



OCTOBER 2017

# FRONTSAFE A/S

## ISAE 3402 TYPE 2 ASSURANCE REPORT

Independent auditor's report on general IT controls in relation to the operation of Frontsafe Cloud Backup.

Beierholm  
Statsautoriseret Revisionspartnerselskab  
Knud Højgaards Vej 9  
2860 Søborg  
CVR-nr. 32 89 54 68  
Tlf +45 39 16 76 00

[www.beierholm.dk](http://www.beierholm.dk)

# Structure of the assurance report

## Chapter 1:

Frontsafe A/S' Letter of Representation

## Chapter 2:

Frontsafe A/S' description of general IT controls for the operation of Cloud Backup.

## Chapter 3:

Independent Auditor's Assurance Report on the description of the general IT controls, their design and operating effectiveness.

## Chapter 4:

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

CHAPTER 1:

## Frontsafe A/S' Letter of Representation

This description in Chapter 2 of Frontsafe A/S' general IT controls has been prepared for customers, who have used or plan to use Frontsafe A/S' Cloud Backup, and their auditors, who have sufficient understanding to consider the description, along with other information, including information about controls operated by customers themselves, when assessing the risks of material misstatement in their financial statements. Frontsafe A/S hereby confirms that

- (A) The description in Chapter 2 gives a true and fair description of Frontsafe Cloud Backup's general IT controls throughout the period 1 May 2016 - 30 September 2017. The criteria for this assertion are that this description:
- (i) gives an account of how the controls were designed and implemented, including:
    - the types of services delivered, when relevant
    - the processes in both IT and manual systems that are used to manage the general IT controls
    - relevant control objectives and control procedures designed to achieve these goals
    - control procedures that we have assumed – with reference to the system's design – would be implemented by Frontsafe A/S and which, if necessary to fulfil the control objectives mentioned in the description, have been identified in the description together with the specific control objectives that we cannot fulfil ourselves
    - other aspects of our control environment, risk assessment process, information system and communication, control activities and monitoring controls that have been relevant for the general IT controls
  - (ii) includes relevant information about changes in Frontsafe A/S' general IT controls made during the period 1 May 2016 - 30 September 2017
  - (iii) does not omit or misrepresent information that is 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 system that each individual customer may consider important in his 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 May 2016 to 30 September 2017. The criteria for this assertion are that:
- (i) The risks that threatened 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 these 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 May 2016 - 30 September 2017.
- (C) the accompanying description and the related criteria for fulfilling the control objectives and controls, Chapter 2, have been prepared based on compliance with Frontsafe A/S' standard agreement, the basis for Cloud Backup and services regarding the general IT controls. The criteria for this basis are:
- (i) Service Level Agreement for Cloud Backup Version 7 – 2016
  - (ii) General conditions for Cloud Backup Version 7 - 2016

Taastrup, 2 October 2017

  
**Sigve Torvik, General Manager**

  
**Maurice Akkermans, Principal Operations Engineer**

Frontsafe A/S, Spotorno Alle 12, DK-2639 Taastrup, Tel (+45) 8743 4090, CVR: 29631123

CHAPTER 2:

# Frontsafe A/S' description of general IT controls for the operation of Cloud Backup

## Introduction

The purpose of this description is to provide Frontsafe A/S' customers and their auditors with information regarding the requirements of ISAE 3402, which is the international auditing standard for assurance reports on controls at service organisations.

Furthermore, the description also provides information on the controls used for the operation of Frontsafe Cloud Backup during the period 1 May 2016 – 30 September 2017.

## Description of Frontsafe A/S and scope of services

Frontsafe A/S is part of j2 Global, which is one of the world's biggest service supplier within Cloud backup. There is still Danish support, operations and sales focusing on building a well-functioning partner strategy.

Frontsafe A/S has its domicile in Taastrup and data centres situated in Viby J.

Frontsafe A/S is a specialised and focused supplier of Cloud backup for businesses on the Danish market. Frontsafe A/S provides its Cloud Backup solutions to thousands of customers, whose more than 13.000 servers are secured on a daily basis through reliable service and support with more than 10 years' experience of operating Storage and Backup.

In recent years, Frontsafe A/S has developed knowhow and competences, and today offers the market backup-related services, including VEEAM Cloud Repository, which together with IBM Spectrum Protect is leading on the world market for Backup, both as a service and On-Premise solutions.

