Time synchronisations: We make use of Internet NTP servers for synchronisations of all servers.

Managing software in operating systems: Via our patch process we ensure that only approved and tested updates are being installed. All patching follows a patch management procedure.

Managing technical vulnerabilities: Safety warnings from DK-CERT, version 2 (or others) are monitored and analysed. If relevant, they are installed on our internal systems within one month from the date of issue. Our internal solutions are subject to ongoing risk assessments.

**Communication security**
Network measures: All traffic, incoming as well as outgoing, is filtered by the firewall rules and advanced IPS tools.

Ensuring network services: The customers access our systems via https. Data transferred from our systems to external partners are IP allowlisted and, if this is possible, sent via encrypted data protocols.

Network division: Our network is divided into service segments to ensure independence between the offered services. Furthermore, test and production environments are divided into two segments.

**Incident management**
We ensure a consistent and effective approach to information security breach management, including communication of security incidents and vulnerabilities. We have policies in place to ensure that employees know how security breaches are defined, managed, and reported. This policy also instructs that employees are required to report information security weaknesses.

**Business continuity management**
Emergency planning: Paychex Europe Denmark has prepared an emergency plan for the handling of an emergency. The emergency plan is anchored in the IT risk analysis and maintained at least once a year following the performance of the analysis.

The plan and the procedures are anchored in our operating documentation and procedures.

Testing, maintenance and re-evaluation of emergency plans: The plan is tested once a year as a part of our emergency preparedness procedure to ensure that the customers, at the lowest possible level, will be affected by an emergency situation.

Redundancy: We seek to ensure that all services are redundant to make sure that we, in the shortest possible time, will be able to re-establish the production environment in a new environment in case of non-repairable errors in the production environment. We continue to focus on this area.

## Compliance

Independent evaluation of information security: An evaluation will be carried out by an external IT auditor when preparing the annual ISAE 3402 report.

Compliance with security policies and standards: We carry out internal audits once a year in order to test if our internal policies and procedures are followed. The audits include all services and the infrastructure as well as other areas, if necessary.

## Changes implemented during the period

No significant changes have been implemented during the period.

## Complementary user entity controls with the data controller

Paychex Europe Denmark’s customers are, unless otherwise agreed, responsible for establishing connection to Paychex Europe Denmark’s servers.

Furthermore, the customers of the Paychex Europe Denmark are, unless otherwise agreed, responsible for:

- Ensuring their own employees' IT security awareness in relation to the use of our solutions
- Ensuring their own user profiles
- Ensuring their own Internet connection
- Ensuring own data

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

## Purpose and scope

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

This statement is issued according to the carve-out method and therefore does not include controls of Paychex Europe Denmark's subservice organisations.

Controls, which are specific to the individual customer solutions, or are performed by Paychex Europe Denmark's customers, are not included in this report.

## Tests performed

We performed our test of controls at Paychex Europe Denmark, by taking the following actions:

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

## Test results

Below, we have listed the tests performed by Grant Thornton as basis for the evaluation of the IT general controls with Paychex Europe Denmark.

### A.5 Organisational controls

Control objective: To ensure continuing suitability, adequacy, effectiveness of management direction and support for information security in accordance with business, legal, statutory, regulatory and contractual requirements.

| ***No.*** | ***Paychex Europe Denmark's control*** | ***Grant Thornton's test*** | ***Test results*** |
|---|---|---|---|
| 5.1 | *Policies for information security*<br>Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur. | We have inspected that the information security policy has been approved by management, published, and communicated to employees and relevant stakeholders.<br>We have inspected that the information security policy has been updated. | No deviations noted. |
| 5.2 | *Information security roles and responsibilities*<br>Information security roles and responsibilities should be defined and allocated according to the organisation's needs. | We have inspected an organisation chart showing the information security organisation.<br>We have inspected the description of roles and responsibilities within the information security organisation. | No deviations noted. |
| 5.3 | *Segregation of duties*<br>Conflicting duties and conflicting areas of responsibilities should be segregated. | We have inspected organisation charts showing that segregation of duties is established on an organisational level. | No deviations noted. |
| 5.4 | *Management responsibilities*<br>Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and the organisation's procedures. | We have inspected, that the management, in employment contracts, has required that personnel must comply with information security policies and procedures.<br>We have, by sample test, inspected that the requirements for compliance with information security measures are included in the employees' contracts of employment. | No deviations noted. |

