www.pwc.dk

B4Restore A/S

Independent service auditor's ISAE 3000 assurance report on IT general controls during the period from 1 January 2023 to 31 December 2023 in relation to B4Restore A/S's Backup as a Service (BaaS) and Storage as a Service (StaaS) to customers

February 2024

Contents

1 Management's statement

The accompanying description has been prepared for B4Restore A/S's customers who have used Backup as a Service (BaaS) and Storage as a Service (StaaS) and who have a sufficient understanding to consider the description, along with other information, including information about controls operated by customers themselves, when assessing the risks of material misstatements.

B4Restore A/S uses GlobalConnect A/S as a subservice supplier for housing services. This report uses the carve-out method and does not comprise control objectives and related controls that GlobalConnect A/S performs for B4Restore A/S.

Some of the control objectives stated in our description in section 3 can only be achieved if the complementary controls at the customers are suitably designed and operating effectively with our controls. This report does not comprise the suitability of the design and operating effectiveness of these complementary controls.

B4Restore A/S confirms that:

a) The accompanying description in section 3 fairly presents the IT general controls for Backup as a Service (BaaS) and Storage as a Service (StaaS) used by B4Restore's customers throughout the period from 1 January 2023 to 31 December 2023. The criteria used in making this statement were that the accompanying description:

   (i) Presents how IT general controls in relation to Backup as a Service (BaaS) and Storage as a Service (StaaS) were designed and implemented, including:

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

   (ii) Includes relevant details of changes to IT general controls in relation to Backup as a Service (BaaS) and Storage as a Service (StaaS) during the period from 1 January 2023 to 31 December 2023

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

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 January 2023 to 31 December 2023. The criteria used in making this statement were that:

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

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

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 January 2023 to 31 December 2023.

Aarhus, 8 February 2024
B4Restore A/S

Henrik Lind
CEO

Jørgen Pedersen
COO/CISO

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

Independent service auditor's ISAE 3000 assurance report on IT general controls during the period from 1 January 2023 to 31 December 2023 in relation to B4Restore A/S's Backup as a Service (BaaS) and Storage as a Service (StaaS) to customers

To: B4Restore A/S and B4Restore A/S's customers who have used Backup as a Service (BaaS) and Storage as a Service (StaaS)

Scope

We have been engaged to provide assurance about B4Restore A/S's description in section 3 of its IT general controls in relation to Backup as a Service (BaaS) and Storage as a Service (StaaS) throughout the period from 1 January 2023 to 31 December 2023 and about the design and operating effectiveness of controls related to the control objectives stated in the description.

B4Restore A/S uses GlobalConnect A/S as a subservice supplier for housing services. This report uses the carve-out method and does not comprise control objectives and related controls that GlobalConnect A/S performs for B4Restore A/S.

Some of the control objectives stated in B4Restore A/S's description in section 3 can only be achieved if the complementary controls at the customers are suitably designed and operating effectively with B4Restore A/S's controls. This report does not comprise the suitability of the design and operating effectiveness of these complementary controls.

We express reasonable assurance in our conclusion.

B4Restore A/S's responsibilities

B4Restore A/S is responsible for: preparing the description and accompanying statement in section 1, including the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives and designing and effectively operating controls to achieve the stated control objectives.

Service auditor's independence and quality control

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

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

Service auditor's responsibilities

Our responsibility is to express an opinion on B4Restore A/S's description and on the design and operating effectiveness of controls related to the control objectives stated in that description, based on our procedures.

We conducted our engagement in accordance with ISAE 3000, "Assurance engagements other than audits or reviews of historical financial information", and additional requirements applicable in Denmark to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its Backup as a Service (BaaS) and Storage as a Service (StaaS) and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgement, including the assessment of risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures 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 by B4Restore A/S in the Management's statement section.

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

Limitations of controls at a service organisation

B4Restore A/S's description is prepared to meet the common needs of a broad range of customers and may not, therefore, include every aspect of Backup as a Service (BaaS) and Storage as a Service (StaaS) that the individual customer may consider important in its particular circumstances. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions. Furthermore, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organisation may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in the Management's statement section. In our opinion, in all material respects:

a) The description fairly presents how IT general controls in relation to Backup as a Service (BaaS) and Storage as a Service (StaaS) were designed and implemented throughout the period from 1 January 2023 to 31 December 2023;

b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 January 2023 to 31 December 2023; and

c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 January 2023 to 31 December 2023.

Description of test of controls

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

Intended users and purpose

This report and the description of tests of controls in section 4 are intended only for customers who have used B4Restore A/S's Backup as a Service (BaaS) and Storage as a Service (StaaS) and who have a sufficient understanding to consider it along with other information, including information about controls operated by the customers themselves, in assessing the risk of using B4Restore A/S's Backup as a Service (BaaS) and Storage as a Service (StaaS).