## Business strategy/IT security strategy

At Frontsafe A/S, our goal is continuously reducing the impact that the operation of our services has on the environment. We have set a specific goal, which is to reduce the energy consumption per stored GB by at least 5 per cent each year. Accordingly, Frontsafe Purchasing Department is required to ensure that the acquisitions of hardware and software for the operations have a positive impact on the fulfilment of our goal. The following figures show the savings in percentages from year to year in KW power consumption per stored GB in the Frontsafe production over the last six years of operation:

KW/GB savings in percent in relation to the previous year

2011:	34.66%
2012:	24.63%
2013:	5.79%
2014:	22,86%
2015:	30,57%
2016:	10,08%

As shown above, Frontsafe A/S has lived up to the goal of an annual reduction in the power consumption per stored GB of at least 5 per cent.

It is an important element in Frontsafe A/S' strategy that sufficient security is incorporated in the business so that the company is not exposed to unacceptable risks.

Frontsafe A/S has three overall strategic benchmarks:

- Frontsafe A/S helps companies make optimum use of modern information technology
- Frontsafe A/S is operating primarily with administrative systems to secure data
- Frontsafe A/S is a good place to work for a stable and well-trained team of employees

Frontsafe A/S is working with IT security at a business-strategic level and is therefore making a continuous effort to secure high service and quality levels. In the company's security policy, Management emphasises that IT security is and must be an important part of the company's business culture. Frontsafe A/S has chosen to base its IT security strategy on ISO27002:2013, and has used the ISO methodology for implementation of relevant security measures within the following areas:

- Information security policies
- Organisation of information security
- Human resource security
- Asset management
- Access control
- Physical and environmental security
- Operations security
- Communication security
- Supplier relationships
- Information security management
- Information security aspects of business continuity management

The precautionary measures implemented at Frontsafe A/S appear from appendix 1 of this description.

### Frontsafe A/S' organisation and organisation of IT security

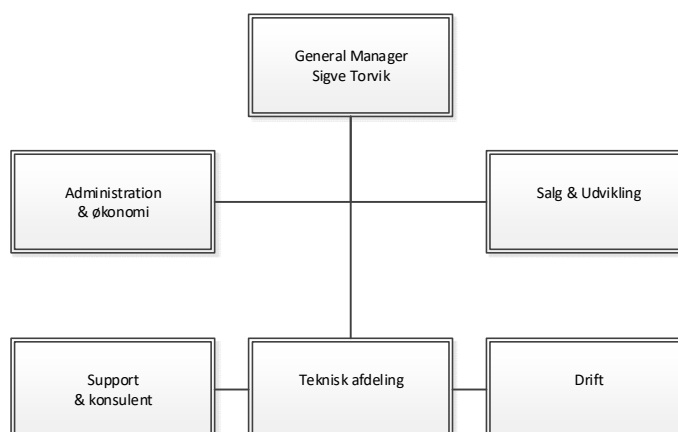
J2 Global is listed on the US stock exchange NASDAQ. It was founded in 1995 with focus on business critical technology and employs a staff of more than 2.000.

J2 Global services more than 11 million satisfied customer on 6 continents.

Frontsafe A/S employs a staff of 12 and has a flat organisational structure.

In charge of IT security: Principal Operations Engineer

For the purpose of external cooperation partners, a cooperation agreement is prepared before any work is initiated.



Frontsafe A/S has decided on an 17—months Assurance Report due to changes within staff and Management, in order to go over and reassess security, procedures etc.

During the said period, the domicile is moved to Spotorno Allé in Taastrup, and new staff members have been employed as replacement for existing and former employees. There has been a reasonable transfer period from former to new employees, we have now got the Frontsafe group of employees sorted out, and they cover the key functions described in the Report. Due to the ownership by j2 Global, the name Frontsafe will be changed to KeepitSafe during the first half of 2018, making the group a 100% integrated part of j2 Global, and in this way a number of new backup services will be introduced on the Danish market, too.

### **Risk management at Frontsafe A/S**

It is Frontsafe policy that the risks related to the company's activities must be covered or limited to such an extent that the company will be able to continue normal operations. Frontsafe A/S performs risk management and internal controls within several areas and at different levels. An annual risk and threat assessment is made. The approach is very informal. The informal risk assessment is conducted at intervals, and when we make changes to existing systems or implement new systems, which we consider relevant in connection with re-assessing our general risk assessment. The responsibility for handling this is placed at the General Manager, and must subsequently be deployed and approved by the Management of the company.

As part of the above-mentioned IT security strategy, Frontsafe A/S is working with the international standards for IT security – ISO27002:2013 – constituting the primary framework for the IT security. The work process regarding IT security is a continuous and dynamic process ensuring that Frontsafe A/S lives up to its customers' requirements and needs at all times.

### **IT security management**

The Principal Operations Engineer holds the day-to-day responsibility for IT security supported by the Management, which ensures compliance with all overall requirements and frameworks for IT security. In the central IT security policy, management has described Frontsafe A/S' IT security structure. The IT security policy has to be revised at least once a year.

