

NOVEMBER 2023

CYBERPILOT APS

ISAE 3402 TYPE 2 ASSURANCE REPORT

CVR 37435392

Independent auditor's report on the control environment related to the IT operation of SaaS solutions.

In addition, a paragraph has been added to the description about the role as data processor in accordance with the General Data Protection Regulation.

Beierholm
State Authorized Public Accountants
Knud Højgaards Vej 9
DK-2860 Søborg
Denmark
CVR no. DK 32 89 54 68
Tlf +45 39 16 76 00

www.beierholm.dk



Structure of the Assurance Report

Chapter 1:

Letter of Representation.

Chapter 2:

Description of the control environment related to the IT operation of SaaS solutions.

Chapter 3:

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

Chapter 4:

Auditor's description of control objectives, security measures, tests and findings.

CHAPTER 1:

Letter of Representation

CyberPilot ApS processes personal data on behalf of Data Controllers according to Data Processor Agreements regarding IT operation of SaaS solutions.

The accompanying description has been prepared for the use of customers and their auditors, who have used CyberPilot ApS' SaaS solutions, and who have sufficient understanding to consider the description along with other information, including information about controls operated by the customers i.e. the Data Controllers themselves, when assessing, whether the demands to the control environment as well as requirements laid down in the General Data Protection Regulation are complied with.

CyberPilot ApS hereby confirms that

- (A) The accompanying description, Chapter 2 gives a true and fair description of CyberPilot ApS' control environment in relation to operations of SaaS solutions throughout the period 1 November 2022 - 31 October 2023. The criteria for this assertion are that the following description:
- (i) Gives an account of how the controls were designed and implemented, including:
 - The types of services delivered, including the type of personal data processed
 - The processes in both IT and manual systems that are used to initiate, record, process and, if necessary, correct, erase and limit the processing of personal data
 - The processes utilized to secure that the performed data processing was conducted according to contract, directions or agreements with the customer i.e. the Data Controller
 - The processes securing that the persons authorized to process personal data have pledged themselves to secrecy or are subject to relevant statutory confidentiality
 - The processes securing that - at the Data Controller's discretion - all personal data is erased or returned to the Data Controller, when the data processing is finished, unless personal data must be stored according to law or regulation
 - The processes supporting the Data Controller's ability to report to the Supervisory Authority as well as inform the Data Subjects in the event of personal data security breaches
 - The processes ensuring appropriate technical and organizational security measures for processing personal data taking into consideration the risks connected to processing, in particular accidental or illegal actions causing destruction, loss, change, unauthorized forwarding of or access to personal data that is transmitted, stored or in other ways processed
 - Control procedures, which we assume - with reference to the limitations of SaaS solutions - have been implemented by the Data Controllers and which, if necessary to fulfil the control objectives mentioned in the description, have been identified in the description
 - Other aspects of our control environment, risk assessment process, information system (including the accompanying work routines) and communication, control activities and monitoring controls relevant for processing of personal data
 - (ii) Includes relevant information about changes in SaaS solutions' processing of personal data performed throughout the period 1 November 2022 - 31 October 2023
 - (iii) Does not omit or misrepresent information relevant for the scope of the controls described, taking into consideration that the description has been prepared to meet the common needs of a broad range of customers and their auditors, and may not, therefore, include every aspect of the control 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 operated effectively throughout the period 1 November 2022 - 31 October 2023. The criteria for this assertion are that:
- (i) The risks threatening the fulfilment of the control objectives mentioned in the description were identified
 - (ii) The identified controls would, if used as described, provide reasonable assurance that the risks in question would not prevent the fulfilment of the said control objectives, and
 - (iii) The controls were applied consistently as designed, including that manual controls were performed by persons with adequate competences and authority throughout the period 1 November 2022 - 31 October 2023.
- (C) Appropriate technical and organizational security measures are established in order to honour the agreements with the Data Controllers, compliance with generally accepted data processor standards and relevant demands to Data Processors according to the General Data Processing Regulation.
- (D) The accompanying description and the related criteria for fulfilling the control objectives and controls, Chapter 2, have been prepared based on compliance with CyberPilot ApS' standard agreement as well as related Data Processor Agreement. The criteria for this basis are:
- (i) CyberPilot Information Security Statement V.1
 - (ii) CyberPilot Information Security Manual V.1.2
 - (iii) Data Processor Agreement (appendix to terms and conditions of the agreement)

Aarhus, 22 November 2023



Rasmus Hangaard Vinge, CEO

CyberPilot ApS, Mejlgade 39, 1. Floor, DK-8000 Aarhus C, CVR 37435392

Description of the control environment in connection with IT operation of SaaS solutions

Scope of this description

The purpose of the present description is to inform CyberPilot ApS' customers and their auditors of the requirements of ISAE 3402, which is the international standard for Assurance Reports on Controls at a Service Organisation.

The scope of this description includes the technical and organizational security measures implemented in connection with the operation of the following security services managed by CyberPilot ApS:

- Awareness training
- Phishing training

The services are supplied as "Software as a Service" (SaaS) solutions.

As a supplement to the description is added an independent paragraph (Compliance with the role as data processor), including a description of essential requirements in connection with the role as data processor combined with general requirements from data processor agreements.

Description of CyberPilot ApS

CyberPilot is an information security company that offers, develops, operates and markets managed cyber security and compliance services to companies and organizations. The services are offered as Software-as-a-Service solutions to our clients. We both develop our own applications and supported by third party applications to deliver high quality and value-creating services to our customers.

The services include:

- **Awareness training** – e-learning courses on information security and GDPR-compliance delivered through the CyberPilot e-learning platform
- **Phishing training** – phishing-simulations including access to web-plugin with all relevant data about the phishing-campaigns

The core activity in CyberPilot is the development and operation of these CyberPilot services.

CyberPilot operates 24/7/365 in hosted IT environments provided by suppliers.

CyberPilot Information security

CyberPilot follows the principles of ISO27001+2. Processes and working methods based on ISO27001+2 are in place to ensure high standards regarding confidentiality, integrity and availability of the product and services provided to customers and partners.

