

Assurance report

Paperflow ApS

ISAE 3402 type 2 assurance report on general IT-controls for the period 1 August 2021 to 31 July 2022 related to Paperflow ApS' SaaS-platform

Grant Thornton | www.grantthornton.dk

Højbro Plads 10, 1200 København K

November 2022

CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

Table of contents

Section 1:	Description of Paperflow ApS' services in connection with operating of Paperflow ApS' SaaS-platform, and related general IT-controls.....	1
Section 2:	Paperflow ApS' statement	8
Section 3:	Independent service auditor's assurance report on the description of controls, their design and functionality	9
Section 4:	Control objectives, controls and service auditor testing.....	12

Section 1: Description of Paperflow ApS' services in connection with operating of Paperflow ApS' SaaS-platform, and related general IT-controls

The following is a description of Paperflow ApS' services which are included in the general IT-controls of this assurance report. The report includes general processes and system setups etcetera with Paperflow ApS. Processes and system setups etcetera, individually agreed with Paperflow ApS' customers, are not included in this report. Assessment of customer specific processes and system setups etcetera will be stated in specific assurance reports for customers who may have ordered such. Controls in the application systems are not included in this report.

1.1. General IT-controls at Paperflow ApS

In the following, a description of the general IT-controls related to Paperflow ApS' services to customers (or customer in case of a specific report), according to the above description in paragraph 1.1.

Use of subservice organisations

Paperflow ApS uses significant subservice organisations (Microsoft Azure and Google G-Suite) in connection with the supply of their SaaS service.

Paperflow ApS and our services

Paperflow ApS was founded to solve inefficient and heavy processes that exist in document management as well as to eliminate manual work.

Paperflow ApS' mission is elimination of all manual work in accounting, and to be the best and cheapest solution for document automation.

Paperflow ApS' scanning engine is easy to integrate with existing software systems in the cloud and does not require training or customization.

The purpose of Paperflow ApS is to lower bookkeeping costs by seamless automation of data processes for invoices and receipts, as well as being cost effective by reducing the cost of bookkeeping.

Organization and responsibility

Paperflow ApS employs about 10 employees, and is divided into the departments sales, administration, delivery and development. Sales and development work closely together to optimize our customers' business.

Responsibility

Development: Development and maintenance based on Product priorities. At the same time, it is development's responsibility that standard processes for development, deployment and server environments are complied with. Likewise, IT security is primarily here.

Sales: Sales' primary task is to increase the top line in the company through the partner-based strategy the company has set. Sales are measured on the revenue achieved with the resources allocated.

Delivery: Delivery is responsible for both delivery of operations (manual check of vouchers) and onboarding of new partners. There are critical SLAs associated with operations for which delivery is responsible. This requires coordination with all departments, as it requires insight into sales, server pressure, roadmap and finances. Delivery is also held directly responsible for customers' experience of integrating with the company's platform.

Administration: Administration is responsible for budget, reporting, financial operations, supplier agreements, GDPR and all legal tasks. Administration is measured on whether the budget is complied with, and the quality of the agreements entered.

All departments report to the CEO.

Management has the overall responsibility for the IT security in Paperflow ApS but can delegate controls to relevant employees.

Information security requirements

The information security requirements below are further described and specified as rules in relevant independent policies, procedures, handbooks and intranet pages.

Our methodology for implementing controls is defined with reference to ISO 27002 (Code of practice for information security controls), and is thereby overall divided into the following control areas:

- 4 – Risk assessment and management
- 5 – Information security policies
- 6 – Organisation of information security
- 7 – Human resource security
- 8 – Asset management
- 9 – Access control
- 10 – Cryptography
- 11 – Physical and environmental security
- 12 – Operations security
- 13 – Communications security
- 14 – System acquisition, development, and maintenance
- 15 – Supplier relationships
- 16 – Information security incident management
- 17 – Information security aspects of business continuity management
- 18 – Compliance

The controls are carried out either monthly, quarterly, or annually. All controls are gathered in our control wheel and completion of the controls is supported by automation of the control process.

Policies, procedures, guidelines, and controls are reviewed and updated on an ongoing basis.

5. Information Security Policy

The IT Security Group is responsible for Paperflow ApS' information security policy and must ensure that it is implemented and that employees of Paperflow ApS follow it.

There must be an Information Security Policy approved by Management and published to employees and relevant parties. The IT Security Policy and associated strategic and tactical documents can always be found in updated versions in our Intranet.

All Paperflow ApS' employees are obliged to comply with the Information Security Policy in force at any time with associated guidelines, procedures, and related documents. A violation can, depending on the circumstances, result in penalties or, in the worst case, dismissal. The Executive Board makes the final decision in relation to the aforementioned.

If an employee has knowledge or suspicion that Paperflow ApS' information security is being breached, the employee must notify the IT Security Group or management team as soon as possible after he/she has become aware of the breach.

The Information Security Policy is periodically reassessed or in connection with significant changes to systems or architecture - however at least once per year.

If situations arise where the requirements of the information security policy cannot be complied with, a written exemption from management must be made available. Any exemptions must be included in the annual risk assessment and included in the reporting to the Board of Directors of Paperflow ApS. Any deviations from the requirements must always be documented and alternative security measures must be introduced.

Risk assessment and management

We have procedures to ensure that the risks connected with the products and services that we provide are minimized to an acceptable level, and we regularly perform a risk assessment.

Risk assessment is performed periodically as well as when we perform changes or implement new systems that we consider relevant for reviewing our general risk assessment.

Risks can be accepted if it is assessed that the risk is low, or if the expenses related to rectifying the risks are not cost-effective for the company.

6. Organization of information security

We have comprehensive role and responsibility descriptions at all levels. The overall responsibility for information security lies with the IT Security Group, consisting of a member of Executive Board and Head of operations.

It is the responsibility of the IT Security Group to ensure, that the IT Security Policy is compliant with laws and regulations. Also, the IT Security Group is responsible for physical security.

Segregation of duties

Our documentation and processes ensure in general that we eliminate or minimize dependency on key persons, and that critical or sensitive tasks and processes are segregated.