The Frontsafe quality assurance system has been defined based on the overall objective about delivering stable and secure IT operations to the customers. In order to be able to do so, it is necessary that we have introduced policies and procedures ensuring that our deliveries are consistent and transparent.

The Frontsafe IT security policy has been prepared with reference to the above, and the policy applies to all employees and all deliveries. In the event of errors and security flaws in our operating environment, the error/security flaw will be remedied immediately.

All servers and network devices are documented in the Frontsafe documentation system. Here, all changes are logged by our system. Configuration files for network devices (firewall, routers, switches, etc.) are stored in our documentation system.

The security policy lays down the general policies for the infrastructure of Frontsafe A/S and does not deal with issues regarding specific products, services or users.



The security policy has been prepared to provide Frontsafe A/S with one common set of rules. In this way, we achieve a stable operating environment and a high security level. We are making regular improvements to policies, procedures and operations.

Frontsafe A/S' current technical setup is described in Service Level Agreement version 7.

### **HR, employees and training**

At the start of their employment, all employees must get security clearance and a background check is made incl. that they have no criminal record. They must sign j2 Global's security policies and a "Business code of ethics". Furthermore, we go over Frontsafe A/S' local information security together with the employee, including confidentiality in relation to customers and partners.

All employees must know their responsibility and role in connection with IT security in order to minimise the risk of human error such as theft, fraud and misuse of information assets.

Frontsafe A/S is a certified IBM Partner with capabilities on IBM Spectrum Protect, and is furthermore a certified Veeam Partner.

All performing consultants possess qualifications within their respective fields of work. Documentation for these exists in the form of relevant certifications.

Frontsafe A/S has to comply with various requirements from IBM and Veeam, including specific requirements that a specific number of consultants have passed specific product certifications, which must be renewed regularly. Through regular product training and course participation, Frontsafe A/S ensures that this high certification status is maintained.

### **Physical security**

Frontsafe A/S' backup facilities are placed in a safe data centre for which assurance reports have been issued according to ISAE 3402 and with the following security measures based on the ISO 27002 standard:

- The emergency power system will start automatically in case of failure or errors in the primary power supply. Furthermore, all equipment is equipped with UPS to ensure that normal operations can continue without interruptions.
- Cooling ensures an ideal temperature in the operations environment.
- To avoid disasters in the event of smoke development and fire, a highly sensitive fire-alarm system has been installed. This system has a smoke sniffer system and ion alarms that take in and analyse the air in the server room and trigger fire-fighting measures in the event of the slightest smoke development.
- Inergen systems have been installed for fire fighting purposes making use of gases that remove oxygen from the air and extinguishes the fire immediately. The server room is designed as a separate fire cell. The fire-fighting system has direct alarm transfer to the fire brigade.
- Distributor boxes and network equipment are placed in a locked server room.
- Personal access cards with codes are used.
- Alarm system is used for all alarm monitoring. Alarm logs are kept. All alarms are transferred to a call centre and/or operations monitoring service team, who initiates and decides on the required actions.
- Primary data lines are established as redundant lines. These lines are forwarded as independent fibres to two different TDC centrals.

## Monitoring

Frontsafe A/S has established automatic monitoring of servers, storage systems, networks, etc. and has trained staff on call in a rotation systems, which ensures that the required qualifications are available 24/7/365.

If an error is identified, an alarm is sent both visually on the monitoring screen and by SMS/e-mail. In the event that errors are identified in a component that is not subject to the automatic monitoring, actions will be taken for future registration hereof in the system. The data centre is monitored with respect to power failure, temperature, fire, water, air humidity. Moreover, the entire data centre is under camera surveillance.

If incidents occur that might affect operations, the monitoring systems will automatically alert the contingency team and well-established escalation procedures exist with ultimate involvement of the General Manager.

The list of persons with access to the data centre is reviewed regularly in accordance with the procedure above.

## Backup

At present Frontsafe A/S offers 3 backup services:

### 1. Cloud backup

Data are sent directly to Frontsafe's IBM Spectrum Project backup servers and storage. Then the customer's data are copied to Frontsafe's secondary datastore on a different physical location.

With Cloud backup solution the customer has 2 offsite copies of the data.

### 2. Hybrid backup

By choosing this solution, the customer has a local copy and an offsite copy of the backup data.

- a. The customer has a local IBM Spectrum Protect server, which is a Front Server. This Front Server synchronises its backup storage with data stored on Frontsafe's backup servers.
- b. The customer has a local Veeam backup solution sending an offsite copy of its backup storage to Frontsafe's storage.