IT security statement and strategy

CyberPilot's overall framework and strategic objectives related to information security is defined in CyberPilot's information security statement. This statement is drawn up by the board and is reviewed annually.

By following the information security statement put forward by the board, the management prioritizes information security as an important part of the company's business culture.

The overall objectives for CyberPilot's information security are:

- CyberPilot works with information security to secure confidentiality, integrity and availability of CyberPilot's assets, systems and data.
- CyberPilot must comply with ISO 27001+2:2017. This will be documented through an ISAE 3402 report.
- A risk-based approach must be applied to identify and manage the relevant risks related to CyberPilot information security. CyberPilot must therefore implement a continuous process of risk assessment.
- An information security manual must be developed and continuously reviewed and updated. The information security manual should include descriptions of the measures implemented to manage the information security of CyberPilot and should include references to further relevant policies, working procedures and work instructions related to the information security of CyberPilot.
- The information security statement and the objectives will be reviewed on an annual basis.

Organization of information security

The steering managing and prioritization of CyberPilot's activities related to information security is carried out by the person responsible for information security – Rasmus Hangaard Vinge, CEO of CyberPilot.

The CEO of CyberPilot has the day-to-day responsibility for IT security, and it is thus ensured that the overall requirements and framework for IT security are maintained.

Other employees will be involved in the activities when considered necessary.

The rules for the employees regarding CyberPilot's usage of IT is defined in specific guidelines. All employees are subject to these rules, which cover:

- Confidentiality
- Access codes
- Etc.

Human Resource Security

CyberPilot acknowledges the fact that its employees play an important role in the information security of the company. CyberPilot has therefore implemented measures to ensure processes concerning information security prior to, during and after employment. The CEO and direct line managers have specified responsibilities to perform the relevant tasks set out in the specific guidelines.

All individuals employed by CyberPilot are subject to screening prior to employment.

Employees are furthermore contractually informed and obligated to follow the rules and guidelines set out by the management of CyberPilot regarding information security.

During the employment at CyberPilot, individual employees are obligated to participate in the information security awareness training program.

And in the case of termination of employment, CyberPilot has a defined procedure to ensure that the relevant IT equipment is returned, and user access rights are revoked or in other ways handled.

Asset Management

CyberPilot has limited ownership of physical assets. Trusted suppliers primarily deliver operating servers and IT infrastructure. CyberPilot has an interest in ensuring that all assets are securely operated. CyberPilot has therefore assigned ownership of each of assets to specific employees within CyberPilot.

Ownership of an assets means that the specified employee has the responsibility of ensuring that the asset is implemented and operated with respect to the overall objectives for the information security of CyberPilot.

Ownership of asset can be delegated from the management to relevant employees. Ownership of hardware and software assets is documented, reviewed, and adjusted as part of the yearly risk assessment process.

Access Control

Physical and logical access control is of priority in CyberPilot. There is a clear motivation to control access to CyberPilot's assets and limit it to the people, who have a clear need-to-know and carry out tasks related to the access given.

CyberPilot's overall guidelines to controlling the access to assets are documented in the access control policy.

Access control is focused around 1) access to the CyberPilot IT infrastructure and 2) access within the CyberPilot services:

- 1) IT infrastructure: CyberPilot is dependent on suppliers for the IT infrastructure and sets demands for the suppliers about access management and user rights.
- 2) Within CyberPilot services: For all services, a logical layered access control scheme is implemented, which ensures that the relevant user categories (both internal and external) have the appropriate access to the CyberPilot system and underlying data.

Physical and environmental security

CyberPilot's offices are located in Aarhus, Denmark.

The IT infrastructure (servers) from where the CyberPilot services is operated is physically located in data centers operated by selected suppliers. CyberPilot has entered into an agreement with these suppliers, who are responsible for the physical security of the servers.

Employees are instructed to follow guidelines related to the daily work routines.

Operation Security

CyberPilot has implemented security measures, which require operational attention. The daily task of operation is shared between tasks handled by CyberPilot and tasks handled by external suppliers.

See below for a description of the operational measures:

Firewall

All traffic to the CyberPilot servers is routed through firewalls.

Backup

To prevent data loss, CyberPilot has implemented backup procedures for the individual services.

The backup is also tested continuously to make sure that restore is possible if needed.

Patch management procedures

CyberPilot has defined clear processes for patch management to ensure that applications and systems are continuously kept up to date which significantly decreases the risk of vulnerabilities on the systems.

Monitoring

The CyberPilot servers are monitored to ensure continuous and stable operation.

The monitoring combined with alerts ensures that any disruption of the operation of the servers can be quickly identified and handled.

Technical vulnerability management

To identify technical vulnerabilities in the CyberPilot IT infrastructure, continuous testing is performed. This ensures that any new vulnerabilities, misconfigurations etc. are identified and managed accordingly.

Description of development, test and production environment

CyberPilot has separate environments for the development, test and production. The purpose of the separated development, test and production environments is to ensure a continuous development of the applications while making sure that only changes which have been appropriately tested are launched into the production environment.

Network security management

CyberPilot uses primarily two networks, one for workstations and a separate network of Cloud IAAS.

CyberPilot's use of the CP network is limited to workstations and shared office resources. The employees' use of the network is regulated in the IT-usage guidelines.

The cloud IAAS-network is operated by AWS and is strictly used for operation of the CyberPilot servers. This means that there are several security measures implemented on the network.

System acquisition, development, and maintenance

There is a strong focus on securing that the development of the services meets the requirements of CyberPilot's customers and partners.

CyberPilot has established separate environments for the development, test and production of the services.

The overall goal is to ensure that updates and new developments meet high standards by following development, testing and approving processes before release and at the same time maintain a flexible approach, which enables CyberPilot to constantly develop the services.

Supplier relationships

CyberPilot is dependent on a few key suppliers in our daily operation and development of the CyberPilot services.

All supplier relationships are governed through formal contracts.