Segregation of duties is an important part of our organisation and operations, which is why we, by means of access control and rights management, ensure that only authorized personnel can perform the necessary actions on systems and data.

Mobile equipment and remote workstations

Paperflow ApS' policy for the use of laptops, tablets, smartphones, and USB keys outside the company is that employees may not use WIFI where no code and security is required for use. The employees have activated two-factor authentication, which ensures that only the specific employee has access to their mobile devices.

For employees who use BYOD (bring your own device), these have been instructed that they may not download documents etc. relating to Paperflow ApS and that they must therefore work online in drive.

This is further described in Paperflow ApS' employee handbook and applies if an employee works at home.

7. Human resource security

Employees and consultants must know their responsibilities in relation to information security and comply with the company's security requirements set out in the company's procedures related to information security.

Employees and consultants must receive the required education and training to minimize the risk of human error, abuse, and fraud. Employees and consultants undertake, in connection with their employment, confidentiality through an NDA, DPA or employment contract.

The company only hires competent employees, which is ensured by obtaining references from previous employers as well as by assessing competencies in connection with reviewing the application and by job interview.

We have procedures in place for managing employee safety, for hiring, developing and termination of employees.

8. Asset Management

Identification and ownership of critical assets is defined and documented. Delivery is responsible for ensuring that software, servers, and network equipment are registered and documented.

Every employee is responsible for handling handed out equipment in accordance with the company's policies.

Data classification

There are different categories of information assets in Paperflow ApS. They are protected to varying degrees based on assessment in the categories: public, internal, confidential and secret.

Critical assets must be maintained and securely updated to protect any contained data.

Media management

All portable media that has access is subject to virus protection so that the best possible protection is ensured.

An employee's personal assets are cleaned and reset after leaving the company, to ensure that data cannot be recovered.

9. Access Control

Business requirements of access control

Access management must be documented and must be in accordance with business requirements, regulatory requirements, and security requirements.

Access must be granted based on work-related needs. Access must comply with specific customer agreements and NDAs.

User access management

Formalized procedures provide a framework for the creation, decommissioning and ongoing review of assigned roles, rights, and responsibilities. Access controls support a complete separation of duties where possible.

10. Cryptography

Access to systems and information assets are encrypted. Confidential information is always encrypted when it is stored on portable equipment such as laptops, USB connectors, tablets, and smartphones. If access to portable devices cannot be encrypted, confidential information on the device must not be processed. Necessary tools are made available to the company's employees, enabling them to comply with the encryption requirement.

Password encryption is based on recognized encryption technology. Passwords must never be stored unencrypted.

All APIs, both for receiving and sending customer data, must be encrypted with recognized standards.

11. Physical and environmental security

Access to the company's office must be restricted to avoid any possible damage, theft, and interruptions.

Administration of keys to the office must be documented. In addition, access to areas used for technical installations must be restricted, this must also be done for access to archives or where access is only relevant for selected groups.

Access to areas is based on the principle of work-related needs and is outlined in the Employee Handbook.

Paperflow ApS is a cloud Company, and the company does not have any on premise servers or a server room.

The company has a clean desk, clear screen policy lined out in the employee Handbook.

12. Operations security

Documented operating procedures

Operating procedures are documented in Paperflow ApS' IT Handbook and various procedures available in the company.

Systems for development, testing and operating must be separated as lined out in the IT Handbook.

Change management

All changes to IT services and systems must be logged with time and responsible person and undergo relevant approvals and tests.

Capacity management

Paperflow ApS monitors the capacity of our production system in several areas.

Malware protection

Paperflow ApS uses standard, pre-hardened system images for our servers, ensuring against unintentional access. The few accesses that have been opened for our system to work are secured against malware by various measures such as rate limiting, access control and scanning of submitted voucher files. Paperflow ApS' employee handbook describes our policy on antivirus on employee machines, for which periodic inspections are performed.

Backup

Paperflow ApS backs up every night and always has the latest backup available as well as 30 days back in time.

Logging and monitoring

Paperflow ApS' systems generate relevant log lines continuously, at different levels depending on how critical they are. The monitoring system alerts relevant persons and eventual corrections are included in the daily work.

Management of software on operating systems

Paperflow ApS makes use of standard, pre-hardened system images from Google. This means that the company knows and controls software it knows. All updates are examined and tested before they are commissioned following our process of patching and updating systems. Our employee machines are periodically updated with the latest security updates.

Management of technical vulnerabilities

Paperflow ApS subscribes to security news from the company's core software vendors for our systems. With the new software update, it is assessed whether a manual test of the software must be performed before it is accepted.

13. Communication security

Network security management

To be able to access Paperflow ApS' network, an access code is required. The code is provided by the nearest manager or service desk. Customers are asked to use their own mobile network.

Information transfer

Confidential information is only exchanged via e-mail stating that the information is confidential. Confidential information is only shared with the company's employees. If the confidential information is needed in conclusion of a customer contract it can be shared with the customer.

Before entering into an agreement with a subcontractor, the company's "Form for concluding an agreement with a subcontractor" is used, which states that certain conditions must exist before it is possible to enter into such an agreement. Confidentiality agreements with subcontractors and partners are stored in the company's digital contract system.

14. Acquisition, development, and maintenance of systems

Information security requirements for IT systems and test data are documented in our IT Handbook, our intranet (Confluence) and procedure documents.

Security requirements for information systems

Paperflow ApS uses standard pre-hardened system images for our servers, and it is only through access that our proprietary software needs to be opened in these images. The company periodically reviews open ports as well as access to our operating system, where ports that should no longer be open are closed. All "of the shelf" software is examined internally, and it is documented which accesses are needed during installation.

Security in development and support processes

All changes that are added to the operating environment are planned as part of our development process, which is described in the company's IT handbook. The changes will be commissioned on an ongoing basis, where relevant customers will be notified in advance. Decisions are made on fallback opportunities as well as any outstanding issues, and a risk assessment of the commissioning will be made here. All changes to the company's database schema are performed as a migration.

15. Supplier relationships

Information Security in Supplier Relationships

Paperflow ApS enters into a data processor agreement with all suppliers, to ensure that they comply with the Data Protection Regulation, in the case of a supplier located in the United States, it is ensured that the supplier has acceded to the U.S. Privacy Shield.