Aarhus, 8 February 2024
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

Rico Lundager
Senior Manager

3 Description of IT general controls related to operation, monitoring, maintenance, support, etc. of B4Restore A/S's Backup as a Service (BaaS) and Storage as a Service (StaaS)

3.1 Introduction

B4Restore A/S (hereinafter B4Restore) delivers Backup as a Service (BaaS) and Storage as a Service (StaaS) to its customers through its operations, monitoring, support and maintenance located at B4Restore or at the customer's own location, to which this description, including assurance report, relates. We deliver enterprise-class performance and employ a professional staff of dedicated specialists within architecture, development, operations and quality assurance.

For Backup as a Service (BaaS) customers, B4Restore offers Business Continuity as a Service (BCaaS) as an add-on service to Backup as a Service (BaaS), which provides organisations with the ability to recover their data and maintain business continuity in the event of a disaster or other disruption.

B4Restore's work in relation to the IT general controls is based on risk assessment and ISO 27001:2013 "Information Technology – Security Techniques – Information security management systems – Requirements" as well as agreement between B4Restore and the customer as described in the operating agreement and accompanying appendices.

This description and assurance report cover the period from 1 January 2023 to 31 December 2023 and is intended for B4Restore Backup as a Service (BaaS) and Storage as a Service (StaaS) customers.

The description, statement and assurance report cover our storage and backup services delivered to customers in their own dedicated storage and/or backup environments or on the B4Restore Backup as a Service (BaaS) and Storage as a Service (StaaS) located in Viby, Denmark, and Skanderborg, Denmark.

B4Restore generally manages the following IT services and tasks for its storage and backup customers:

- Backup of individual customer IT solutions based on hybrid or dedicated storage and backup services as well as environments. Backup of individual customer IT environments takes place from IT data centres in Viby, Skanderborg, or at the customer's own location. The backup device is owned either by B4Restore or by the customer itself.

- Backup monitoring.

- Support of customers' backup and storage solutions, including various error corrections.

B4Restore is responsible for ensuring the implementation and operating effectiveness of control systems in order to prevent and detect errors, including deliberate errors, with the aim of complying with the requirements set out in the operating agreement.

This assurance report has been prepared in accordance with the carve-out method and does not include control objectives and related controls at our subcontractor GlobalConnect A/S (hereinafter GlobalCon-

nect). B4Restore has regular meetings with key subcontractors and retrieves annually an independent auditor's assurance report on selected controls, where relevant. As part of our work, we have tested specific controls regarding GlobalConnect to gain comfort on controls performed by them. If not possible for us to test, we have obtained a management statement from Management at GlobalConnect to ensure that a sufficient control environment has been maintained during the period in scope.

Storage and backup environments located at the customer are not covered in this assurance report.

3.2 Risk management

B4Restore manages and controls IT environments, including storage and backup environments, based on a risk management process. Risk management includes the following:

- Identification of potential risks that can affect the IT environments, both from a technical and business point of view
- Assessment of the identified potential risks, significance, likelihood and consequences in the IT environments
- Measures to reduce the likelihood of risks in a cost-effective manner.

Once a year, a risk assessment is carried out as well as when major organisational and/or technical changes occur. This contributes to ensuring that B4Restore complies with high standards, best practise, collaborative risk assessment and Service Level Agreements review, with particular focus to ensure that IT environments support high confidentiality, integrity and availability of storage and backup environments and solutions.

Based on the risk assessment, an information security policy has been prepared and implemented with the accompanying information security procedures and guidelines.

Risks are classified and documented.

Regular acceptance or implementation of risk mitigation activities or measures are carried out. These issues are regularly reported to the Executive Management.

3.3 Information security framework and management system

B4Restore has chosen to apply ISO/IEC 27001:2013 (hereinafter ISO 27001) and ISO/IEC 27002:2013 (hereinafter ISO 27002) as information security framework. B4Restore has established its information security management system (ISMS) according to ISO 27001. The ISMS has been ISO 27001-certified since 2015. B4Restore uses ISO 27002 as a reference framework for the Statement of Applicability (SOA) in ISO 27001 Certification and operationalisation of the ISMS. Thus, in the SOA of ISO 27002, implementation of relevant security mechanisms and measures for the following areas has been decided:

5. Information security policies
6. Organisation of information security
7. Human resource security
8. Asset management
9. Access control
11. Physical and environmental security
12. Operation security
13. Communication security
14. System acquisition, development and maintenance
15. Supplier relationships
16. Information security incident management
17. Business continuity management

18. Compliance.

The areas have been selected based on the service and tasks for which B4Restore is responsible for the individual customer as described in the operating agreement with accompanying appendices as well as in the information security policy, procedures and guidelines.

A more detailed description of implemented measures is found in B4Restore's Information Security Manual Version 5.0, in section 4 on the description of our control objectives and related controls as well as in the auditor's description of the test of controls for this assurance report.