Risks and relevant security controls related to specific assets/suppliers are (as a minimum) discussed as part of the yearly risk assessment. To ensure that information security is evaluated and prioritized before entering into agreements with new suppliers, CyberPilot has defined specific policies for selection of suppliers. Agreements with key suppliers are reviewed annually.

Information security incident management

At CyberPilot we have prepared ourselves for security incidents by delegating the responsibility of the management of security incidents to the various organisational levels.

Furthermore, all employees are instructed to report any security incidents to ensure that all incidents are handled quickly and effectively.

All security incidents are logged to ensure that incidents are categorized, handled appropriately and closed when dealt with. The purpose of this is also to ensure that new controls are implemented, and that the organisation can 'learn' from past incidents and avoid similar incidents in the future.

Information security aspects of business continuity management

CyberPilot has taken relevant measures to ensure business continuity. Plans define the actions needed to be taken in the case of security incidents that are affecting the CP-services. The main priority is to re-establish service of the production environments.

Measures have been implemented to ensure that the production environment is protected, that relevant redundancies are in place and that service can be restored in cases of hardware and/or software failures.

Important changes in relation to IT security

During the period covered by the report, there have been no significant changes in relation to IT security.

Compliance with the role as Data Processor CyberPilot works with the legal advisors to ensure that the company is constantly aware of laws and regulations that can affect the operation of the company. The main areas for CyberPilot regarding compliance are:

- Contracts with partners and end-users
- Personal data protection legislation i.e. GDPR

The identification of compliance risk is included in the overall risk assessment process of CyberPilot.

CyberPilot ensures that all legal contracts with partners and customers are developed in close collaboration with our legal advisors.

CyberPilot also works to ensure that requirements in contracts i.e. obligations to perform independent reviews on CyberPilot's information security are met.

Furthermore, CyberPilot is continuously working to ensure that CyberPilot services follow the relevant regulations regarding standards and personal data protection.

In relation to GDPR, CyberPilot is working to secure full compliance and responsible handling of personal data. Examples of processes and procedures in place:

- Periodic supervision/ monitoring of business-critical subcontractors
- Records of processing operations
- Ensuring proper processing in relation to transfer to third countries, including decision and risk assessment about the use of cloud service (see, the Schrems II verdict)
- Ongoing scrutiny and assessment of existing procedures and documentation

CHAPTER 3:

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

For the customers / users of CyberPilot ApS' SaaS solutions and their auditors

Scope

We have been engaged to report on CyberPilot ApS' description in Chapter 2, which is a description of the information security and data protection related to the IT operation of SaaS solutions, see Data Processor Agreements with customers, throughout the period 1 November 2022 - 31 October 2023, as well as on the design and function of controls regarding the control objectives stated in the description.

We express our opinion with reasonable assurance.

The report is based on a partial approach, which means this report does not include the IT security controls and control objectives related to use of external business partners. The report does not include control or supervision with subcontractors in relation to SaaS solutions. These subcontractors are listed in detail in Data Processor Agreements with the customers.

The scope of our report does not cover customer-specific conditions, and the report does not include the complementary controls and control activities conducted by the user company.

CyberPilot ApS' responsibility

CyberPilot ApS is responsible for the preparation of the Description and Letter of Representation in Chapter 1 and 2, including the completeness, accuracy, and method of presentation of the description and assertion; for providing the services covered by the description; for stating the control objectives; and for designing, implementing and effectively operating controls to achieve the stated control objectives.

Beierholm's independence and quality management

We have complied with the requirements of independence and other ethical requirements laid down in FSR's Ethical Rules based on fundamental principles of integrity, objectivity, professional competence and requisite care, confidentiality, and professional conduct.

We apply ISQM 1 and thus sustain a comprehensive system of quality management, including documented policies and procedures for compliance with ethical rules, professional standards as well as requirements in force under existing laws and additional regulation.

Auditor's responsibility

Our responsibility is to express an opinion, based on our procedures, on CyberPilot ApS' description and on the design and operation of controls related to the control objectives stated in the said description. We have conducted our engagement in accordance with ISAE 3402, Assurance Reports on Controls at a Service Organisation, issued by the IAASB. The standard requires that we comply with ethical requirements and that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and whether the controls in all material aspects are appropriately designed and operate 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 about the design and operating effectiveness of controls. The procedures selected depend on the judgement of the service organisation's auditor, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or not operating effectively.

Our procedures included testing the operating effectiveness of such controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description have been 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 and described by CyberPilot ApS in Chapter 2.

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

Limitations of controls at CyberPilot ApS

CyberPilot ApS' 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. Moreover, because of their nature, controls at CyberPilot ApS may not prevent or detect all errors or omissions in processing or reporting transactions. Furthermore, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at the service organisation may become inadequate or fail.

Opinion

Our opinion is based on the matters outlined in this report. The criteria on which our opinion is based are those described in Chapter 1 under Letter of Representation. In our opinion,

- a) The description fairly presents the control environment in connection with IT operation of SaaS solutions, such as this control environment was designed and implemented throughout the period 1 November 2022 - 31 October 2023 in all material respects; and
- b) The controls related to the control objectives stated in the description were in all material respects suitably designed throughout the period 1 November 2022 - 31 October 2023; and
- c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved in all material respects, had operated effectively throughout the period 1 November 2022 - 31 October 2023.

Description of tests of controls

The specific controls tested and the nature, timing and findings of those tests are listed in Chapter 4.

Intended users and purpose

This report and the description of the test of controls in Chapter 4 are solely intended for CyberPilot ApS' customers and their auditors, who have sufficient understanding to consider them along with other information, including information about the customers' own control measures, which the customers i.e. the Data Controllers themselves have performed, when assessing compliance with the demands to the control environment as well as with the requirements of the General Data Protection Regulation.