For each supplier, a Supplier Owner must be appointed. It is the duty of this Supplier Owner to ensure, that required agreements covering IT security matters are in place and reviewed on a regular basis, and that the system and data access to and from this supplier is correctly defined and maintained.

Before entering into an agreement with a subcontractor, the company's "Form for concluding an agreement with a subcontractor" is used, which states that certain conditions must exist before it is possible to enter into

such an agreement. Confidentiality agreements with subcontractors and partners are stored in the company's digital contract system.

Management of third-party services

Where possible, Paperflow ApS obtains the auditor's statements from suppliers if they have an ISO 27001 or similar. Paperflow ApS also makes physical visits to the company's supplier in Bulgaria.

16. Information security incident management

Management of information security breaches and improvements

If an employee becomes aware of a security incident, he or she must notify the IT Security Group. The IT Security Group will then, together with the employee, follow the procedure for handling security incidents - in this it is determined which steps are to be taken after the IT security group has become aware of the security incident. The handling of a security incident is documented and uploaded in the company's digital folder for security incidents.

The IT Security Group is also responsible for coordinating the process, updating the priority, and provide what is necessary to be able to stop the incident, also it must ensure ongoing communication about the incident, the consequences that have arisen, the status of the process, measures, and remedial measures.

17. Information security aspects of business continuity management

Contingency plans must include information security requirements that apply during a crisis. The plans are updated when significant changes happen and are tested based on a risk assessment.

18. Compliance

Paperflow ApS is subject to Danish law and complies with the laws and regulations that are relevant to the conduct its business. The company has also taken measures to comply with the Data Protection Regulation, including the Data Protection Act.

The Company will yearly undergo an audit from an external auditor to achieve an ISAE 3402 statement.

Complementary controls

Paperflow ApS' customers are, unless otherwise agreed, responsible for establishing a secure connection to Paperflow ApS' servers. In addition, Paperflow ApS' customers, unless otherwise agreed, are responsible for:

- To have and maintain all equipment necessary to connect to Paperflow ApS' servers / networks
- To ensure that relevant equipment is up to date
- To have backups of all submitted invoices, documents etc.
- Inform Paperflow ApS in a timely manner about relevant changes in the customer's organization so that Paperflow ApS can best provide a secure service to the customer. This could be changes in responsibility, termination of contract and the like.

Section 2: Paperflow ApS' statement

The accompanying description has been prepared for customers who have used Paperflow ApS' SaaS-platform 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.

Paperflow ApS is using subservice organisations Microsoft Azure and Google G-Suite. This assurance report is prepared in accordance with the carve-out method and Paperflow ApS' description does not include control objectives and controls within Microsoft Azure and Google G-Suite.

Paperflow ApS confirms that:

- (a) The accompanying description in Section 1 fairly presents the general IT-controls related to Paperflow ApS' SaaS-platform processing customer transactions throughout the period 1 August 2021 to 31 July 2022
- 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 general IT-controls
 - Relevant control objectives and controls designed to achieve these objectives
 - Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary, to achieve the control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by us alone
 - Other aspects of our control environment, risk assessment process, information system and communication, control activities, and monitoring controls that were relevant to general IT-controls
 - (ii) Contains relevant information about changes in the general IT-controls, performed during the period 1 August 2021 to 31 July 2022
 - (iii) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in their own particular environment
- (b) The controls related to the control objectives stated in the accompanying description were suitably designed and functioning during the period 1 August 2021 to 31 July 2022. The criteria used in making this statement were that:
- (i) The risks that threatened achievement of the control objectives stated in the description were identified
 - (ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved
 - (iii) The controls were used consistently as drawn up, including the fact that manual controls were performed by people of adequate competence and authorization, during the period from 1 August 2021 to 31 July 2022

Copenhagen, 15 November 2022

Paperflow ApS

Mikael Boyum
CEO

Section 3: Independent service auditor's assurance report on the description of controls, their design and functionality

To Paperflow ApS, their customers and their auditors.

Scope

We have been engaged to report on Paperflow ApS' description in Section 1 of its system for delivery of Paperflow ApS' services throughout the period 1 August 2021 to 31 July 2022 (the description) and on the design and operation of controls related to the control objectives stated in the description.

Paperflow ApS is using subservice organisations Microsoft Azure and Google G-Suite. This assurance report is prepared in accordance with the carve-out method and Paperflow ApS' description does not include control objectives and controls within Microsoft Azure and Google G-Suite.

Some of the control objectives stated in Paperflow ApS' description in Section 1 of general IT-controls, can only be achieved if the complementary controls with the customers (or the specific customer) have been appropriately designed and works effectively with the controls with Paperflow ApS. The report does not include the appropriateness of the design and operating effectiveness of these complementary controls.

Paperflow ApS' responsibility

Paperflow ApS is responsible for preparing the description (section 1) and accompanying statement (section 2) including the completeness, accuracy, and method of presentation of the description and statement. Additionally, Paperflow ApS 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 Thorntons 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 Control ¹ and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Grant Thorntons responsibility

Our responsibility is to express an opinion on Paperflow ApS' description (Section 1) 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.

¹ ISQC 1, Quality control for firms that perform audits and reviews of financial statements, and other assurance and related services engagements.

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.

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

Paperflow ApS' description in section 1, 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 Paperflow ApS' statement in Section 2 and based on this, it is our opinion that:

- (a) The description of the controls, as they were designed and implemented throughout the period 1 August 2021 to 31 July 2022, is fair in all material respects.
- (b) The controls related to the control objectives stated in the description were suitably designed throughout the period 1 August 2021 to 31 July 2022, in all material respects.
- (c) The controls tested, which were the controls necessary for providing reasonable assurance that the control objectives in the description were achieved in all material respects, have operated effectively throughout the period 1 August 2021 to 31 July 2022.

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 Paperflow ApS 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, 15 November 2022

Grant Thornton

State Authorised Public Accountants

Jacob Helly Juell-Hansen
State Authorised Public Accountant

Basel Rimon Obari
Executive director, CISA, CISM

Section 4: Control objectives, controls and service auditor testing

4.1. 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 Paperflow ApS' subservice organisations.