During the last years, B4Restore has continuously worked on improving the information security. This has resulted in B4Restore having made necessary improvements and adjustments to a number of essential procedures and guidelines according to ISO 27001 and/or ITIL. This work has been demonstrated by the fact that B4Restore received its ISO 27001 certificate from DNV-GL Business Assurance on 8 July 2015. The certificate covers B4Restore's Information Security of Managed Services (Backup and Storage). In 2018, B4Restore was re-certified in accordance with SOA 4.0 according to ISO 27001, and in 2021, B4Restore was re-certified again, this time by Bureau Veritas, in accordance with SOA 7.0 according to ISO 27001. The certificate is valid from 7 July 2021 to 8 July 2024. In 2023, internal and external audits have been conducted for B4Restore's information security management system. The external audit had no deviation, a few observations and improvement points.

B4Restore continues to work with continuous improvements in the information security management system.

Based on the risk assessment, B4Restore has taken a position on:

- Control objectives that are relevant for managing the security
- Risks that threaten the achievement of control objectives
- Controls making it possible to mitigate risks.

Control objectives and related controls that mitigate risks are selected from ISO 27002 and applied to the extent required. The adjustment has primarily been a clarification of controls, which are presented in the standard as guidelines and not actual controls where operating effectiveness can be assessed. In the auditor's section of results of test of controls, section 4, a description of control objectives and related controls can be found. For the individual controls, the same numbering as in ISO 27002 has been used. Selection of control objectives and associated risk mitigation have been based on recommendations from the FSR Cyber Security Committee and our independent auditor.

3.4 Significant changes in IT environments

In 2023, the following significant changes have been made:

- Regular updating and maintenance of systems and procedures.

3.5 Complementary controls at the customers

See section 5 "Additional information from B4Restore".

3.6 Controls and implemented measures from ISO/IEC 27002:2013

A more detailed description of implemented measures appears in section 4 on the description of our control objectives and related controls as well as the auditor's description of the test of controls for this assurance report.

4 Control objectives, control activity, tests and test results

4.1 Purpose and scope

We conducted our engagement in accordance with ISAE 3000, "Assurance engagements other than audits or reviews of historical financial information", and additional requirements applicable in Denmark.

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

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

4.2 Test actions

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

Inspection	Reading of documents and reports containing specifications regarding the execution of the control. This includes reading and consideration of reports and other documentation in order to assess whether specific controls are designed so they may be expected to become effective if implemented. Furthermore, it is assessed whether controls are being monitored and checked sufficiently and at appropriate intervals.
Inquiries	Inquiry of appropriate personnel. Inquiries have included how the controls are performed.
Observation	We have observed the execution of the control.
Reperformance of the control	Repetition of the relevant control. We have repeated the execution of the control to verify whether the control functions as assumed.

4.3 Control objectives, control activity, tests and test results

5. Security policy

Control objective: *An information security framework and policy are established to ensure that:*

- *an updated and management-approved information security policy has been prepared*
- *an information security manual has been prepared*
- *Management is involved in information security work.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
5.1.1	**Policies for information security** Management has developed and prepared an information security manual that contains relevant security areas and measures from ISO 27002.	We have inspected that the information security procedures and guidelines cover relevant areas from ISO 27002 as described in Management's description of its system. We have observed that new employees are educated in information security and are informed that they are instructed to read the information security manual.	No exceptions noted.
5.1.2	**Review of the policies for information security** Management approves the information security policy which is available and communicated to the employees and relevant external parties. The information security policy is reviewed yearly or in case of material changes to ensure its continued relevance and effectiveness.	We have observed that the information security policy is updated. We have observed that the CEO has approved the information security policy.	No exceptions noted.

6. Organisation of information security

Control objective: *Sufficient controls are designed and implemented to ensure that:*

- *information security is managed in the company*
- *security requirements are reflected in contractual commitments and expectations with customers*
- *written agreements have been concluded with relevant suppliers.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
6.1.1	**Information security roles and responsibilities** Management supports active security by showing direction, commitment, precise task allocation and recognition of information security responsibilities. Security tasks and responsibilities are determined in accordance with the company's guidelines and information security policy. Information security activities are coordinated across the company. Responsibility for all information security activities, including protection of the company's information assets and the execution of specific security procedures, is formally defined.	We have inquired of Management about how they actively support security (including setting direction, goals), are engaged, delegate and are accountable for information security. We have inquired of Management about its assignments and responsibility with regards to information security. We have inquired of Management about how security activities are coordinated across the company. We have observed information distributed regarding information security.	No exceptions noted.
6.1.2	**Segregation of duties** Segregation of duties is an organisational control to minimise the risk of erroneous or fraudulent abuse of systems. Segregation of duties is established to minimise the risk of unauthorised or unintended changes or abuse of the company's information assets. Due to the size of B4Restore, it cannot ensure a complete segregation of duties of all critical features.	We have observed that networks are segregated and jump hosts are utilised when connecting to client networks. We have inspected that segregation of duties is addressed in the information security manual. We have inspected that employees have job descriptions which describe their responsibilities.	No exceptions noted.