Søborg, 23 November 2023

Beierholm

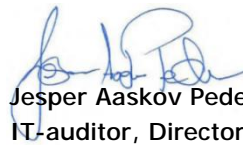
State-Authorized Public Accountants

CVR-no 32 89 54 68



Kim Larsen

State-authorized Public Accountant



Jesper Aaskov Pedersen

IT-auditor, Director

CHAPTER 4:

Auditor's description of control objectives, security measures, tests, and findings

We have structured our engagement in accordance with ISAE 3402 – Assurance Reports on Controls at a Service Organisation. For each control objective, we start with a brief summary of the control objective as described in the frame of reference ISO27001+2:2017.

With respect to the period, we have tested whether CyberPilot ApS has complied with the control objectives throughout the period 1 November 2022 - 31 October 2023.

Below the grey field are three columns:

- The first column tells the activities CyberPilot ApS, according to its documentation, has put into practice in order to comply with the requirements.
- The second column tells how we have decided to test, whether facts tally with descriptions.
- The third column tells the findings of our test.

The Tests Performed

The tests performed in connection with establishing the control measures' design, implementation and operational efficiency are conducted using the methods described below:

Inspection	Reading of documents and reports containing information about execution of the control. This includes, inter alia, reading and deciding about reports and other documentation in order to assess, whether it can be expected that the design of specific control measures will be efficient, if implemented. Furthermore, it is assessed whether control measures are monitored and controlled sufficiently and with appropriate intervals.
Enquiries	Enquiries to/interview with relevant staff at CyberPilot ApS. Enquiries have included how control measures are performed.
Observation	We have observed the performance of the control.
Repeating the control	Repeated the relevant control measure. We have repeated the performance of the control in order to verify that the control measure works as assumed.

CONTROL OBJECTIVE - INTRODUCTION:

Risk Assessment and Management

The risk assessment must identify and prioritise the risks based on the IT operation of SaaS solutions. The findings are to contribute to the identification and prioritisation of management interventions and precautionary measures necessary to address relevant risks.

CyberPilot ApS' control procedures	Auditor's test of controls	Test findings
<p>Through a risk assessment, risks have been identified and prioritised. The SaaS solutions defined in the description are used as basis for the assessment.</p> <p>The findings contribute to the identification and prioritisation of management interventions and precautionary measures necessary to address relevant risks.</p>	<p>We have requested and obtained the relevant material in connection with the audit of risk management.</p> <p>We have checked that regular risk assessments are carried out for SaaS solutions in relation to business conditions and their development. We have checked that the risk assessment is deployed down through the company's organisation.</p> <p>We have checked that the company's exposure is managed on a current basis and that relevant adaptations of consequences and probabilities are made regularly.</p>	<p>No comments.</p>

CONTROL OBJECTIVE 5:

Information Security Policies

Management must prepare an information security policy that covers, among other things, management's security objectives, policies, and overall action plan. The information security policy will be maintained, taking the current risk assessment into consideration.

CyberPilot ApS' control procedures	Auditor's test of controls	Test findings
<p>There is a written strategy covering, among other things, Management's security objectives, policies and overall action plan.</p> <p>The IT security policy and accompanying supporting policies are approved by the company's Management, and then deployed down through the company's organisation.</p> <p>The policy is available for all relevant employees.</p> <p>The policy is re-evaluated according to planned intervals.</p>	<p>We have obtained and audited CyberPilot ApS' latest IT security policy.</p> <p>During our audit, we checked that maintenance of the IT security policy is conducted on a regular basis. At the same time, we checked during our audit that the underlying supporting policies have been implemented.</p> <p>We have checked that the policy is approved and signed by the company's Supervisory and Executive Boards and made available for the employees on CyberPilot ApS' intranet.</p>	<p>No comments.</p>

CONTROL OBJECTIVE 6:

Organisation of Information Security

Management of the IT security must be established in the company. Organisational responsibility for the IT security must be placed with appropriate business procedures and instructions. The person responsible for IT security must, among other things, ensure compliance with security measures, including continuous updating of the overall risk assessment.

CyberPilot ApS' control procedures	Auditor's test of controls	Test findings
<p>Organisational responsibility for IT security has been assigned, documented, and implemented.</p> <p>The IT security has been coordinated across the company's organisation.</p>	<p>Through inspection and tests, we have ensured that the organisational responsibility for IT security is documented and implemented.</p> <p>We have checked that the IT security is deployed across the organisation in relation to SaaS solutions.</p> <p>By making interviews, we have checked that the person responsible for IT security knows his/her role and responsibilities.</p>	<p>No comments.</p>

CONTROL OBJECTIVE 7:

Human Resource Security

It must be ensured that all new employees are aware of their specific responsibilities and roles in connection with the company's information security in order to minimise the risk of human errors, theft, fraud and abuse of the company's information assets.

CyberPilot ApS' control procedures	Auditor's test of controls	Test findings
<p>Based on the specified work processes and procedures, it is ensured that all new employees are informed of their specific responsibilities and roles in connection with their employment at CyberPilot ApS. This includes the framework laid down for the work and the IT security involved.</p> <p>Security responsibilities, if any, are determined and described in job descriptions and in the form of employment contract terms.</p> <p>The employees are familiar with their professional secrecy based on a signed employment contract and through CyberPilot ApS' HR policy.</p>	<p>We have verified that routines and procedures developed by Management in connection with start of employment and termination of employment have been adhered to.</p> <p>Based on random samples, we have tested whether the above routines and procedures have been complied with in connection with start of employment and termination of employment.</p> <p>Through interviews, we have checked that employees of significance to SaaS solutions are familiar with their professional secrecy.</p> <p>We have examined the job descriptions and employment contracts of key employees and subsequently tested the individual employee's awareness of their roles and related security responsibility.</p> <p>We have ensured that CyberPilot ApS' HR policy is easily accessible and has a section about terms for professional secrecy with respect to information obtained in connection with work conducted at CyberPilot ApS.</p>	<p>No comments.</p>

CONTROL OBJECTIVE 8:

Asset Management

Necessary protection of the company’s information assets must be ensured and maintained, all the company’s physical and functional assets related to information must be identified, and a responsible owner appointed. The company must ensure that information assets related to SaaS solutions have an appropriate level of protection.