Due to j2 Global's acquisition of Frontsafe A/S, new backup services will eventually be introduced to supplement the existing services, inter alia:

- Cloud2Cloud backup
- DRaaS
- Endpoint protection

Backup at Frontsafe A/S is stored at Danish data centres secured physically and electronically (described under Control Objectives 9-13).

The purpose of backup is securing that the customer's data at Frontsafe A/S's data centre can be restored, accurately and quickly.

All data are secured on a daily basis in another server room at a different geographical location.



## Patch management / change management

The purpose of patch management is to ensure that all relevant updates, such as patches, fixes and service packs from suppliers, are implemented to protect the systems against downtime and unauthorised access and that the implementation is carried out in a well-managed fashion.

All production servers are updated by critical and important updates in the monthly service window. This ensures that production servers do NOT have critical or important updates older than 30 days.

Frontsafe A/S has prepared a fall-back plan in relation to patch management. The purpose of the fall-back plan is to ensure that the systems can return to normal operations, if the updates do not perform as intended.

## Managing IT security incidents

Security incidents and weaknesses in the Frontsafe A/S' systems must be reported in a way that allows for timely adjustments.

All Frontsafe A/S' employees are familiar with the procedure for reporting different types of incidents and weaknesses that may impact the security of Frontsafe operations. Security incidents and weaknesses must be reported to Management as quickly as possible.

It is Management's responsibility to define and coordinate a structured management process ensuring an appropriate reaction to security incidents.

## User management / access security

The logical security includes logical protection of electronic systems and information regarding the service. For example, it specifies that only authorised persons have electronic access.

- Password requirements – all users with access to Frontsafe A/S' systems use passwords containing at least 7 characters including both numbers and letters.
- Screen savers are required – screen savers are activated for all our users to protect them against unauthorised access.

## Business Continuity Management

In the event of serious errors, an e-mail is sent to the e-mail group "All Frontsafe Security Group". The e-mail includes a brief error description and a time horizon for the downtime. At the end of the error correction procedure, a new e-mail is sent to the e-mail group with a message that the error has been solved and a thorough error description.

If one of the server rooms is completely damaged, an action plan is prepared about what is going to happen, including re-establishment of hardware. The systems will then be restored from the backup server.

Every six months, a simulation testing the Frontsafe disaster recovery plan will be performed.

## Significant changes in relation to IT security

During the period under review, there have been no significant changes in relation to IT security.

## The customers' responsibility (complementary customer controls)

The above description is based on the framework above, which means that agreements with individual customers have not been taken into consideration.

Frontsafe A/S is not responsible for access rights, including granting, changes and removal, in relation to the individual customer's users and their access to Frontsafe Cloud Backup. The customer is responsible for ensuring the controls necessary in connection with this control objective.

For some user companies the security in relation to creation of passwords might be below the frame, if the customer's Management wanted it. The responsibility for reconciliation of the control environment for password security stays with each user company, and with those using this report.

The business systems and user systems running via Frontsafe Cloud Backup are the customers' own responsibility. It is the responsibility of the customers to ensure the required control procedures in connection with system development, acquisition and change management.

The customers are responsible for data transmission to Frontsafe Cloud Backup solution, and it is the responsibility of the customers to create the required data transmission to the Frontsafe data centre. The customer must ensure the controls necessary in connection with this control objective.

Frontsafe continuity management is constructed based on an overall contingency plan that describes the approach and procedures to be applied, if recovery of Frontsafe A/S' Cloud Backup is needed. Specific contingency plans can be prepared for the individual customer according to need in proportion to the risk of interrupting business processes.

APPENDIX 1:

## Frontsafe A/S applies the following control objectives and security measures from ISO27002:2013

### 5. Information security policies

- 5.1 Management direction for information security
- 

### 6. Organisation of information security

- 6.1 Internal organisation
  - 6.2 Mobile devices and teleworking
- 

### 7. Human resource security

- 7.1 Prior to employment
  - 7.2 During employment
  - 7.3 Termination or change of employment
- 

### 8. Asset management

- 8.1 Responsibility for assets
  - 8.3 Handling of media
- 

### 9. Access control

- 9.1 Business requirements of access control
  - 9.2 User access management
  - 9.3 Users' responsibility
- 

### 12. Operations security

- 12.1. Operational procedures and responsibilities
  - 12.2. Protection from malware
  - 12.3. Backup
  - 12.4. Logging and monitoring
  - 12.5. Operational software management
- 

### 13. Communication security

- 13.1. Network security management
- 

### 15. Supplier security

- 15.1. Information security in supplier relationships
  - 15.2. Supplier service delivery management
- 

### 16. Information security incident management

- 16.1. Management of Information security incidents and improvements
- 

### 17. Information security aspects of business continuity management

- 17.1. Information security continuity
- 17.2. Redundancies

## CHAPTER 3:

# Independent Auditor's Assurance Report on the description of the general IT controls, their design and operating effectiveness

For the customers of Frontsafe Cloud Backup and their auditors

## Scope

We have been engaged to report on Frontsafe A/S's description in Chapter 2 (including appendix 1), which is a description of general IT controls conducted in connection with the operation of Frontsafe Cloud Backup for processing customers' transactions during the period 1 May 2016 - 30 September 2017, and on the design and operating effectiveness of controls related to the control objectives mentioned in the description.