6. Organisation of information security

Control objective: *Sufficient controls are designed and implemented to ensure that:*

- *information security is managed in the company*
- *security requirements are reflected in contractual commitments and expectations with customers*
- *written agreements have been concluded with relevant suppliers.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
6.1.3	**Contact with authorities** B4Restore has a procedure in case of breach of personal data security. Review is made to the supervisory authority. The nature of the breach, the nature of the breach of personal data security, consequences and remedial actions must be described. In case of a breach, relevant evidence will be collected.	We have inspected that formal procedures for securing evidence and contacting authorities are implemented and available to employees.	No exceptions noted.
6.1.5	**Information security in project management** Information security is integrated into the organisation's project management model. To ensure that information security risks are identified an information security risk assessment is conducted at an early stage of the project to identify necessary controls.	We have inspected that information security aspects are part of the project model including risk assessments. Furthermore, we have inspected a risk assessment on a single project.	No exceptions noted.
6.2.1	**Mobile device policy** Mobile phones connected to the company mail server have password protection enforced.	We have inquired of Management about security on mobile devices. We have inspected that mobile device security is addressed in the security manual.	No exceptions noted.

7. Human resource security

Control objective: *Sufficient controls have been established to ensure that all employees are aware of their particular responsibilities in relation to the company's information security, thereby minimising the risk of human error, fraud and misuse of information assets.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
7.1.1	**Screening** Before recruiting employees, the following background check is made: • A personal reference • The applicant's CV • Education and professional qualifications • Identity control. Where applicable, the candidate must show a criminal record.	We have inquired of Management about background checks and checks of criminal records. We have inspected that the procedure for appointment and termination covers relevant areas. By inspection of a sample of employees, we have ascertained that background checks are performed.	No exceptions noted.
7.1.2	**Terms and conditions of employment** As part of the agreement with both permanent and temporary employees, a contract is signed which describes the company's and employee's responsibilities and obligations regarding information security.	We have inquired of the person responsible for HR about the procedures for non-disclosure agreements. We have inspected a sample of an employee's contract in which the employee's secrecy is stated	No exceptions noted.
7.2.1	**Management responsibilities** Management ensures that all employees are educated in and work in accordance with the company's security policies, guidelines and procedures.	We have inquired of Management about how Management assures that the employees follow the information security policy.	No exceptions noted.
7.2.2	**Information security awareness, education and training** Awareness and training in information security policies and procedures are continuously provided to employees.	We have inspected that information security topics are addressed at department meetings. We have inspected that employees are required to complete mandatory awareness training.	No exceptions noted.

7. Human resource security

Control objective: *Sufficient controls have been established to ensure that all employees are aware of their particular responsibilities in relation to the company's information security, thereby minimising the risk of human error, fraud and misuse of information assets.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
7.2.3	**Disciplinary process** Management ensures that proper disciplinary action is taken when employees violate B4Restore's policies, guidelines or procedures. Actions are consistent and in accordance with applicable legislation.	We have inquired of Management about how disciplinary action is taken. We have inquired of Management if any disciplinary action has been taken against employees for violating B4Restore's policies. We have inspected the policy for disciplinary process.	No exceptions noted.
7.3.1	**Termination or change of employment responsibilities** In connection with termination of the employment relationship, it is ensured that confidentiality is maintained, assets are returned and access rights are removed.	We have inquired of Management about procedures and controls at employees' termination. We have inspected controls for employees terminated in 2023	No exceptions noted.

8. Asset management

Control objective: *Sufficient controls are designed and implemented to ensure proper protection of assets.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
8.1.1	**Inventory of assets** All critical information assets are identified, and an updated inventory of all significant assets has been established.	We have observed that procedures cover asset management. We have inspected a sample of assets registration in the asset management system.	No exceptions noted.
8.3.1	**Management of removable media** Secret and confidential information is secured with passwords when stored or transported on portable media bounded to PCs and mobile phones.	We have inquired of Management about security on PCs and mobile phones. We have inspected that the information security manual contains policies for passwords on removable media. We have inspected password policies on Windows Active Directory.	No exceptions noted.
8.3.2	**Disposal of media** All data media must be securely disposed of or physically destroyed before disposal if they contain information classified as secret or confidential.	We have inquired of Management about procedures for disposal of media containing classified information. We have inspected procedures for disposal of IT equipment. We have observed that a waste bin for confidential documents and media exists. We have inspected documentation showing that media are physically destroyed.	No exceptions noted.
8.3.3	**Physical media transfer** Data media containing information are protected against loss, corruption and misuse during transportation. Transportation of data media by external parties is carried out by an authorised carrier. The carrier must be insured for the current physical media.	We have inquired of Management about transfer of physical media. We have inspected that policies require transfers to be done by an authorised carrier and that the carrier must be insured. We have observed that an authorised carrier is used for transportation of data media and that the carrier is insured.	No exceptions noted.