There must be reassuring controls to ensure that data media are properly disposed of when no longer needed, in accordance with formal procedures.

CyberPilot ApS’ control procedures	Auditor’s test of controls	Test findings
<p>All information assets have been identified and an updated list of all significant assets has been established.</p> <p>An “owner” of all significant assets is appointed in connection with the IT operation of SaaS solutions.</p>	<p>We have examined and checked the company’s central IT register for significant IT entities in connection with the IT operation of SaaS solutions.</p> <p>Through observations and control, we checked relations to central knowhow systems for the IT operation of SaaS solutions.</p> <p>By observations and enquiries, we have checked that CyberPilot ApS complies with all material security measures for the area in accordance with the security standard.</p>	<p>No comments.</p>
<p>Information and data in relation to SaaS solutions are classified based on business value, sensitivity and need for confidentiality.</p>	<p>We have controlled that there is an appropriate division of assets and accompanying procedures/routines in relation to CyberPilot ApS’ SaaS solutions. In this connection, we have controlled, whether internal procedures/routines regarding ownership to applications and data are complied with.</p> <p>We have checked that contracts and SLA are used as central tools to ensure the definition, segregation and delimitation of CyberPilot ApS’ responsibilities and the customer’s responsibilities with respect to access to information and data.</p> <p>Accordingly, the customer is typically responsible for ensuring that a suitable protection level exists for their own information and data.</p>	<p>No comments.</p>
<p>Procedures for dealing with destruction of data media are established.</p>	<p>We have:</p> <ul style="list-style-type: none"> • Asked Management which procedures/ control activities are performed regarding disposal of data media. • On a sample basis gone through the procedures for destruction of data media. 	<p>No comments.</p>

CONTROL OBJECTIVE 9:

Access Control

Access to the company's systems, information and network must be controlled based on business and statutory requirements. Authorised users' access must be ensured, and unauthorised access must be prevented.

CyberPilot ApS' control procedures	Auditor's test of controls	Test findings
<p>Documentation and updated directions exist for CyberPilot ApS' access control.</p>	<p>We have:</p> <ul style="list-style-type: none"> asked Management whether access control procedures have been established at CyberPilot ApS. verified on a test basis that access control procedures exist and have been implemented; see CyberPilot ApS' directions. by interviewing key staff and by inspection on a test basis, we have verified that access control for the operations environment comply with CyberPilot ApS' directions, and authorisations are granted according to agreement. 	<p>No comments.</p>
<p>A formal business procedure exists for granting and discontinuing user access.</p> <p>Granting and application of extended access rights are limited and monitored.</p>	<p>We have asked Management, whether access control procedures have been established at CyberPilot ApS.</p> <p>We have by inspection on a test basis verified:</p> <ul style="list-style-type: none"> that adequate authorisation systems are used in relation to access control at CyberPilot ApS. that the formalised business procedures for granting and discontinuing user access have been implemented in CyberPilot ApS' systems, and registered users are subject to regular follow-up. 	<p>No comments.</p>
<p>Internal users' access rights are reviewed regularly according to a formalised business procedure.</p>	<p>By inspection on a test basis, we have verified that a formalised business procedure exists for follow-up on authorisation control according to the directions, including:</p> <ul style="list-style-type: none"> that formal management follow-up is performed on registered users with extended and ordinary rights every 6 months. 	<p>No comments.</p>

<p>The granting of access codes is controlled through a formalised and controlled process, which ensures, among other things, that standard passwords are changed.</p>	<p>We have asked Management whether procedures granting access code have been established at CyberPilot ApS.</p> <p>By inspection on a test basis, we have verified</p> <ul style="list-style-type: none"> • that an automatic systems control takes place, when access codes are granted to check that passwords are changed after first login. • that standard passwords are changed in connection with implementation of systems software, etc. • if this is not possible, that procedures ensure that standard passwords are changed manually. 	<p>No comments.</p>
<p>Access to operating systems and networks are protected by passwords.</p> <p>Quality requirements have been specified for passwords, which must have a minimum length, and requirements as to complexity. However, no requirements in relation to maximum duration of password, and likewise password setup means that password can be reused.</p> <p>In addition, 2-factor logon is a requirement.</p> <p>Furthermore, the user will be barred, in the event of repeated unsuccessful attempts to login.</p>	<p>We have asked Management whether procedures ensuring quality passwords in CyberPilot ApS are established.</p> <p>By inspection on a test basis, we have verified that appropriately programmed controls have been established to ensure quality passwords complying with the policies for:</p> <ul style="list-style-type: none"> • minimum length of password • complexity of password (both digits and letters) • lockout after unsuccessful login attempts • 2-factor logon 	<p>No comments.</p>

CONTROL OBJECTIVE 12:

Operations Security

Control objective: Operations procedures and areas of responsibility.

A correct and adequate running of the company's operating systems must be ensured. The risk of technology related crashes must be minimised. A certain degree of long-term planning is imperative in order to ensure sufficient capacity. A continuous capacity projection must be performed based on business expectations for growth and new activities and the capacity demands derived hereof.

CyberPilot ApS' control procedures	Auditor's test of controls	Test findings
<p>The operations procedures for business-critical systems are documented, and they are available to staff with work-related needs.</p> <p>Management has implemented policies and procedures to ensure satisfactory segregation of duties.</p>	<p>We have:</p> <ul style="list-style-type: none"> • Asked Management whether all relevant operation procedures are documented. • In connection with our audit of the individual areas of operation verified on a test basis that documented procedures exist and that there is concordance between the documentation and the procedures actually performed. • Inspected users with administrative rights in order to verify that access is justified by work-related needs and does not compromise the segregation of duties. 	<p>No comments.</p>
<p>Management of operational environment is established in order to minimise the risk of technology related crashes.</p> <p>Continuous capacity projection is performed based on business expectations for growth and new activities and the capacity demands derived hereof.</p>	<p>We have:</p> <p>Asked Management about the procedures and control activities performed.</p> <p>On a test basis examined that the operation environment's consumption of resources is monitored and adapted to the expected and necessary capacity requirements.</p>	<p>No comments.</p>

Control objective: Protection from malware

To protect from malicious software, such as virus, worms, Trojan horses and logic bombs. Precautions must be taken to prevent and detect attacks from malicious software.