## A.5 Organisational controls

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

| No. | Paychex Europe Denmark's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 5.6 | *Contact with special interest groups*<br>The organisation should establish and maintain contact with special interest groups or other specialist security forums and professional associations. | We have inspected that a procedure for contact with special interest groups has been designed.<br>We have inspected documentation that appropriate contact with special interest groups has been maintained. | No deviations noted. |
| 5.7 | *Threat intelligence*<br>Information relating to information security threats should be gathered and analysed to establish threat intelligence. | We have inspected that a procedure for threat intelligence has been designed.<br>We have inspected that identified threats are being registered and analysed. | No deviations noted. |

## A.5 Organisational controls

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

| No. | Paychex Europe Denmark's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 5.9 | *Inventory of information and other associated assets*<br>An inventory of information and other associated assets, including owners, should be developed and maintained. | We have inspected that an inventory of assets, including owners, has been developed and is maintained. | No deviations noted. |
| 5.11 | *Return of assets*<br>Personnel and other interested parties as appropriate should return all the organisation's assets in their possession upon change or termination of their employment, contract or agreement. | We have inspected that a procedure for return of assets has been designed.<br>We have, by sample test, inspected that personnel upon termination of employment have returned assets to the organisation. | No deviations noted. |

## A.5 Organisational controls

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

| No. | ***Paychex Europe Denmark's control*** | ***Grant Thornton's test*** | ***Test results*** |
|---|---|---|---|
| 5.12 | *Classification of information*<br>Information should be classified according to the information security needs of the organisation based on confidentiality, integrity, availability and relevant interested party requirements. | We have inspected that a procedure for classification of information has been designed.<br>We have inspected that information is classified according to the procedure. | No deviations noted. |

## A.5 Organisational controls

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

| No. | ***Paychex Europe Denmark's control*** | ***Grant Thornton's test*** | ***Test results*** |
|---|---|---|---|
| 5.15 | *Access control*<br>Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements. | We have inspected that both access management policy and procedure have been designed and updated. | No deviations noted. |
| 5.16 | *Identity management*<br>The full life cycle of identities should be managed. | We have, by sample test, inspected that identities are assigned unique user IDs enabling the traceability of actions performed.<br>We have, by sample test, inspected that assignment of user access rights is granted based on the job function and an approval from the immediate manager.<br>We have, by sample test, inspected that removal of user access rights is performed in a timely manner upon termination. | No deviations noted. |

| No. | Paychex Europe Denmark's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 5.17 | *Authentication information*<br>Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information. | We have inspected that a password management procedure has been designed.<br>We have inspected that the password configuration settings are set in accordance with the defined procedure. | No deviations noted. |
| 5.18 | *Access rights*<br>Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organisation's topic-specific policy on and rules for access control. | We have, by sample test, inspected that assignment of user access rights is granted based on the job function and an approval from the immediate manager.<br>We have, by sample test, inspected that removal of user access rights is performed in a timely manner upon termination.<br>We have inspected that access rights have been reviewed on a regular basis, and at least annually. | No deviations noted. |

## A.5 Organisational controls

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

| No. | Paychex Europe Denmark's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 5.22 | *Monitoring, review and change management of supplier services*<br>The organisation should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery. | We have inspected that monitoring activities, covering outsourced supplier services, have been performed for all significant suppliers.<br>We have inspected that any significant risks identified as part of the monitoring activities are followed up on. | No deviations noted. |
| 5.23 | *Information security for use of cloud services*<br>Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organisation's information security requirements. | We have inspected that information security measures covering the use of cloud services has been defined and implemented. | No deviations noted. |

## A.5 Organisational controls

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

| No. | Paychex Europe Denmark's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 5.24 | *Information security incident management planning and preparation*<br>The organisation should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities. | We have inspected that an incident management procedure has been designed.<br>We have inspected that roles and responsibilities related to the incident management procedure have been defined and made available to relevant employees. | No deviations noted. |
| 5.25 | *Assessment and decision on information security events*<br>The organisation should assess information security events and decide if they are to be categorised as information security incidents. | We have inspected the procedure for assessment and decision on information security events.<br>We have, by sample test, inspected that information security incidents have been categorised according to the procedure. | No deviations noted. |
| 5.26 | *Response to information security incidents*<br>Information security incidents should be responded to in accordance with the documented procedures. | We have inspected the procedure for responding to information security incidents.<br>We have, by sample test, inspected that information security incidents have been responded to, according to the procedure. | No deviations noted. |
| 5.27 | *Learning from information security incidents*<br>Knowledge gained from information security incidents should be used to strengthen and improve the information security controls. | We have inspected the procedure for learning from information security incidents.<br>We have inspected that security incidents have been registered in order to gain information to reduce the probability of recurrence. | No deviations noted. |