Controls, which are specific to the individual customer solutions, or are performed by Paperflow ApS' customers, are not included in this report.

4.2. Tests

We performed our test of controls at Paperflow ApS, by taking the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at Paperflow ApS regarding controls.
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.
Re-performance	Re-performance of controls in order to verify that the control is working as assumed.

4.3. Results of tests

Below, we have listed the tests performed by Grant Thornton as basis for the evaluation of the general IT-controls with Paperflow ApS.

A.5 Information security policies

A.5.1 Management direction for information security

Control objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations

No.	Paperflow ApS' control	Grant Thornton's test	Test results
5.1.1	<p><i>Policies for information security</i></p> <p>A set of policies for information security is defined and approved by management, and then published and communicated to employees and relevant external parties.</p>	<p>We have inspected the information security policy and we have inspected documentation for management approval of the information security policy, as well as communication to employees.</p>	No deviations noted.
5.1.2	<p><i>Review of policies for information security</i></p> <p>The policies for information security are reviewed at planned intervals or if significant changes occur, to ensure their continuing suitability adequacy and effectiveness.</p>	<p>We have inquired about the procedure for periodic review of the information security policy.</p> <p>We have inspected, that the information security policy has been reviewed, based on updated risk assessments, to ensure that it still is suitable, adequate, and effective.</p> <p>We have inquired about evaluation of the risk assessment within the period, and we have inspected that the risk assessment has been reviewed and signed by the management.</p>	No deviations noted.

A.6 Organisation of information security

A.6.1 Internal organisation

Control objective: To establish a management framework to initiate and control the implementation and operation of information security within the organisation

No.	Paperflow ApS' control	Grant Thornton's test	Test results
6.1.1	Information security roles and responsibilities All information security responsibilities are defined and allocated.	We have inspected the organisation chart. We have inspected the guidelines for information security roles and responsibilities.	No deviations noted.
6.1.2	Segregation of duties Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organisations' assets.	We have inspected documentation regarding granting and maintenance of segregation of duties and functions. By inquiries and inspection of system data, we have investigated whether operating staff, only have access to administering rights on systems of which they are responsible, and whether developers have access to the production environment.	No deviations noted.
6.1.4	Contact with special interest groups Appropriate contacts with special interest groups or other specialist security forums and professional associations are maintained.	We have inspected documentation regarding maintenance of rules for appropriate contact with special interest groups, security fora and professional organisations.	No deviations noted.
6.1.5	Information security in project management Information security is addressed in project management, regardless of the type of project.	We have inquired about how information security is used in project management. We have inspected the project model to ensure that information security is being addressed in projects.	No deviations noted.

A.6.2 Mobile devices and teleworking

Control objective: To ensure the security of teleworking and use of mobile devices

No.	Paperflow ApS' control	Grant Thornton's test	Test results
6.2.1	Mobile device policy Policy and supporting security measures are adopted to manage the risk introduced by using mobile devices.	We have inspected policy for securing of mobile devices. We have inspected, that technical controls for securing of mobile devices have been defined.	No deviations noted.
6.2.2	Teleworking. Policy and supporting security measures are implemented to protect information accessed, processed and stores at teleworking sites.	We have inspected policy to secure teleworking, and we have inspected the underlying security measures for protection of remote workspaces with two-factor authentication.	No deviations noted.

A.7 Human ressource security

A.7.1 Prior to employment

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

No.	Paperflow ApS' control	Grant Thornton's test	Test results
7.1.1	Screening Background verification checks on all candidates for employment is being carried out in accordance with relevant laws regulations and ethics and are proportional to the business requirements the classification of the information to be accessed and the perceived risks.	We have inquired into the procedure for employment of new employees and the security measures needed in the process. We have, by sample test, inspected documentation for the acquiring of criminal records for all new employees, in order to determine whether the procedure regarding background check has been followed.	No deviations noted.

No.	Paperflow ApS' control	Grant Thornton's test	Test results
7.1.2	Terms and conditions of employment The contractual agreements with employees and contractors are stating their and the organisation's responsibilities for information security.	We have by sample test, inspected a selection of contracts with employees and consultants in order to determine whether these are signed by the employees and whether responsibilities regarding information security is described.	We have in one (1) out of five (5) sample tests observed, that an employee's contract is not describing responsibilities regarding information security and has no date written for the signature of the contract. No further deviations noted.

A.7.2 During employment

Control objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities

No.	Paperflow ApS' control	Grant Thornton's test	Test results
7.2.1	Management responsibility Management is requiring all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation.	We have inquired about the procedure concerning establishing requirements for employees and partners. We have inspected that management has required that employees observe the IT-security policy.	No deviations noted.
7.2.2	Information security awareness education and training All employees of the organisation and where relevant contractors, are receiving appropriate awareness education and training and regular updates in organisational policies and procedures as relevant for their job function.	We have inquired about procedures to secure adequate training and education (awareness training). We have inspected documentation for activities developing and maintaining security awareness with employees.	No deviations noted.
7.2.3	Disciplinary process There is a formal and communicated disciplinary process in place, to act against employees who have committed an information security breach.	We have inspected sanctioning guidelines and we have inspected that the guidelines have been communicated.	No deviations noted.

A.7.3 Termination and change of employment

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

No.	Paperflow ApS' control	Grant Thornton's test	Test results
7.3.1	<p><i>Termination or change of employment responsibility</i></p> <p>Information security responsibilities and duties that remain valid after termination or change of employment have been defined, communicated to the employee or contractor and enforced.</p>	<p>We have inquired about employees and contractors' obligation to maintain information security in connection with termination of employment.</p> <p>We have, by sample test, inspected documentation that offboarding checklists have been used for terminated employees.</p>	No deviations noted.