CyberPilot ApS' control procedures	Auditor's test of controls	Test findings
Preventive, detecting and remedial security and control measures have been established, including the required training and provision of information for the company's users of information systems against malicious software.	We have: <ul style="list-style-type: none"> enquired about and inspected the procedures/ control activities performed in the event of virus attacks or outbreaks. enquired about and inspected the activities meant to increase the employees' awareness of precautions against virus attacks or outbreaks. verified that anti-virus software has been installed on servers and inspected signature files documenting that they have been updated. 	No comments.

Control objective: Backup

To ensure the required accessibility to the company's information assets. Set procedures must be established for backup and for regular testing of the applicability of the copies.

CyberPilot ApS' control procedures	Auditor's test of controls	Test findings
Backup is made of all of the company's significant information assets, including, e.g. parameter setup and other operations-critical documentation, according to the specified directions.	We have: <ul style="list-style-type: none"> asked Management about the procedures/ control activities performed. examined backup procedures on a test basis to confirm that these are formally documented. examined backup log on a test basis to confirm that backup has been completed successfully and that failed backup attempts are handled on a timely basis. examined physical security (e.g. access limitations) for internal storage locations to confirm that backup is safely stored. 	No comments.

Control objective: Logging and monitoring

To reveal unauthorised actions. Business-critical IT systems must be monitored, and security events must be registered. Logging must ensure that unwanted incidences are detected.

CyberPilot ApS' control procedures	Auditor's test of controls	Test findings
<p>Operating systems and network transactions or activities involving special risks are monitored. Abnormal conditions are examined and resolved on a timely basis.</p> <p>CyberPilot ApS logs, when internal users log off and on the systems.</p> <p>Only in the event of suspected or identified abuse of the systems, users are actively monitored.</p>	<p>We have:</p> <ul style="list-style-type: none"> asked Management about the procedures/ control activities performed, and have examined the system setup on servers and important network units as well as verified that parameters for logging have been set up, thus transactions made by users with extended rights are being logged. checked on a test basis that logs from critical systems are subject to sufficient follow-up. 	<p>No comments.</p>
<p>A central monitoring tool is used which sends alerts, if known errors occur. If possible, it is monitored whether an error is about to occur in order to react proactively.</p> <p>Alerts are shown on the monitoring screen mounted in the project and operations department. Critical alerts are also sent by email and SMS.</p> <p>Status reports are sent by email from different systems. Some daily – others when incidents occur in the system. The operation function is responsible for checking these emails daily.</p>	<p>We have:</p> <ul style="list-style-type: none"> asked Management about the procedures/ control activities performed. ensured that a monitoring tool is used and that this is available to all employees. ensured that alerts are sent by email and SMS, if errors occur. examined status reports. ensured that an operations function is established and checks reports on a daily basis. 	<p>No comments.</p>

Control objective: Managing operations software and managing vulnerability.

Ensuring establishment of appropriate procedures and controls for implementation and maintenance of operating systems.

CyberPilot ApS' control procedures	Auditor's test of controls	Test findings
<p>Changes in the operation environment comply with established procedures.</p>	<p>We have asked Management, whether procedures for patch management are established in CyberPilot ApS.</p> <p>By inspection on test basis, we have verified that</p> <ul style="list-style-type: none"> • adequate procedures are applied, when controlled implementation of changes to the production environment of CyberPilot ApS is performed. • changes to CyberPilot ApS' operation environment comply with directions in force, including correct registration and documentation of applications about changes. <p>On a test basis, we have inspected that the operating systems are updated in compliance with procedures in force and that current status is registered.</p>	<p>No comments.</p>
<p>Changes in user systems and operation environments comply with formalised procedures and processes.</p>	<p>We have asked Management, whether procedures for patch management are established in CyberPilot ApS.</p> <p>By inspection on test basis, we have verified that adequate procedures are applied for controlled implementation of changes in the production environments, including that demands to the patch management controls ensure that</p> <ul style="list-style-type: none"> • applications for change are registered and described. • all changes are subject to formal approval before implementation • changes are subject to formal impact assessments. • fall-back plans are described. • systems affected by changes are identified. • documented test of changes is performed before implementation • documentation is updated reflecting the implemented changes in all material respects. • procedures are subject to managing and coordination in a "change board". 	<p>No comments.</p>

CONTROL OBJECTIVE 14:

System acquisition, development, and maintenance

Ensure that software development related to SaaS solutions is managed using suitable IT control measures, including appropriate segregation between production and development environment.

CyberPilot ApS' control procedures	Auditor's test of controls	Test findings
<p>CyberPilot ApS has planned system development and maintenance activities based on the proprietary model for project management.</p> <p>All changes meant to be put into operation in the production environment, must be approved by the development department.</p>	<p>We have checked the existence of formal procedures and work routines for segregation between production and development.</p> <p>User management ensures suitable control measures in connection with managing the logical access control. We have checked that the different user groups are controlled at set intervals.</p> <p>The structure of the development organisation includes a central steering committee responsible for providing suitable work routines and accompanying control measures for the management.</p> <p>In connection with our audit, we have checked that internal education is conducted for staff working with SaaS solutions and the accompanying development environment. During the process we tested, whether staff was trained in using CyberPilot ApS' quality model for development.</p> <p>The control environment for the development platform is based on the same IT security structure as stated for the production environment.</p> <p>All user activities are recorded and logged in the central database. The person responsible for IT security reviews the log database on a regular basis.</p>	<p>No comments.</p>

CONTROL OBJECTIVE 15:

Supplier Relationships

External business partners are obliged to comply with the company’s established framework for IT security level.