9. Access control

Control objective: *Sufficient controls have been established to ensure that access to systems, data and networks is governed in accordance with business and regulatory requirements.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
9.1.1	**Access control policy** Guidelines are established for granting access rights.	We have inquired of Management about how granting of access rights is performed. We have inspected procedures for user access administration.	No exceptions noted.
9.2.1	**User registration and de-registration** There is a procedure for granting and revoking user access.	We have inquired of Management about how granting of access rights is performed. We have inspected procedures for user access administration.	No exceptions noted.
9.2.2	**User access provisioning** There is a procedure for provisioning access to users. Access to systems is approved by Management in a ticket system.	We have inquired of Management about how granting of access rights is performed. We have inspected procedures for user access administration. We have checked by way of inspection that access for new users is approved.	No exceptions noted.
9.2.3	**Management of privileged access rights** Granting and use of privileged access rights are limited and monitored.	We have inquired of Management about how granting of access rights is performed. By way of inspection, we have checked access rights to Spectrum Protect (Linux/AIX/Windows), Veeam and ServiceNow.	No exceptions noted.
9.2.5	**Review of user access rights** User access rights are reviewed regularly.	We have inspected procedures for review of access rights. We have inspected that periodic review of administrative access rights is performed.	No exceptions noted.

9. Access control

Control objective: *Sufficient controls have been established to ensure that access to systems, data and networks is governed in accordance with business and regulatory requirements.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
9.2.6	**Removal or adjustment of access rights** All employees' access rights are removed at termination of employment.	We have inspected a list of terminated employees in 2023. We have inspected that access rights for terminated employees in 2023 have been removed.	No exceptions noted.
9.3.1	**Use of secret authentication information** Formal procedures are in place for granting passwords. Guidelines for user passwords follow best practice. Users have a unique user ID, and proper authentication is used for verification of the user's identity.	We have inquired about how passwords are granted. We have inspected the password quality on a sample of servers. We have inspected a sample of servers' users and ensured they have a unique user ID.	No exceptions noted.
9.4.2	**Secure log-on procedures** Access to network and systems is protected by a secure log-on procedure.	We have observed procedures for log-on.	No exceptions noted.
9.4.3	**Password management system** Interactive systems for managing passwords ensure that only passwords of the right quality are used.	We have inquired of Management about how the administration of password quality is managed. We have inspected work instructions for the password management system.	No exceptions noted.

11. Physical and environmental security – Viby

Control objective: *Sufficient controls are designed and implemented to ensure that:*

- *information assets are protected against unauthorised physical access, damage and interference*
- *critical information processing equipment and storage media are located in secure areas protected by necessary barriers and access controls*
- *equipment is protected against physical threats*
- *necessary supplies of electricity and sufficient ventilation and cable installations are provided.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
11.1.1	**Physical security perimeter** Physical security for areas for information processing equipment and storage media is designed and applied.	We have inspected processing facilities where storage and backup equipment is located at B4Restore.	No exceptions noted.
11.1.2	**Physical entry controls** Secure areas are protected with proper entry controls so only authorised persons can access.	We have observed that access cards with personal codes are used to get access to the processing facilities. We have had the list of employees with access to the facilities confirmed.	No exceptions noted.
11.1.4	**Protection against external and environmental threats** Physical security has been designed and applied to minimise damage from fire, floods, earthquakes, civilian riots, explosions, terrorism and other forms of natural or man-made threats.	We have inspected areas where storage and backup equipment is located at B4Restore to ensure that there are fire alarms and fire extinguishers as well as cooling and UPS.	No exceptions noted.
11.1.6	**Delivery and loading areas** Delivery and loading areas and other areas with public access are controlled.	We have observed that there is no public access to areas where storage and backup equipment is located and that the area is monitored.	No exceptions noted.
11.2.1	**Equipment siting and protection** Equipment is sited and protected to reduce the risks from environmental threats and hazards and unauthorised access. Data rooms where backup equipment is sited are protected against static electricity by installing copper wire in the floor and grounding them.	We have inspected areas where storage and backup equipment is located at B4Restore to ensure that entry controls are designed and applied. We have inquired if areas where storage and backup equipment is located at B4Restore are protected against static electricity.	No exceptions noted.

11. Physical and environmental security – Viby

Control objective: *Sufficient controls are designed and implemented to ensure that:*

- *information assets are protected against unauthorised physical access, damage and interference*
- *critical information processing equipment and storage media are located in secure areas protected by necessary barriers and access controls*
- *equipment is protected against physical threats*
- *necessary supplies of electricity and sufficient ventilation and cable installations are provided.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
11.2.2	**Supporting utilities** Equipment is protected against supply failure according to how critical the equipment is for the solution.	We have inspected areas where storage and backup equipment is located at B4Restore to ensure UPS is installed. We have inspected that yearly service is maintained for the UPS.	No exceptions noted.
11.2.3	**Cabling security** Cables for electricity and data communication are protected against interception, damage and interference.	We have inspected areas where storage and backup equipment is located at B4Restore to ensure cables to electricity and data communication are secure.	No exceptions noted.
11.2.4	**Equipment maintenance** Equipment is maintained to ensure its continued availability and integrity.	We have inquired about maintenance procedures for equipment. We have inspected service agreements for UPS, servers, cooling equipment, tape libraries and storage equipment.	No exceptions noted.
11.2.5	**Removal of assets** Removal off-site of equipment and other assets needs proper authorisation.	We have inquired of Management about the procedures for removal off-site of equipment. We have inspected that formal procedures are in place.	No exceptions noted.
11.2.7	**Secure disposal or re-use of equipment** All equipment with storage media is verified to ensure that any critical/sensitive information and licensed systems are removed or overwritten when disposed of or re-used.	We have inquired about procedures for disposal of tapes. We have inquired about procedures for re-use of discs.	No exceptions noted.