A.8 Asset management

A.8.1 Responsibility for assets

Control objective: To identify organisational assets and define appropriate protection responsibilities

No.	Paperflow ApS' control	Grant Thornton's test	Test results
8.1.1	<p><i>Inventory of assets</i></p> <p>Assets associated with information and information processing facilities have been identified and an inventory of these assets has been drawn up and maintained.</p>	We have inspected asset listings for physical assets.	No deviations noted.
8.1.2	<p><i>Ownership of assets</i></p> <p>Assets maintained in the inventory are being owned.</p>	We have inspected record of asset ownership.	No deviations noted.
8.1.3	<p><i>Acceptable use of assets</i></p> <p>Rules for the acceptable use of information and of assets associated with information and information processing facilities are being identified, documented and implemented.</p>	We have inspected employee handbook about guidelines for the use of assets and we have inspected the guidelines.	No deviations noted.

No.	Paperflow ApS' control	Grant Thornton's test	Test results
8.1.4	Return of assets All employees and external party users are returning all the organisational assets in their possession upon termination of their employment contract or agreement.	We have inquired into the procedure for securing the return of assets delivered, and we have inspected the procedure. We have by sample test inspected checklists in regards to offboarding and documentation that access keys have been delivered in the offboarding proces.	No deviations noted.

A.8.2 Classification of information

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

No.	Paperflow ApS' control	Grant Thornton's test	Test results
8.2.1	Classification Information is classified in terms of legal requirements value criticality and sensitivity to unauthorised disclosure or modification.	We have inspected the policy for classification of information. We have inspected that information is classified depending on how sensitive and critical it is.	No deviations noted.
8.2.2	Labelling of information An appropriate set of procedures for information labelling are developed and implemented in accordance with the information classification scheme adopted by the organisation.	We have inquired about the procedures for labelling of data, and we have inspected, that information is labelled in accordance with the classification system.	No deviations noted.
8.2.3	Handling of assets Procedures for handling assets are developed and implemented in accordance with the information classification scheme adopted by the organisation.	We have inspected the procedure for handling of assets and that it has been implemented.	No deviations noted.

A.8.3 Media handling

Control objective: To prevent unauthorised disclosure, modification, removal or destruction of information stored on media

No.	Paperflow ApS' control	Grant Thornton's test	Test results
8.3.1	Management of removable media Procedures have been implemented for the management of removable media in accordance with the classification scheme adopted by the organisation.	We have inquired about managing portable media and we have inspected documentation of the solution.	No deviations noted.
8.3.2	Disposal of media Media are being disposed of securely when no longer required using formal procedures.	We have inspected the procedure for media disposal. We have inquired about whether media have been disposed of during the audit period.	We have been informed that there have been no media disposals during the period, whereby we have not been able to test the effectiveness of the procedure. No deviations noted.

A.9 Access control

A.9.1 Business requirements of access control

Control objective: To limit access to information and information processing facilities

No.	Paperflow ApS' control	Grant Thornton's test	Test results
9.1.1	Access control policy An access control policy has been established, documented and reviewed based on business and information security requirements.	We have inquired into the policy of managing access control in order to establish whether it is updated and approved. We have inspected that the policy for access control is updated, reviewed and approved.	No deviations noted.
9.1.2	Access to network and network services Users are only being provided with access to the network and network services that they have been specifically authorized to use.	We have inquired about managing access to networks and network services, and we have inspected the solution. We have inspected a number of users, in order to establish that they only have access to approved networks and services, based on work-related needs.	No deviations noted.

A.9.2 User access management

Control objective: To ensure authorised user access and to prevent unauthorised access to systems and services.

No.	Paperflow ApS' control	Grant Thornton's test	Test results
9.2.1	User Registration and de-registration A formal user registration and de-registration process has been implemented to enable assignment of access rights.	We have inquired into the procedure for creating and removing users and we have inspected the procedures. We have, by sample test, inspected documentation of removal of users and offboarding procedures.	No deviations noted.
9.2.2	User access provisioning A formal user access provisioning process has been implemented to assign or revoke access rights for all user types to all systems and services	We have inquired into whether a procedure for user administration has been established. We have, by sample test, inspected that the procedure for user administration has been implemented and employees are granted user access based on management's approval.	No deviations noted.
9.2.3	Management of privileged access rights The allocation and use of privileged access rights have been restricted and controlled.	We have inspected policy for managing access related to privileged access rights. We have inquired about documentation regarding the review and control of privileged users in the audit period.	We have observed that a former employee with administrator rights in Azure, in part of the period, has been employed as an external consultant, where it has not been possible to document the monitoring of the consultant's use of his admin account. No further deviations noted.
9.2.4	Management of secret-authentication information of users The allocation of secret authentication information is controlled through a formal management process.	We inspected documentation that a password manager is used to manage user passwords.	No deviations noted.
9.2.5	Review of user access rights Asset owners are reviewing user's access rights at regular intervals	We have inspected documentation of periodic reviews of users every six months.	No deviations noted.

No.	Paperflow ApS' control	Grant Thornton's test	Test results
9.2.6	Removal or adjustment of access rights Access rights of all employees and external party users to information and information processing facilities are being removed upon termination of their employment contract or agreement or adjusted upon change.	We have inquired into procedures about discontinuation and adjustment of access rights. We have, by sample test, inspected terminated employees and we have inspected whether their access rights have been cancelled.	No deviations noted.

A.9.3 User responsibilities

Control objective: To make users accountable for safeguarding their authentication information

No.	Paperflow ApS' control	Grant Thornton's test	Test results
9.3.1	Use of secret authentication information Users are required to follow the organisation's practices in the use of secret authentication information.	We have inspected the guidelines for use of secret authentication information. We have inspected that technical documentation for password requirements is fulfilled.	No deviations noted.

A.9.4 System and application access control

Control objective: To prevent unauthorised access to systems and applications

No.	Paperflow ApS' control	Grant Thornton's test	Test results
9.4.1	Information access restriction Access to information and application system functions has been restricted in accordance with the access control policy.	We have inquired into guidelines and procedures for securing access restriction to application system functions. We have inspected the access matrix, to determine that limited access is given to employees using application systems.	No deviations noted.
9.4.2	Secure log-on procedures Access to systems and applications is controlled by procedure for secure logon.	We have inspected the policy for access management. We have inspected the procedure for secure log-on and have inspected the implementation of secure log-on through two-factor-authentication.	No deviations noted.