The report is based on a partial approach, which means that the present report does not include the IT controls and control activities related to the use of external business partners. Frontsafe A/s uses the following external partners in connection with operations of their Cloud Backup in the following areas: Co-location / data centre – the physical security in relation to Frontsafe production equipment.

The report does not cover customer-specific conditions. Furthermore, the report does not cover the complementary controls and control activities conducted by the user company; see the description of the company in Chapter 2 under the section about complementary controls.

## Frontsafe A/S' responsibility

Frontsafe A/S is responsible for the preparation of the description and accompanying assertion in Chapter 2 (including appendix 1), 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 ISQC 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 on Frontsafe A/S's description and on the design and operation of controls related to the control objectives stated in that description based on our procedures. We conducted our engagement in accordance with ISAE 3402, Assurance Reports on Controls at a Service Organisation, issued by the 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 are appropriately designed and operate effectively in all material respects.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service

organisation's description of its system, and the design and operating effectiveness of controls. The procedures selected depend on the 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 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 and described in Chapter 2 (including appendix 1) by Frontsafe A/S.

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

### Limitations of controls at Frontsafe A/S

Frontsafe A/S's description is prepared to meet the common needs of a broad range of customers and their auditors and thus may not include every aspect of the system that each individual customer may consider important in its own particular environment. In addition, because of their nature, controls at Frontsafe A/S may not prevent or detect all errors or omissions in processing or reporting transactions. The projection of any evaluation of effectiveness to future periods is subject to the risk that controls at the service organisations 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 general IT controls of Frontsafe A/S for Cloud Backup, such as they were designed and implemented throughout the period 1 May 2016 – 30 September 2017 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 May 2016 - 30 September 2017; 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, operated effectively throughout the period 1 May 2016 - 30 September 2017.

### 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 intended only for Frontsafe A/S' customers and their auditors, who have sufficient understanding to consider them, along with other information, including information about controls operated by customers themselves, when assessing the risks of material misstatement in their financial statements.

Søborg, 2 October 2017

#### Beierholm

State-Authorized Public Accountant Partner Company



Kim Larsen

State Authorised Public Accountant



Jesper Aaskov Pedersen

IT Auditor, Manager

CHAPTER 4:

# Auditor's Description of Control Objectives, Security Measures, Tests and Findings

We have structured our engagement in accordance with IASE 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 ISO27002:2013.

With respect to the period, we have tested whether Frontsafe A/S has complied with the control objectives throughout the period 1 May 2016 - 30 September 2017.

Each control objective has its own section starting with a recital of the requirements laid down in the Executive Order about Security - Danish: "Sikkerhedsbekendtgørelsen" - (gray text field). Below the gray field are three columns:

- The first column tells the activities Frontsafe A/S, 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 Frontsafe A/S. 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 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.

Frontsafe A/S' 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 Frontsafe A/S' 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 Frontsafe A/S' intranet.</p>	<p>During our test, we did not identify any material deviations.</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 ensure, among other things, compliance with security measures, including continuous updating of the overall risk assessment. External cooperation partners must comply with the company's IT security level framework.

Frontsafe A/S' control procedures	Auditor's test of control procedures	Test findings
<p>Organisational responsibility for IT security has been placed, documented and implemented.</p> <p>The IT security has been coordinated across the company's organisation.</p> <p>Appropriate business procedures exist for employees regarding professional secrecy statements.</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 Cloud Backup.</p> <p>By making interviews, we have checked that the person responsible for IT security knows his/her role and responsibilities.</p> <p>Through enquiries and samples from employment contracts, we checked that Frontsafe A/S' employees are familiar with their professional secrecy.</p>	<p>During our test, we did not identify any material deviations.</p>
<p>Risks in relation to use mobile devices and teleworking are identified, and managing security conditions is appropriate.</p>	<p>We checked that formal cooperation agreements exist in connection with the use of mobile devices and teleworking.</p> <p>On a test basis, we have inspected that the policy is implemented regarding employees using mobile devices.</p> <p>Regarding the use of teleworking at Frontsafe A/S we have checked whether appropriate security measures have been implemented ensuring that this area is covered in relation to the risk assessment of the area.</p>	<p>During our test, we did not identify any material deviations.</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.