## A.5 Organisational controls

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

| No. | Paychex Europe Denmark's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 5.29 | *Information security during disruption*<br>The organisation should plan how to maintain information security at an appropriate level during disruption. | We have inspected that business contingency plans are designed and approved by management.<br>We have inspected that the business contingency plans are made available to relevant employees.<br>We have inspected that the business contingency plans have been tested. | No deviations noted. |

## A.5 Organisational controls

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

| No. | Paychex Europe Denmark's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 5.30 | *ICT readiness for business continuity*<br>ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements. | We have inspected that a business impact analysis (BIA) has been performed.<br>We have inspected that time recovery time objectives (RTO) and recovery point objectives (RPO) have been identified for relevant resources.<br>We have inspected that continuity plans, including recovery time objectives (RTO) and recovery point objectives (RPO), have been tested. | No deviations noted. |

## A.5 Organisational controls

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

| No. | Paychex Europe Denmark's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 5.36 | *Compliance with policies, rules and standards for information security*<br>Compliance with the organisation's information security policy, topic-specific policies, rules and standards should be regularly reviewed. | We have inspected that the organisation has defined a list of controls for compliance with policies and procedures.<br>We have, by sample test, inspected that the controls for compliance with policies and procedures, have been performed and that identified control deficiencies are followed up on. | No deviations noted. |
| 5.37 | *Documented operating procedures*<br>Operating procedures for information processing facilities should be documented and made available to personnel who need them. | We have inspected that operating procedures have been designed and documented.<br>We have inspected that the operating procedures are made available to relevant employees. | No deviations noted. |

## A.6 People controls

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

| No. | Paychex Europe Denmark's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 6.1 | *Screening*<br>Background verification checks on all potential candidates should be carried out prior to joining the organisation and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. | We have inspected that a procedure for screening of new employees has been designed.<br>We have, by sample test, inspected that background verification checks have been performed for new hires in accordance with the procedure. | No deviations noted. |

| No. | Paychex Europe Denmark's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 6.2 | *Terms and conditions of employment*<br>The employment contractual agreements should state the personnel's and the organisation's responsibilities for information security. | We have, by sample test, inspected that signed employment agreements state the personnel's and the organisation's responsibilities for information security. | No deviations noted. |

## A.6 People controls

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

| No. | Paychex Europe Denmark's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 6.5 | *Responsibilities after termination or change of employment*<br>Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties. | We have inspected that information security responsibilities and duties that remain valid after termination or change of employment have been defined.<br>We have, by sample test, inspected that terminated employees have been informed that information security responsibilities and duties are still valid after termination of employment. | No deviations noted. |

## A.6 People controls

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

| No. | Paychex Europe Denmark's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 6.8 | *Information security event reporting*<br>The organisation should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner. | We have inspected that a procedure for reporting of information security events has been designed.<br>We have inspected that employees are able to report information security events and that these are followed up on by appropriate personnel. | No deviations noted. |

## A.7 Physical controls

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

| No. | Paychex Europe Denmark's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 7.1 | *Physical security perimeters*<br>Security perimeters should be defined and used to protect areas that contain information and other associated assets. | We have inspected the procedure for physical protection of facilities and security perimeters.<br>We have inspected relevant locations and their security perimeters to establish whether security measures have been implemented to prevent unauthorised access. | No deviations noted. |
| 7.2 | *Physical entry*<br>Secure areas should be protected by appropriate entry controls and access points. | We have inspected the procedure for granting physical access.<br>We have inspected access points and entry ways to establish, whether personal access cards are used to gain access to the office.<br>We have inspected that alarms have been installed for physical access control and that these are active.<br>We have inspected that review of physical access rights have been performed during the period. | No deviations noted. |
| 7.4 | *Physical security monitoring*<br>Premises should be continuously monitored for unauthorised physical access. | We have inspected appropriate level of monitoring of premises.<br>We have inspected continuous monitoring of unauthorised physical access. | No deviations noted. |