No.	Paperflow ApS' control	Grant Thornton's test	Test results
9.4.3	<i>Password management system</i> Password management systems are interactive and have ensured quality passwords.	We have inspected that systems for administration of access codes are configured in accordance with the requirements.	No deviations noted.
9.4.5	<i>Access control to program source code</i> Access to program source code has been re-restricted.	We have inspected documentation for users with access to the source code. We have inspected documentation that access to program source code is being logged.	No deviations noted.

A.10 Cryptography

A.10.1 Cryptographic controls

Control objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information

No.	Paperflow ApS' control	Grant Thornton's test	Test results
10.1.1	<i>Policy on the use of cryptographic controls</i> A policy for the use of cryptographic controls for protection of information has been developed and implemented.	We have inspected the policy for cryptographic controls.	No deviations noted.
10.1.2	<i>Key Management</i> A policy on the use protection and lifetime of cryptographic keys has been developed and implemented through their whole lifecycle.	We have inquired into the policies for administering cryptographic keys, which supports the company use of cryptographic techniques. We have inspected a sample of documentation, in order to establish whether the techniques are used as described.	No deviations noted.

A.11 Physical and environmental security

A.11.1 Secure areas

Control objective: To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities

No.	Paperflow ApS' control	Grant Thornton's test	Test results
11.1.1	Physical security perimeter Security perimeters have been defined and used to protect areas that contain either sensitive or critical information and information.	We have inquired into the procedure for physical security of facilities and security perimeters. We have inquired into relevant locations and their security perimeter, in order to establish whether security measures have been implemented to prevent unauthorized access. We have observed the physical conditions.	No deviations noted.
11.1.2	Physical entry control Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	We have inquired into the procedures for access control to secure areas. We have observed that the physical conditions are secure.	No deviations noted.
11.1.3	Securing offices, rooms, and facilities Physical security for offices rooms and facilities has been designed and applied.	We have observed the physical conditions and observed that measures have been taken to secure offices, premises, and facilities.	No deviations noted.

A.11.2 Equipment

Control objective: To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations

No.	Paperflow ApS' control	Grant Thornton's test	Test results
11.2.8	<i>Unattended user equipment</i> Users are ensuring that unattended equipment has appropriate protection.	We have inspected the procedure for protection of unattended user equipment. We have inspected the policy for screensavers and observed that it has been implemented.	No deviations noted.
11.2.9	<i>Clean desk and clear screen policy.</i> A clean desk policy for papers and removable storage media and a clear screen policy for information processing facilities has been adopted.	We have inquired into the policy of tidy desk and clear screen. We have observed that the policy is implemented on the premises.	No deviations noted.

A.12 Operations security

A.12.1 Operational procedures and responsibilities

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

No.	Paperflow ApS' control	Grant Thornton's test	Test results
12.1.1	<i>Documented operating procedures.</i> Operating procedures have been documented and made available to all users.	We have inquired about requirements for documentation and maintenance of operating procedures. We have inspected that documentation for operating procedures is accessible to relevant employees through the IT-handbook.	No deviations noted.

No.	Paperflow ApS' control	Grant Thornton's test	Test results
12.1.2	Change management Changes to the organisation business processes information processing facilities and systems that affect information security have been controlled.	We have inquired about the procedure regarding changes of information handling equipment and -systems. We have inquired into whether a selection of changes, made on platforms, databases and network equipment have been approved, tested, documented, and implemented in the production environment, according to the change management procedure. We have, by sample test, inspected that the procedure for change management is implemented.	No deviations noted.
12.1.3	Capacity management The use of resources is monitored and adjusted, and future capacity requirements are projected to ensure that the required system performance is obtained.	We have inquired into the procedure for monitoring use of resources and adjustments of capacity, to meet future capacity requirements. We have inspected that relevant platforms are included in the capacity requirement procedure and that alarms are implemented.	No deviations noted.
12.1.4	Separation of development-, test- and operations facilities. Development testing and operational environments are separated to reduce the risks of unauthorized access or changes to the operational environment.	We have inquired into securing the separation of development-, test- and operations facilities. We have, by sample test, inspected that development, test and production are either physically or logically separated.	No deviations noted.

A 12.2 Protection from malware

Control objective: To ensure that information and information processing facilities are protected against malware

No.	Paperflow ApS' control	Grant Thornton's test	Test results
12.2.1	Control against malware Detection prevention and recovery controls to protect against malware have been implemented combined with appropriate user awareness.	We have inquired into measures against malware. We have inquired about the use of antivirus software and we have inspected documentation for its use.	No deviations noted.

A.12.3 Backup

Control objective: To protect against loss of data

No.	Paperflow ApS' control	Grant Thornton's test	Test results
12.3.1	<p><i>Information backup</i></p> <p>Backup copies of information software and system images are taken and tested regularly in accordance with an agreed backup policy.</p>	<p>We have inquired into configuration of backup and we have inspected samples of documentation for the setup according to requirements.</p> <p>We have inspected that backup is being monitored.</p> <p>We have inquired about testing of backupfile recovery and we have inspected documentation for recovery test.</p>	No deviations noted.

A.12.4 Logging and monitoring

Control objective: To record events and generate evidence

No.	Paperflow ApS' control	Grant Thornton's test	Test results
12.4.1	<p><i>Event logging</i></p> <p>Event logs recording user activities exceptions faults and information security events shall be produced, kept and regularly reviewed.</p>	<p>We have inquired into user activity logging.</p> <p>We have inspected samples of logging configurations.</p>	No deviations noted.
12.4.2	<p><i>Protection of log information</i></p> <p>Logging facilities and log information are being protected against tampering and unauthorized access.</p>	<p>We have inquired about secure log information and we have inspected the solution.</p> <p>We have, by physical inspection, inspected a selection of logging configurations in order to establish whether login information is protected against manipulation and unauthorized access.</p>	No deviations noted.