11. Physical and environmental security – GlobalConnect

Control objective: *Sufficient controls are designed and implemented to ensure that:*

- *information assets are protected against unauthorised physical access, damage and interference*
- *critical information processing equipment and storage media are located in secure areas protected by necessary barriers and access controls*
- *equipment is protected against physical threats*
- *necessary supplies of electricity and sufficient ventilation and cable installations are provided.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
11.1.1	**Physical security perimeter** Physical security for areas for information processing equipment and storage media is designed and applied.	We have inspected B4Restore's primary processing facilities. We have received Management's statement from GlobalConnect stating that controls related to data centres were effective throughout 2023.	No exceptions noted.
11.1.2	**Physical entry controls** Secure areas are protected with proper entry controls so only authorised persons can access.	We have observed that access cards with personal codes are used to get access to the primary processing facilities. We have inspected who has access to the primary processing facilities. We have received Management's statement from GlobalConnect stating that controls related to data centres were effective throughout 2023.	No exceptions noted.
11.1.4	**Protection against external and environmental threats** Physical security has been designed and applied to minimise damage from fire, floods, earthquakes, civilian riots, explosions, terrorism and other forms of natural or man-made threats.	We have inspected B4Restore's primary processing facilities to ensure that there are fire alarms and fire extinguishers as well as cooling and UPS. We have received Management's statement from GlobalConnect stating that controls related to data centres were effective throughout 2023.	No exceptions noted.
11.1.6	**Delivery and loading areas** Delivery and loading areas and other areas with public access are controlled.	We have observed that there is no public access to primary processing facilities and that the area is monitored. We have received Management's statement from GlobalConnect stating that controls related to data centres were effective throughout 2023.	No exceptions noted.

11. Physical and environmental security – GlobalConnect

Control objective: *Sufficient controls are designed and implemented to ensure that:*

- *information assets are protected against unauthorised physical access, damage and interference*
- *critical information processing equipment and storage media are located in secure areas protected by necessary barriers and access controls*
- *equipment is protected against physical threats*
- *necessary supplies of electricity and sufficient ventilation and cable installations are provided.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
11.2.1	**Equipment siting and protection** Equipment is sited and protected to reduce the risks from environmental threats and hazards and unauthorised access.	We have inspected B4Restore's primary processing facilities to ensure that entry controls are designed and applied. We have received Management's statement from GlobalConnect stating that controls related to data centres were effective throughout 2023.	No exceptions noted.
11.2.2	**Supporting utilities** Equipment is protected against supply failure according to how critical the equipment is for the solution. UPS and generator are tested monthly.	We have inspected B4Restore's primary processing facilities to ensure UPS and generator are installed. We have received Management's statement from GlobalConnect stating that controls related to data centres were effective throughout 2023.	No exceptions noted.
11.2.3	**Cabling security** Cables for electricity and data communication are protected against interception, damage and interference.	We have inspected whether cables to electricity and data communication are secure. We have received Management's statement from GlobalConnect stating that controls related to data centres were effective throughout 2023.	No exceptions noted.
11.2.4	**Equipment maintenance** Equipment is maintained to ensure its continued availability and integrity.	We have inquired about maintenance procedures for equipment. We have inspected the service agreement for UPS, servers, cooling equipment, tape libraries and storage equipment. We have received Management's statement from GlobalConnect stating that controls related to data centres were effective throughout 2023.	No exceptions noted.

11. Physical and environmental security – GlobalConnect

Control objective: *Sufficient controls are designed and implemented to ensure that:*

- *information assets are protected against unauthorised physical access, damage and interference*
- *critical information processing equipment and storage media are located in secure areas protected by necessary barriers and access controls*
- *equipment is protected against physical threats*
- *necessary supplies of electricity and sufficient ventilation and cable installations are provided.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
11.2.5	**Removal of assets** Removal off-site of equipment and other assets needs proper authorisation.	We have inquired of Management about the procedures for removal off-site of equipment. We have inspected that formal procedures are in place. We have received Management's statement from GlobalConnect stating that controls related to data centres were effective throughout 2023.	No exceptions noted.
11.2.6	**Security of equipment and assets off-premises** Equipment and assets off-premises are well-secured.	We have inspected B4Restore's primary processing facilities to ensure equipment is well-secured. We have received Management's statement from GlobalConnect stating that controls related to data centres were effective throughout 2023.	No exceptions noted.
11.2.7	**Secure disposal or re-use of equipment** All equipment with storage media is verified to ensure that any critical/sensitive information and licensed systems are removed or overwritten when disposed of or re-used.	We have inquired about procedures for disposal of tapes. We have inquired about procedures for re-use of discs. We have received Management's statement from GlobalConnect stating that controls related to data centres were effective throughout 2023.	No exceptions noted.