## A.8 Technological controls

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

| No. | Paychex Europe Denmark's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 8.2 | *Privileged access rights*<br>The allocation and use of privileged access rights should be restricted and managed. | We have inspected the procedures for allocation, use and restrictions of privileged access rights.<br>We have inspected a list of privileged users, and we have inquired into whether access rights have been allocated based on a work-related need.<br>We have inspected that privileged user accesses are personally identifiable.<br>We have inspected that periodical review of privileged access rights is being performed. | No deviations noted. |
| 8.3 | *Information access restriction*<br>Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control. | We have inspected that both access management policy and procedure have been designed and updated.<br>We have, inspected that assignment of user access rights is based on user groups and roles that comprises of specific access, such as read, write, delete and execute.<br>We have inspected that access to sensitive information is restricted to a work-related need.<br>We have inspected that access rights have been reviewed on a regular basis and at least annually. | No deviations noted. |
| 8.5 | *Secure authentication*<br>Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control. | We have inspected that a password management procedure has been designed.<br>We have inspected that the password configuration settings are set in accordance with the defined procedure.<br>We have inspected that multi-factor authentication is installed and enabled. | No deviations noted. |

## A.8 Technological controls

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

| No. | Paychex Europe Denmark's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 8.6 | *Capacity management*<br>The use of resources should be monitored and adjusted in line with current and expected capacity requirements. | We have inspected that information processing resources are monitored.<br>We have inspected that detective controls are implemented to identify problems. | No deviations noted. |
| 8.7 | *Protection against malware*<br>Protection against malware should be implemented and supported by appropriate user awareness. | We have inspected that a procedure for protection against malware has been designed.<br>We have, by sample test, inspected that anti-malware has been implemented on servers.<br>We have, by sample test, inspected that anti-malware has been implemented on laptops. | No deviations noted. |
| 8.8 | *Management of technical vulnerabilities*<br>Information about technical vulnerabilities of information systems in use should be obtained, the organisation's exposure to such vulnerabilities should be assessed and appropriate measures should be taken. | We have inspected that a procedure for management of technical vulnerabilities has been designed.<br>We have inspected that the organisation has established a control for identification and registration of technical vulnerabilities.<br>We have, by sample test, inspected that registered technical vulnerabilities are evaluated and responded to. | No deviations noted. |

## A. 8 Technological controls

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

| No. | Paychex Europe Denmark's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 8.10 | *Information deletion*<br>Information stored in information systems, devices or in any other storage media should be deleted when no longer required. | We have inspected that a procedure for the deletion of information has been established.<br>We have inspected that systems are configured to automatically delete information in accordance with the procedure.<br>We have inquired whether any relevant media has been disposed of during the audit period. | No deviations noted. |
| 8.11 | *Data masking*<br>Data masking should be used in accordance with the organisation's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration. | We have inspected that a procedure for data masking has been designed.<br>We have inspected that sensitive information is protected by masking procedures. | No deviations noted. |
| 8.12 | *Data leakage prevention*<br>Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information. | We have inspected that a procedure for data leakage prevention has been designed.<br>We have inspected that data leakage prevention measures have been implemented in accordance with the procedure. | No deviations noted. |

## A.8 Technological controls

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

| No. | Paychex Europe Denmark's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 8.13 | *Information backup*<br>Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup. | We have inspected that a procedure for backup of data has been designed.<br>We have, by sample test, inspected that backup copies are made continuously in accordance with the procedure.<br>We have, by sample test, inspected that daily backup reports are received from the backup system specifying whether the backup has been successfully completed.<br>We have, by sample test, inspected that failed or erroneous backup jobs are identified and corrected.<br>We have inspected that regular tests of backup data are performed to verify whether the data can be restored from backup files. | No deviations noted. |