CyberPilot ApS’ control procedures	Auditor’s test of controls	Test findings
<p>Risks related to external business partners are identified, and security in relation to external business partners is managed.</p>	<p>We have verified that in connection with the use of external business partners there are formal cooperation agreements.</p> <p>On a test basis, we have inspected that the cooperation agreements with external suppliers comply with the requirements about covering relevant security conditions in relation to the individual agreement.</p>	<p>No comments.</p>
<p>In case of changes with impact on the production environment, and where services from external suppliers are used, suppliers are selected by the IT Security Manager. Solely approved suppliers are used.</p>	<p>We have asked Management about relevant procedures applied in connection with choosing external partners.</p> <p>We have ensured that appropriate procedures for managing cooperation with external partners are established.</p> <p>We have tested that key suppliers have updated and approved contracts.</p>	<p>No comments.</p>
<p>Monitoring must be conducted on a regular basis, including supervision of external business partners.</p>	<p>We have ensured that there are appropriate processes and procedures for ongoing monitoring of external suppliers.</p> <p>We have checked that ongoing supervision is conducted by means of independent auditor’s reports.</p>	<p>No comments.</p>

CONTROL OBJECTIVE 16:

Information Security Incident Management

To achieve reporting of security incidents and weaknesses in the company's information processing systems in a way that allows for timely corrections.

CyberPilot ApS' control procedures	Auditor's test of controls	Test findings
<p>Security incidents are reported to Management as soon as possible, and the handling is performed in a consistent and efficient way.</p>	<p>We have asked Management whether procedures are established for reporting security incidents.</p> <p>We have verified that procedures and routines are developed for reporting and handling of security incidents, and that the reporting is submitted to the right places in the organisation; see the directions.</p> <p>We have verified that the responsibility for the handling of critical incidents is clearly delegated, and that the related routines ensure that security breaches are handled expediently, efficiently and methodically.</p>	<p>No comments.</p>

CONTROL OBJECTIVE 17:

Information Security Aspects of Business Continuity Management

Business continuity management is to counteract interruption in the company's business activities, protect critical information assets against the impact of a major crash or disaster, as well as ensure fast recovery.

CyberPilot ApS' control procedures	Auditor's test of controls	Test findings
<p>A consistent framework has been established for the company's contingency plans to ensure that all the plans are coherent and meet all security requirements and to determine the prioritisation of tests and maintenance.</p>	<p>We have asked Management whether business continuity management has been developed for SaaS solutions at CyberPilot ApS.</p> <p>By inspection on a test basis, we have verified</p> <ul style="list-style-type: none"> • that appropriate framework for preparation of business continuity management has been established • that contingency plans are prepared and implemented • that the plans include business continuity management across the organisation • that the plans include appropriate strategy and procedures for communication with the stakeholders of CyberPilot ApS. • that contingency plans are tested on a regular basis • that maintenance and reassessment of the total basis for business continuity management is undertaken on a regular basis. 	<p>No comments.</p>

CONTROL OBJECTIVE 18:

Compliance with the Role as Data Processor

Principles for processing personal data:

Procedures and controls are complied with to ensure that collecting, processing and storing of personal data are performed in accordance with the agreements for processing personal data.

CyberPilot ApS' control procedures	Auditor's test of controls	Test findings
<p>A uniform framework is established in the form of standard contracts, Service Level Agreements, as well as Data Processor Agreements or the like, containing an outline of the basis for processing personal data.</p>	<p>We have controlled the existence of updated procedures in writing for processing personal data, and that the procedures include requirements to legal processing of personal data.</p>	<p>No comments.</p>
<p>Personal data is only processed according to directions from the Data Controller.</p>	<p>We have controlled that Management secures that personal data is only processed according to directions.</p> <p>We have controlled by random check of a suitable number of processing that these are conducted according to directions.</p>	<p>No comments.</p>
<p>Management immediately informs the Data Controller, if a direction, in the Data Processor's opinion, infringes the GDPR or the data protection rules according to other EU or member state data protection provisions.</p>	<p>We have controlled that Management secures that processing is examined, and that formalised procedures exist ensuring verification that processing is not against the GDPR or other legislation.</p> <p>We have controlled that procedures are in place for informing the Data Controller of cases where the processing of personal data is evaluated to be against legislation.</p> <p>We have controlled that the Data Controller was informed in cases, where the processing of personal data was evaluated to be against legislation.</p>	<p>No comments.</p>

Data processing:

Procedures and controls are complied with to ensure that personal data can be deleted or returned if arrangements are made with the data controller to this effect.

CyberPilot ApS' control procedures	Auditor's test of controls	Test findings
<p>Written procedures exist which include as a requirement that personal data must be stored and deleted in accordance with the agreement with the Data Controller.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have controlled that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the Data Controller.</p> <p>We have controlled that the procedures are up to date.</p>	<p>No comments.</p>
<p>Upon termination of the processing of personal data for the Data Controller, data has, in accordance with the agreement with the Data Controller, been:</p> <ul style="list-style-type: none"> • Returned to the Data Controller; and/or • Deleted if this is not in conflict with other legislation. 	<p>We have controlled that formalised procedures are in place for processing the Data Controller's data upon termination of the processing of personal data.</p> <p>We have controlled by using a suitable random sample of terminated data processing sessions during the assurance period that documentation exists proving that the agreed deletion or return of data has taken place.</p>	<p>No comments.</p>
<p>Written procedures exist which include a requirement that personal data must only be stored in accordance with the agreement with the Data Controller.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have controlled that formalised procedures exist for only storing and processing personal data in accordance with the data processor agreements.</p> <p>We have controlled that the procedures are up to date.</p> <p>We have controlled by way of random samples, whether underlying documentation exist ensuring that data processing takes place in accordance with the data processor agreement.</p>	<p>No comments.</p>

The Data Processor’s responsibility:

Procedures and controls are complied with to ensure that only approved sub-processors are used and that, when following up on such processors' technical and organisational measures to protect the rights of Data Subjects and the processing of personal data, the Data Processor ensures adequate security of processing.