Frontsafe A/S' control procedures	Auditor's test of control procedures	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 Frontsafe A/S. 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 terms of the employment contract.</p> <p>The employees are familiar with their professional secrecy based on a signed employment contract and through Frontsafe A/S' 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 Cloud Backup are familiar with their professional secrecy.</p> <p>We have examined the job descriptions of key employees and subsequently tested the awareness of the individual employee of their roles and related security responsibility.</p> <p>We have ensured that Frontsafe A/S' HR policy is easily accessible and has a section on terms for professional secrecy with respect to information obtained in connection with work conducted at Frontsafe A/S.</p>	<p>During our test, we did not identify any material deviations.</p>

CONTROL OBJECTIVE 8:

## Asset Management

The required protection of the company's information assets must be ensured and maintained, and all of the company's physical and functional information-related assets must be identified, and a responsible "owner" must be appointed. The company must ensure that the information assets in relation to Cloud Backup are suitably protected.

Frontsafe A/S' control procedures	Auditor's test of control procedures	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 operation of Cloud Backup.</p>	<p>We have examined and checked the company's central IT register for significant IT entities in connection with the operation of Frontsafe Cloud Backup.</p> <p>Through observation and control, we have checked relations to central knowhow systems for the operation of Cloud Backup.</p> <p>By observations and enquiries, we have checked that Frontsafe A/S complies with all material security measures for the area in accordance with the security standard.</p>	<p>During our test, we did not identify any material deviations.</p>
<p>Information and data in relation to Cloud Backup and the subsequent hosting centre operation are classified based on business value, sensitivity and need for confidentiality.</p>	<p>We have checked that appropriate division exists and related procedures/business procedures in connection with protection of ownership between applications and data as well as other entities in relation to Frontsafe A/S' operation of Cloud Backup.</p> <p>We have checked that contracts and SLA are used as central tools to ensure the definition, segregation and delimitation of Frontsafe A/S' 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 own information and data.</p>	<p>During our test, we did not identify any material deviations.</p>
<p>Procedures of dealing with destruction of data media are established.</p>	<p>We have:</p> <ul style="list-style-type: none"> <li>• Asked Management which procedures/control activities are performed.</li> <li>• On a sample basis gone through the procedures for destruction of data media as confirmation that these are formally documented.</li> </ul>	<p>During our test, we did not identify any material deviations.</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.

Frontsafe A/S' control procedures	Auditor's test of control procedures	Test findings
<p>Documentation and updated direction exist for Frontsafe access control.</p>	<p>We have:</p> <ul style="list-style-type: none"> <li>asked Management whether access control procedures have been established at Frontsafe A/S.</li> <li>verified on a test basis that access control procedures exist and have been implemented; see Frontsafe A/S' directions.</li> <li>by interviewing key personnel and by inspection on a test basis, we have verified that access control for the operations environment comply with Frontsafe A/S' directions, and authorisations are granted according to agreement.</li> </ul>	<p>During our test, we did not identify any material deviations.</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 Frontsafe A/S.</p> <p>By inspection on a test basis, we have verified</p> <ul style="list-style-type: none"> <li>that adequate authorisation systems are used in relation to access control at Frontsafe A/S.</li> <li>that the formalised business procedures for granting and discontinuing user access have been implemented in Frontsafe A/S' systems and registered users are subject to regular follow-up.</li> </ul>	<p>During our test, we did not identify any material deviations.</p>
<p>Internal users' access rights are reviewed regularly according to a formalised business procedure.</p>	<p>By inspection on 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"> <li>that formal management follow-up is performed on registered users with extended rights every three months.</li> <li>that formal management follow-up is performed on registered users with ordinary rights every six months.</li> </ul>	<p>During our test, we did not identify any material deviations.</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 access code granting procedures have been established at Front-safe A/S.</p> <p>By inspection on a test basis, we have verified</p> <ul style="list-style-type: none"> <li>• that an automatic systems control takes place, when access codes are granted to check that passwords are changed after first login.</li> <li>• that standard passwords are changed in connection with implementation of systems software etc.</li> <li>• if this is not possible, that procedures ensure that standard passwords are changed manually.</li> </ul>	<p>During our test, we did not identify any material deviations.</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 (7 characters) including requirements as to complexity. However, no maximum duration is required, and likewise password setup means that passwords might be reused.</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 Frontsafe A/S 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"> <li>• minimum length of password</li> <li>• complexity</li> <li>• lockout after unsuccessful login attempts</li> </ul>	<p>During our test, we did not identify any material deviations.</p>

CONTROL OBJECTIVE 11:

## Physical and Environmental Security

The company's premises and information assets must be protected against unauthorised physical access as well as physical damage and interruption. Security measures must be implemented to avoid that the company's information assets are lost, damaged or compromised and to avoid interruption of the company's business activities. The protective measures must also include destruction of outdated or damaged equipment as well as provision of the required supply of electricity, water and ventilation as well as of cable installations.