12. Operations security

Control objective: *Sufficient controls are designed and implemented to ensure:*

- *correct and secure operations of processing facilities*
- *that information and information processing facilities are protected against malware*
- *that systems and information are protected against loss of data*
- *that backup is stored securely and is readable.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
12.1.1	**Documented operating procedures** Operational procedures for business-critical systems are documented, updated and available to service operators and others with a work-related need.	We have inquired of a sample of employees about operational procedures. We have inspected B4Restore's operational procedures.	No exceptions noted.
12.1.2	**Change management** Changes to business-critical information processing equipment, systems and procedures are controlled through a formalised procedure.	We have inquired of a sample of employees about how change management is controlled. We have inspected change management procedures. We have inspected a sample of changes, to ensure they were performed according to procedures.	No exceptions noted.
12.1.3	**Capacity management** Performance is continuously monitored and tuned in order to ensure the required system performance.	We have inquired of Management about what action is taken in case of excessive load on system power, discs or tapes. We have inspected operational procedures for verification of adequate capacity compared with performance.	No exceptions noted.
12.1.4	**Separation of development, testing and operational environments** B4Restore does not have development activities. Test environments are segregated from production environments. Access from the test environment is reduced to a limited number of relevant infrastructure systems.	We have inquired of Management about policies and set-up of test and operational environments. We have inspected firewall rules that filter access from the test environment.	No exceptions noted.

12. Operations security

Control objective: *Sufficient controls are designed and implemented to ensure:*

- *correct and secure operations of processing facilities*
- *that information and information processing facilities are protected against malware*
- *that systems and information are protected against loss of data*
- *that backup is stored securely and is readable.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
12.2.1	**Controls against malware** B4Restore has implemented antivirus on relevant servers and equipment. The software is regularly updated.	We have inquired about procedures for antivirus. We have inquired of the COO about review of malware protection. We have inspected that updated antivirus software is installed on a sample of internal B4Restore servers.	No exceptions noted.
12.3.1	**Information backup** Backups are made of critical information assets, including of parameter settings and other critical documentation in accordance with established guidelines.	We have inquired of Management about backup procedures. We have observed backup monitoring in Wizard Storage Portal. We have inspected that daily status mails for internal backup are handled.	No exceptions noted.
12.4.1	**Event logging** Information processing systems are monitored continuously. Errors are logged and analysed, and necessary remedies and measures are taken.	We have observed how storage and backup processing is monitored. We have observed how erroneous or incomplete backup jobs are managed and resolved based on notifications in Wizard Storage Portal/Spectrum Protect or ServiceNow.	No exceptions noted.
12.4.2	**Protection of log information** Logging facilities and log information are protected against tampering and unauthorised access by using access control systems, physical separation and network segmentation.	We have inquired about how logging facilities and log information are protected against tampering or deletion. We have inspected who have access to log information.	No exceptions noted.
12.4.3	**Administrator and operator logs** Activities of system administrators and operators as well as others with special rights are logged.	We have inspected that system administrator and operator activities are logged.	No exceptions noted.

12. Operations security

Control objective: *Sufficient controls are designed and implemented to ensure:*

- *correct and secure operations of processing facilities*
- *that information and information processing facilities are protected against malware*
- *that systems and information are protected against loss of data*
- *that backup is stored securely and is readable.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
12.5.1	**Installation of software on operational systems** The COO should approve new programs and suppliers before users install them. Operating systems and applications may only be installed and modified after agreement with the COO. Browsers must be set up according to the security policy.	We have inquired of the COO about procedures for installation of system software on servers and PCs. We have inspected that procedures are formally described.	No exceptions noted.
12.6.1	**Management of technical vulnerabilities** The company regularly collects information about possible vulnerabilities in the systems. The vulnerabilities are evaluated, and appropriate measures are implemented to counteract the new risks. B4Restore regularly performs technical scans and reviews of malware protection. Windows updates are managed through Microsoft's Windows Update tool. Windows security-related updates are rolled out at the latest 30 days after publication.	We have inquired of Management about how vulnerabilities for the backup environment are collected and evaluated, and how related measures are implemented. We have inquired of a sample of employees about how vulnerabilities for the backup environment are collected and evaluated, and how related measures are implemented. We have inquired of the COO about the management of security-related Windows updates. We have observed that Spectrum Protect operates on a version supported by the vendor.	We have ascertained, that two Unix servers and one Windows server wasn't patched according to policy. We have ascertained, in January 2024, that the weaknesses was corrected. No further exceptions noted.
12.6.2	**Restrictions on software installation** In general, administrative rights are not granted to the workstations used at B4Restore. Dispensation is given only by the Executive Management.	We have observed how administrative access rights are limited.	No exceptions noted.