## A. Technological controls

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

| **No.** | ***Paychex Europe Denmark's control*** | ***Grant Thornton's test*** | ***Test results*** |
|---|---|---|---|
| 8.15 | *Logging*<br>Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed. | We have inspected that a procedure for log management has been designed.<br>We have inspected that logs are configured in accordance with the procedure including, as a minimum, the caption of:<br>• user IDs<br>• system activities<br>• dates, times and details of events<br>We have inspected that logs are protected against manipulation or deletion. | No deviations noted. |
| 8.16 | *Monitoring activities*<br>Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents. | We have inspected that a procedure for monitoring activities of log information has been designed.<br>We have inspected that log information has been monitored in accordance with the procedure. | No deviations noted. |
| 8.17 | *Clock synchronisation*<br>The clocks of information processing systems used by the organisation should be synchronised to approved time sources. | We have inspected that clocks used by the organisation and supporting information processing systems are synchronised from one reference time protocol. | No deviations noted. |

## A. Technological controls

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

| ***No.*** | ***Paychex Europe Denmark's control*** | ***Grant Thornton's test*** | ***Test results*** |
|---|---|---|---|
| 8.19 | *Installation of software on operational systems*<br>Procedures and measures should be implemented to securely manage software installation on operational systems. | We have inspected that a procedure for installation of software on operational systems has been designed.<br>We have, by sample test, inspected that applications, operating systems, databases and third-party software are patched in accordance with the procedure.<br>We have, by sample test, inspected that applications, operating systems, databases and third-party software are updated or replaced if they are no longer supported by the supplier. | No deviations noted. |

## A. Technological controls

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

| ***No.*** | ***Paychex Europe Denmark's control*** | ***Grant Thornton's test*** | ***Test results*** |
|---|---|---|---|
| 8.20 | *Networks security*<br>Networks and network devices should be secured, managed and controlled to protect information in systems and applications. | We have inspected that a network security policy has been designed.<br>We have inspected that virtual private network (VPN) is used for secure encrypted connection with networks outside of the organisation.<br>We have inspected that the network is monitored for anomalies and that these are followed up on. | No deviations noted. |

| No. | Paychex Europe Denmark's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 8.21 | *Security of network services*<br>Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored. | We have inspected that a network security policy has been designed.<br>We have inspected that firewalls and intrusion detection systems are installed on the network.<br>We have inspected that the network is monitored for anomalies and that these are followed up on. | No deviations noted. |
| 8.22 | *Segregation of networks*<br>Groups of information services, users and information systems should be segregated in the organisation's networks. | We have inspected that a network security policy has been designed.<br>We have inspected that network segmentation is implemented which divides the network into multiple zones. | No deviations noted. |
| 8.24 | *Use of cryptography*<br>Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented. | We have inspected that a policy defining rules for the use of cryptography has been defined.<br>We have, by sample test, inspected that information is protected in accordance with the cryptography policy. | No deviations noted. |

## A.8 Technological controls

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

| No. | Paychex Europe Denmark's control | Grant Thornton's test | Test results |
|---|---|---|---|
| 8.28 | *Secure coding*<br>Secure coding principles should be applied to software development. | We have inspected that a software development procedure has been designed.<br>We have, by sample test, inspected that new software has been developed in accordance with the procedure. | No deviations noted. |

## A.8 Technological controls

Control objective: To ensure that changes to applications, database systems, and associated infrastructure are properly authorised, documented, tested, approved, and implemented in the production environment.

| ***No.*** | ***Paychex Europe Denmark's control*** | ***Grant Thornton's test*** | ***Test results*** |
|---|---|---|---|
| 8.32 | *Change management*<br>Changes to information processing facilities and information systems should be subject to change management procedures. | We have inspected that a change management procedure has been designed.<br>We have, by sample test, inspected that key stakeholders have approved changes prior to release into production.<br>We have, by sample test, inspected that changes – prior to release into production - are tested based on established criteria. | No deviations noted |

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

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

## Henrik Basso Reichsthaler Møller

**Underskriver 1**
*Serial number: e2bb9ab5-a11a-4b50-864e-8c58af066374*
*IP: 2.106.xxx.xxx*
*2026-01-19 12:18:07 UTC*

## Andreas Moos

**Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936**
**Underskriver 2**
*Serial number: 8ba4bf1c-2aac-4cbe-9a4b-48056ec67035*
*IP: 62.243.xxx.xxx*
*2026-01-19 12:22:39 UTC*

## Kristian Randløv Lydolph

**Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936**
**Underskriver 3**
*Serial number: 84758c07-82ce-4650-a48d-5224b246b5c4*
*IP: 62.243.xxx.xxx*
*2026-01-19 15:12:23 UTC*