Frontsafe A/S' control procedures	Auditor's test of control procedures	Test findings
<p>The secure areas are protected by access control that only allows authorised persons access.</p>	<p>We have examined and checked the physical access to both data centres, which are, among other things, secured by an electronic key system combined with a personal code to ensure limited access to Frontsafe A/S' data centre.</p> <p>Through visits, interviews and observations, we have verified that the access to both of Frontsafe A/S' data centres is in accordance with the above mentioned business procedures regarding access limitation.</p>	<p>During our test, we did not identify any material deviations.</p>
<p>Equipment located in the data centre is protected against physical threats such as fire, water damage, power outage, theft or vandalism.</p> <p>Cables for data communication and electricity supply are protected against tampering.</p> <p>All equipment with storage media is controlled in order to secure that critical/sensitive information and systems imposed with licence are removed or overwritten, when the equipment is disposed of or reused.</p>	<p>We have examined and checked that Frontsafe A/S' data centre meets the requirements laid down by Management.</p> <p>Audit has verified compliance with the required security measures according to ISO 27002, section 11, in relation to protection against damage.</p> <p>Specifically we have:</p> <ul style="list-style-type: none"> <li>• verified the protection of cables for data communication and electricity supply.</li> <li>• examined and checked the procedures prepared by Management for disposal of equipment related to the operation of Cloud Backup.</li> </ul>	<p>During our test, we did not identify any material deviations.</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.

Frontsafe A/S' control procedures	Auditor's test of control procedures	Test findings
<p>The operations procedures for business critical systems have been 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"> <li>asked Management whether all relevant operations procedures have been documented.</li> <li>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 actions actually performed.</li> <li>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.</li> </ul>	<p>During our test, we did not identify any material deviations.</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> <ul style="list-style-type: none"> <li>asked Management about the procedures and control activities performed.</li> <li>on a test basis examined that the operation environment's consumption of resources is monitored and adapted to the expected and necessary capacity requirements.</li> </ul>	<p>During our test, we did not identify any material deviations.</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.

Frontsafe A/S' control procedures	Auditor's test of control procedures	Test findings
Preventive, detecting and remedial security and control procedures 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"> <li>enquired about and inspected the procedures/ control activities performed in the event of virus attacks or outbreaks.</li> <li>enquired about and inspected the activities meant to increase the employees' awareness of precautions against virus attacks or outbreaks.</li> <li>verified that anti-virus software has been installed on servers and inspected signature files documenting that they have been updated.</li> </ul>	During our test, we did not identify any material deviations.

Control objective: Backup

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

Frontsafe A/S' control procedures	Auditor's test of control procedures	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"> <li>asked Management about the procedures/ control activities performed.</li> <li>examined backup procedures on a test basis to confirm that these are formally documented.</li> <li>examined backup log on a test basis regarding backup to confirm that backup has been completed successfully and that failed backup attempts are handled on a timely basis.</li> <li>examined physical security (e.g. access limitations) for internal storage locations to confirm that backup is safely stored.</li> </ul>	During our test, we did not identify any material deviations.

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.

Frontsafe A/S' control procedures	Auditor's test of control procedures	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>Frontsafe A/S logs, when internal users log off and on the systems.</p> <p>Only in the event of suspected or identified abuse of the systems, the users are actively monitored.</p>	<p>We have:</p> <ul style="list-style-type: none"> <li>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.</li> <li>checked on a test basis that logs from critical systems are subject to sufficient follow-up.</li> </ul>	<p>During our test, we did not identify any material deviations.</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 every day – others when incidents occur in the system. The operations monitoring function is responsible for checking these emails on a daily basis.</p>	<p>We have:</p> <ul style="list-style-type: none"> <li>asked Management about the procedures/ control activities performed.</li> <li>ensured that a monitoring tool is used and that this is available to all employees.</li> <li>ensured that alerts are sent by email and SMS, if errors occur.</li> <li>examined status reports.</li> <li>ensured that an operations monitoring service is established and that this function checks reports on a daily basis.</li> </ul>	<p>During our test, we did not identify any material deviations.</p>