No.	Paperflow ApS' control	Grant Thornton's test	Test results
12.4.3	Administrator and operator logs System administrator and system operator activities have been logged and the logs are protected and regularly reviewed.	We have inquired into procedures regarding logging of activities performed by system administrators and operators. We have inspected logon setups on chosen servers and database systems, in order to establish whether the actions of system administrators and operators are logged.	No deviations noted.
12.4.4	Clock synchronization The clocks of all relevant information processing systems within an organisation or security domain have been synchronised to a single reference time source.	We have inquired into procedures for synchronization against a reassuring time server and we have inspected the solution.	No deviations noted.

A.12.5 Control of operational software

Control objective: To ensure the integrity of operational systems

No.	Paperflow ApS' control	Grant Thornton's test	Test results
12.5.1	Installation of software on operational systems Procedures are implemented to control the installation of software on operational systems.	We have inquired about software installation guidelines on operating systems and we have, by sample test, inspected that the guidelines are being followed.	No deviations noted.

A.12.6 Technical vulnerability management
Control objective: To prevent exploitation of technical vulnerabilities

No.	Paperflow ApS' control	Grant Thornton's test	Test results
12.6.1	Management of technical vulnerabilities Information about technical vulnerabilities of information systems being used is obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	We have inquired into the procedure regarding gathering and evaluation of technical vulnerabilities and we have inspected documentation that the procedure has been followed.	No deviations noted.
12.6.2	Restriction on software installation Rules governing the installation of software by users have been established and implemented.	We have inquired into restriction of user executed software installations. We have inspected, that regulations for software installations are being followed.	No deviations noted.

A.13 Communications security

A.13.1 Network security management
Control objective: To ensure the protection of information in networks and its supporting information processing facilities

No.	Paperflow ApS' control	Grant Thornton's test	Test results
13.1.1	Network controls Networks are managed and controlled to protect information in systems and applications.	We have inquired into whether requirements for operating and control of network, including requirements and regulations about encryption, segmentation, firewalls, intrusion detection and other relevant security measures have been defined. We have inspected documentation for network design and a range of security setups of network components, in order to establish whether the defined rules and regulations have been implemented.	No deviations noted.

No.	Paperflow ApS' control	Grant Thornton's test	Test results
13.1.2	Security of network services Security mechanisms service levels and management requirements of all network services are identified and included in network services agreements whether these services are provided in-house or outsourced.	We have observed that written requirements about security mechanisms, service levels and management requirements of all network services are present. We have inspected a range of network components in order to estimate whether the components have been set up according to requirements and contractor's recommended baselines.	No deviations noted.
13.1.3	Segregation of networks Groups of information services users and information systems are segregated on networks.	We have inquired into the guidelines for segregation of networks. We have inspected a range of accesses made between network zones to establish whether they are limited to essential services.	No deviations noted.

A.14 Aquisition, development and maintenance of systems

A.14.1 Security requirements of information systems

Control objective: To ensure that information security is an integrated part of information systems through the entire lifecycle. This also includes requirements of information systems, rendering services on public networks

No.	Paperflow ApS' control	Grant Thornton's test	Test results
14.1.1	Information security requirements analysis and specification The information security related requirements are being included in the requirements for new information systems or enhancements to existing information systems.	We have inspected the IT-handbook for analysis and specification of information security requirements. We have inspected a selection of change requests to determine whether requirements of security and controls in new information systems or in connection with existing systems have been described.	No deviations noted.

A.14.2 Security, development- and supporting processes

Control objective: To ensure that information security is planned and implemented with the development life cycle

No.	Paperflow ApS' control	Grant Thornton's test	Test results
14.2.1	<p><i>Secure development policy</i></p> <p>Rules for the development of software and systems have been established and applied to developments within the organisation.</p>	<p>We have inspected the rules for developing software and systems.</p> <p>We have inspected that the rules have been followed.</p>	No deviations noted.
14.2.2	<p><i>Change control procedures</i></p> <p>Changes to systems within the development lifecycle are being controlled using formal change control procedures.</p>	<p>We have inquired about the change management procedure, to establish whether the procedure controls the development lifecycle.</p> <p>We have inspected a range of changes, to establish whether the requirements to change management were followed.</p>	No deviations noted.
14.2.3	<p><i>Technical review of applications after operating system changes</i></p> <p>When operating platforms are changed business critical applications are reviewed and tested to ensure there is no adverse impact on organisational operations or security.</p>	<p>We have inquired into the procedure for technical review of applications after operating system changes.</p> <p>We have, by sample test, inspected that changes in operating systems and infrastructure have been evaluated regarding potential consequences to application systems, before being completed.</p>	No deviations noted.
14.2.5	<p><i>Secure system engineering process</i></p> <p>Principles for engineering secure systems have been established, documented, maintained and applied to any information system implementation efforts.</p>	<p>We have inquired about the procedure for system development.</p> <p>We have inspected that the procedure, stated in the IT-handbook, has been followed.</p>	No deviations noted.
14.2.6	<p><i>Secure development environment</i></p> <p>There is established appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.</p>	<p>We have inquired about establishing a secure development environment.</p> <p>We have inspected, that secure development environments have been implemented.</p>	No deviations noted.

A.14.3 Test Data

Control objective: To ensure the protection of data used for testing.

No.	Paperflow ApS' control	Grant Thornton's test	Test results
14.3.1	Protection of test data Test data are being carefully selected, protected, managed and controlled.	We have inquired the procedure regarding selection and protection of test data. We have, by sample test, inspected that test data is secured and managed in the Kubernetes environment.	No deviations noted.

A.15 Supplier relationships

15.2 Supplier service delivery management

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

No.	Paperflow ApS' control	Grant Thornton's test	Test results
15.2.1	Monitoring and review of third-party services Organisations are regularly monitoring review and audit supplier service delivery.	We have inquired if the procedure for monitoring and review of services from subcontractors is according to the contract. We have been informed, that yearly trips to the Bulgarian department have been made. We have inspected that review and evaluation of relevant audit reports about subcontractors, have been performed.	No deviations noted.
15.2.2	Manage changes to the third-party services Changes in supplier services, including maintenance and improvement of existing information security policies, procedures and controls, are managed under consideration of how critical the business information, systems and processes involved are, and are used for revaluation of risks involved.	We have inquired about change management with the subcontractor, and we have inspected the documentation for this.	No deviations noted.