CyberPilot ApS’ control procedures	Auditor’s test of controls	Test findings
<p>Written procedures exist which include requirements for the data processor when using sub-processors, including requirements for sub-processor agreements and instructions.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have controlled that formalised procedures are in place for using sub-processors, including requirements for sub-processor agreements and instructions.</p> <p>Inspected that procedures are up to date.</p>	<p>No comments.</p>
<p>The Data Processor only uses sub-processors to process personal data, who have been specifically or generally approved by the Data Controller.</p>	<p>Inspected that the Data Processor has a complete and updated list of the sub-processors used.</p> <p>Inspected by way of a sample of 2 sub-processors from the Data Processor’s list of sub-processors that documentation exists that the processing of data by the sub-processor is stated in the data processor agreements – or otherwise approved by the Data Controller.</p>	<p>No comments.</p>
<p>When changing the generally approved sub-processors used, the Data Controller is informed in time to enable such controller to raise objections and/or withdraw personal data from the Data Processor. When changing the specially approved sub-processors used, this has been approved by the Data Controller.</p>	<p>We have controlled that formalised procedures are in place for informing the Data Controller when changing the sub-processors used.</p> <p>Inspected documentation that the Data Controller was informed when changing the sub-processors used throughout the assurance period.</p>	<p>No comments.</p>
<p>The Data Processor has subjected the sub-processor to the same data protection obligations as those provided in the data processor agreement or similar document with the Data Controller.</p>	<p>Checked by way of inspection for the existence of signed Sub-processor Agreements with all sub-processors used and stated on the Data Processor’s list.</p> <p>Inspection by way of a sample of 2 Sub-processors Agreements that such agreements include the same requirements and obligations as are stipulated in the data processor agreements between the Data Controllers and the Data Processor.</p>	<p>No comments.</p>

The Data Processor has a list of approved sub-processors disclosing:

- Name;
- Business Registration No. (CVR-no.);
- Address;
- Description of the processing.

We have controlled that the Data Processor has a complete and updated list of sub-processors used and approved.

Inspected that, as a minimum, the list includes the required details about each sub-processor.

No comments.

Assisting the Data Controller:

Procedures and controls are complied with to ensure that the Data Processor can assist the Data Controller in handing out, correcting, deleting or restricting information on the processing of personal data to the Data Subject.

CyberPilot ApS' control procedures	Auditor's test of controls	Test findings
<p>Written procedures exist which include a requirement that the Data Processor must assist the Data Controller in relation to the rights of Data Subjects.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have controlled that formalised procedures are in place for the Data Processor's assistance to the Data Controller in relation to the rights of Data Subjects.</p> <p>Inspected that procedures are up to date.</p>	<p>No comments.</p>
<p>The Data Processor has established procedures, in so far as this was agreed, that enable timely assistance to the Data Controller in handing out, correcting, deleting, restricting or providing information about the processing of personal data to Data Subjects.</p>	<p>We have controlled that the procedures in place for assisting the Data Controller include detailed procedures for:</p> <ul style="list-style-type: none"> • Handing out data; • Correcting data; • Deleting data; • Restricting the processing of personal data; • Providing information about the processing of personal data to Data Subjects. <p>Inspected documentation that the systems and databases used support the performance of the relevant detailed procedures.</p>	<p>No comments.</p>

Records of processing activities:

Procedures and controls are complied with to ensure that the Data Processor keeps records of processing personal data for which the Data Processor is responsible.

CyberPilot ApS' control procedures	Auditor's test of controls	Test findings
Records exist of processing activities for the SaaS solutions in combination with the relevant Data Controller.	We have controlled documentation displaying the existence of records for processing activities for the SaaS solutions combined with the relevant Data Controller.	No comments.
Assessments are made on a regular basis – and at least once a year - as to whether the records are updated and correct.	We have controlled the documentation disclosing that the records of the processing activities for each Data Controller are updated and correct.	No comments.

Transfer of personal data to third countries etc.

Procedures and controls are complied with to ensure that the data processor will only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller as well as by using a valid basis of transfer.

CyberPilot ApS' control procedures	Auditor's test of controls	Test findings
<p>Written procedures exist which include a requirement that the data processor must only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller and by using a valid basis of transfer.</p> <p>On an ongoing basis, and at least once a year, assessment is made whether the procedures need updating.</p>	<p>Inspected that formalised procedures exist to ensure that personal data is only transferred to third countries or international organisations in accordance with the agreement with the data controller and by using a valid basis of transfer.</p> <p>We have checked that the procedures are updated.</p>	No comments.
The data processor only transfers personal data to third countries or international organisations according to instructions from the data controller.	Inspected that formalized procedures exist ensuring that personal data is only transferred to third countries or international organisations in accordance with instructions from the data controller.	No comments.
The data processor documents instructions obtained from the data controller in relation to transfer of personal data to third countries or international organisations.	Inspected that documented instructions are obtained from the data controller in relation to transfer of personal data to third countries or international organisations.	No comments.

The data processor assesses and documents the existence of a valid basis of transfer in relation to transfer of personal data to third countries or international organisations.

Inspected formalised procedures are in place for ensuring a valid basis of transfer.

No comments.

Reporting breaches of personal data security to the Supervisory Authority (the Danish Data Protection Agency):

There is compliance with procedures and controls ensuring that any security breaches are managed in accordance with the entered Data Processor Agreement.

CyberPilot ApS' control procedures	Auditor's test of controls	Test findings
There are procedures in writing - updated at least once a year – describing how to manage personal data security breaches, including timely communication to the Data Controller.	We have controlled the existence of updated procedures in writing regarding managing personal data security breaches, including description of timely communication to the Data Controller.	No comments.
Data Processor ensures recording of all personal data security breaches.	We have controlled documentation disclosing that all personal data security breaches are recorded at the Data Processor.	No comments.
Management has ensured that all personal data security breaches are timely and sufficiently communicated to the Data Controller, including personal data security breaches happened at Data Processors used as subcontractors.	We have controlled documentation displaying that Management has ensured that all personal data security breaches are timely and sufficiently communicated to the Data Controller, including personal data security breaches happened at Data Processors used as subcontractors.	No comments.