Control objective: Managing operations software and managing vulnerability

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

Frontsafe A/S' control procedures	Auditor's test of control procedures	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 at Frontsafe A/S.</p> <p>By inspection on test basis, we have verified that</p> <ul style="list-style-type: none"> <li>adequate procedures are applied, when controlled implementation of changes to the production environments of Frontsafe A/S are performed.</li> <li>changes to Frontsafe A/S' operation environments comply with directions in force, including correct registration and documentation of change requests.</li> </ul> <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>During our test, we did not identify any material deviations.</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 Frontsafe A/S.</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 change management controls ensure that</p> <ul style="list-style-type: none"> <li>change requests are registered and described</li> <li>all changes are subject to formal approval before implementation</li> <li>changes are subject to formal impact assessments</li> <li>fall-back plans are described</li> <li>systems affected by changes are identified</li> <li>documented test of changes is performed before implementation</li> <li>documentation is updated reflecting the implemented changes in all material respects</li> <li>procedures are subject to managing and coordination in a "change board".</li> </ul>	<p>During our test, we did not identify any material deviations.</p>

CONTROL OBJECTIVE 13:

## Communication Security

To ensure protection of information in networks and support of information processing facilities.

Frontsafe A/S' control procedures	The auditor's test of controls	Test findings
<p>Networks must be protected against threats in order to secure network based systems and the transmitted data.</p> <p>Production environment must be secured against failing supply in relation to redundancy to network connection to the internet.</p> <p>Network traffic/access from production environment to the outside world is available by means of multiple supply entries or access from more than one supplier.</p>	<p>It has been checked that necessary protection against unauthorised access is implemented, including:</p> <ul style="list-style-type: none"> <li>• Appropriate procedures for managing network equipment are established.</li> <li>• Segregation of user functions is established.</li> <li>• Appropriate logging and monitoring procedures are established.</li> <li>• Managing the company's network is coordinated in order to ensure optimal utilisation and a coherent security level.</li> <li>• Ensured that connections for data communication with the internet are established via more than one ISP supplier.</li> <li>• On a sample basis gone through documentation from the supplier about written basis for contract, as well as regular settlement of accounts for services rendered by the ISP supplier.</li> </ul>	<p>During our test, we did not identify any material deviations.</p>
<p>Adequate procedures for managing threats in the form of attacks from the internet (cyber-attacks) must be implemented.</p> <p>In this connection, tools for managing the contingency approach in the event of a cyber-attack must be devised.</p>	<ul style="list-style-type: none"> <li>• We have controlled that an adequate number of procedures with accompanying contingency plans regarding managing threats in relation to cyber-attacks are implemented.</li> </ul> <p>We have by inspection on a test basis ensured</p> <ul style="list-style-type: none"> <li>• that appropriate framework for managing cyber-attacks are devised.</li> <li>• that plans for managing the threat are devised and implemented.</li> <li>• that the plans include cross-organisational collaboration between internal employee and groups.</li> </ul>	<p>During our test, we did not identify any material deviations.</p>

CONTROL OBJECTIVE 15:

## Supplier Security

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

Frontsafe A/S' control procedures	Auditor's test of control procedures	Test findings
Risks related to external business partners are identified, and security in third-party agreements and security in relation to customers are managed.	<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>	During our test, we did not identify any material deviations.
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 recognised suppliers are used.	<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>	During our test, we did not identify any material deviations.
Monitoring must be conducted regularly, including supervision of external business partners.	<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>	During our test, we did not identify any material deviations.

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.

Frontsafe A/S' control procedures	Auditor's test of control procedures	Test findings
<p>Security incidents are reported to Management as soon as possible, and the managing is performed in a consistent and efficient way.</p>	<p>We have asked Management whether procedures have been established for reporting of security incidents.</p> <p>We have verified that procedures and business procedures have been developed for reporting and managing 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 managing critical incidents is clearly delegated and that the related business procedures ensure that security breaches are managed expediently, efficiently and methodically.</p>	<p>During our test, we did not identify any material deviations.</p>

CONTROL OBJECTIVE 17:

## Information Security Aspects of Business Continuity Management

Business continuity management must 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.

Frontsafe A/S' control procedures	Auditor's test of control procedures	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 Frontsafe A/S' Cloud Backup.</p> <p>By inspection on a test basis, we have verified</p> <ul style="list-style-type: none"> <li>• that appropriate framework for preparation of business continuity management has been established</li> <li>• that contingency plans are prepared and implemented</li> <li>• that the plans include business continuity management across the organisation</li> <li>• that the plans include appropriate strategy and procedures for communication with the interested parties of Frontsafe A/S.</li> <li>• that contingency plans are tested on a regular basis</li> <li>• that maintenance and reassessment of the total basis for business continuity management is undertaken on a regular basis.</li> </ul>	<p>During our test, we did not identify any material deviations.</p>