A.16 Information security incident management

A.16.1 Management of information security incidents and improvements

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

No.	Paperflow ApS' control	Grant Thornton's test	Test results
16.1.1	Responsibilities and procedures Management responsibilities and procedures are established to ensure a quick effective and orderly response to information security incidents.	We have inquired about the responsibilities and procedures of information security incidents, and we have inspected documentation for the distribution of responsibilities. Further, we have inspected the procedure for handling information security incidents.	No deviations noted.
16.1.2	Reporting information security events Information security events are being reported through appropriate management channels as quickly as possible.	We have inquired into guidelines for reporting information security incidents and weaknesses, and we have inspected the guidelines.	We have been informed, that there have been no information security incidents during the audit period, wherefore we have not been able to test the effectiveness of the control. No deviations noted.
16.1.3	Reporting security weaknesses Employees and contractors using the organisation's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services.	We have inquired about information security events during the audit period. We have inspected the procedure for reporting and notification of security breaches.	No deviations noted.
16.1.4	Assessment of and decision on information security events Information security events are assessed, and it is decided if they are to be classified as information security incidents.	We have inquired into the procedure for assessment, response and evaluation of information security breaches. We have inspected the procedure for handling security incidents.	No deviations noted.

No.	Paperflow ApS' control	Grant Thornton's test	Test results
16.1.5	<i>Response to information security incidents</i> Information security incidents are responded to in accordance with the documented procedures.	We have, by sample test, inspected that information security incidents have been responded to, in accordance with the documented procedures.	No deviations noted.
16.1.6	<i>Learning from information security incidents</i> Knowledge gained from analysing and resolving information security incidents is used to reduce the likelihood or impact of future incidents.	We have inspected documentation for the Problem Management function, which analyses information security incidents in order to reduce probability of recurrence.	No deviations noted.

A.17 Information security aspects of business continuity management

A.17.1 Information security continuity

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

No.	Paperflow ApS' control	Grant Thornton's test	Test results
17.1.1	<i>Planning information security continuity</i> Requirements for information security and the continuity of information security management in adverse situations e.g., during a crisis or disaster has been decided upon.	We have inquired about the preparation of a contingency plan to ensure the continuity of operations in the event of crashes and the like, and we have inspected the plan.	No deviations noted.
17.1.2	<i>Implementing information security continuity</i> Processes procedures and controls to ensure the required level of continuity for information security during an adverse situation are established, documented, implemented and maintained.	We have inquired about procedures to ensure that efforts regarding maintaining information security is described in the contingency plan, and we have inspected that the contingency plan is updated and properly maintained.	No deviations noted.

No.	Paperflow ApS' control	Grant Thornton's test	Test results
17.1.3	<p><i>Verify review and evaluate information security continuity</i></p> <p>The established and implemented information security continuity controls are verified on a regular basis to ensure that they are valid and effective during adverse situations.</p>	We have inquired about test of the contingency plan, and we have inspected documentation of tests performed.	No deviations noted.

A.17.2 Redundancies

Control objective: To ensure availability of information processing facilities

No.	Paperflow ApS' control	Grant Thornton's test	Test results
17.2.1	<p><i>Availability of information security processing facilities</i></p> <p>Information processing facilities have been implemented with redundancy sufficient to meet availability requirements.</p>	We have inquired about the availability of operating systems and we have inspected the established measures.	No deviations noted.

A.18 Compliance

A.18.2 Information security reviews

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

No.	Paperflow ApS' control	Grant Thornton's test	Test results
18.2.1	<p><i>Independent review of information security</i></p> <p>Processes and procedures for information security) (control objectives, controls, policies, processes and procedures for information security) are reviewed independently at planned intervals or when significant changes occur.</p>	We have observed, that independent evaluation of information security has been established.	No deviations noted.

No.	Paperflow ApS' control	Grant Thornton's test	Test results
18.2.2	<p><i>Compliance with security policies and standards</i></p> <p>Managers are regularly reviewing the compliance of information processing and procedures within their area of responsibility with the appropriate security policies standards and any other security requirements.</p>	<p>We have inquired into management's procedures for compliance with security policies and security standards.</p> <p>We have inspected the annual wheel, which shows the implementation of regular controls regarding review and updates for the security requirements in policies and procedures.</p>	<p>No deviations noted.</p>
18.2.3	<p><i>Technical compliance review</i></p> <p>Information systems are regularly being reviewed for compliance with the organisation' information security policies and standards.</p>	<p>We have inquired about projects with focus on hardening systems in the audit period.</p>	<p>We have observed that no efforts have been made regarding systems hardening in Paperflow ApS, during the audit period.</p> <p>No further deviations noted.</p>

PENNEO

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

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

Mikael Boyum

Underskriver 1

Serienummer: 48fc2f3d-3ec7-4b0c-b33a-c4bfde48b6b6

IP: 213.83.xxx.xxx

2022-11-23 15:27:31 UTC



Basel Obari

Underskriver 2

Serienummer: CVR:34209936-RID:99589866

IP: 188.179.xxx.xxx

2022-11-23 15:29:55 UTC



Jacob Helly Juell-Hansen

Underskriver 3

Serienummer: CVR:34209936-RID:50904197

IP: 62.243.xxx.xxx

2022-11-23 21:15:00 UTC



Dette dokument er underskrevet digitalt via **Penneo.com**. Signeringsbeviserne i dokumentet er sikret og valideret ved anvendelse af den matematiske hashværdi af det originale dokument. Dokumentet er låst for ændringer og tidsstempelt med et certifikat fra en betroet tredjepart. Alle kryptografiske signeringsbeviser er indlejret i denne PDF, i tilfælde af de skal anvendes til validering i fremtiden.

Sådan kan du sikre, at dokumentet er originalt

Dette dokument er beskyttet med et Adobe CDS certifikat. Når du åbner dokumentet

i Adobe Reader, kan du se, at dokumentet er certificeret af **Penneo e-signature service** <penneo@penneo.com>. Dette er din garanti for, at indholdet af dokumentet er uændret.

Du har mulighed for at efterprøve de kryptografiske signeringsbeviser indlejret i dokumentet ved at anvende Penneos validator på følgende websted: <https://penneo.com/validate>