13. Communication security

Control objective: *Sufficient controls are designed and implemented to ensure protection of information in networks and in supporting information processing facilities.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
13.1.1	**Network controls** All servers and networks are protected against threats using a firewall. The COO must ensure that the necessary protection against unauthorised access has been implemented, including logging and monitoring. Physical and logical access to diagnostic and configuration ports is controlled.	We have inquired of a sample of employees about how port rules on firewalls are managed to ensure only allowed traffic is used on the network. We have inspected network documentation and network procedures. We have inspected the rule set of the firewall.	No exceptions noted.
13.1.2	**Security of network services** B4Restore has procedures for using network services.	We have inspected procedures for network services.	No exceptions noted.
13.1.3	**Segregation in networks** Segregation of the network is used to establish appropriate separation between different clients, services or systems.	We have inquired of Management about how the network is segmented. We have inspected network documentation and verified that network segregation is implemented.	No exceptions noted.
13.2.1	**Information transfer policies and procedures** B4Restore has procedures for transfer of data and connection using VPN.	We have inquired of Management about how data is transferred from customers. We have inquired of Management about how remote access (VPN) is used. We have observed the use of VPN to get access to customer sites.	No exceptions noted.
13.2.2	**Agreements on information transfer** Confidential information may not be disclosed to any third party in any form without permission from system and data owner. This is especially true for sensitive information as well as personally identifiable information given to the company.	We have inquired of Management about disclosure of confidential information to third party. We have inquired of Management about the procedures for non-disclosure agreements. We have inspected a sample of an employee's contract and verified that the employee's secrecy is stated.	No exceptions noted.

13. Communication security

Control objective: *Sufficient controls are designed and implemented to ensure protection of information in networks and in supporting information processing facilities.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
13.2.3	**Electronic messaging** B4Restore has procedures for electronic messaging.	We have inspected procedures for the use of electronic messaging.	No exceptions noted.
13.2.4	**Confidentiality or non-disclosure agreements** Procedures are in place for obtaining non-disclosure agreements which reflect B4Restore's needs to protect sensitive/confidential information.	We have inquired about procedures for obtaining non-disclosure agreements with Management. We have inspected a sample of non-disclosure agreements with suppliers.	No exceptions noted.

14. System acquisition, development and maintenance

Control objective: *Sufficient controls are designed and implemented to ensure that:*

- *security management is an integrated part of operating systems, infrastructure and services*
- *the requirements for security are identified and agreed before implementation of information processing systems*
- *system files in the operating environment are secured and protected.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
14.1.1	**Information security requirements analysis and specification** Acquisition and installation of new information processing equipment and systems follow a formal approval procedure.	We have inquired of Management about how system acquisition, development and maintenance are handled. We have inspected the procedure for major system upgrades and new systems.	No exceptions noted.
14.1.2	**Securing application services on public networks** Secure authentication and authorisation processes are used to ensure services over public networks.	We have inquired about how authentication and authorisation processes are used for services over public networks. We have inspected procedures for authentication and authorisation for services over public networks.	No exceptions noted.
14.2.2	**System change control procedures** Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures.	We have inquired of a sample of employees about how change management is controlled. We have inspected change management procedures. By inspection of a sample of changes, we have ascertained that changes are approved and tested prior to implementation.	No exceptions noted.
14.2.3	**Technical review of applications after operating platform changes** Larger and critical changes to systems in operation are properly managed, reviewed and tested. Changes in production environments are announced timely to ensure limited effect in the services, and contingency plans are updated in accordance with the changes.	We have inquired about how larger and critical changes in systems operation are managed and controlled. We have inspected a sample of changes to ensure they were performed according to procedures. We have inspected a sample of an announcement to a client.	No exceptions noted.

14. System acquisition, development and maintenance

Control objective: *Sufficient controls are designed and implemented to ensure that:*

- *security management is an integrated part of operating systems, infrastructure and services*
- *the requirements for security are identified and agreed before implementation of information processing systems*
- *system files in the operating environment are secured and protected.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
14.2.4	**Restrictions on changes to software packages** Only necessary changes to standard systems are made, and such changes are carefully managed and controlled.	We have inquired about how changes to standard systems are managed and controlled.	No exceptions noted.
14.2.8	**System security testing** Formal criteria for validation and approval are in place for new systems or versions and for updates of existing systems. Sufficient tests are performed as needed before they can be approved and put into operation.	We have inquired of Management about procedures for new systems or versions and for updates of existing systems. We have inspected policies for new systems or versions and for updates of existing systems.	No exceptions noted.

15. Supplier relationships

Control objective: *Sufficient controls are designed and implemented to ensure that:*

- *written agreements are made with relevant suppliers, indicating agreed level of information security*
- *company assets to which suppliers and subsuppliers have access are protected.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
15.1.1	**Information security policy for supplier relationships** Before cooperation with other parties that have access to information assets, a risk assessment is carried out, and relevant security measures are identified and implemented.	We have inquired about how other parties are risk-assessed before they get access to the storage and backup environment. We have inspected that risk assessments are executed on strategic suppliers.	No exceptions noted.
15.1.2	**Addressing security within supplier agreements** Supplier agreements are established with all significant suppliers to ensure that B4Restore's security objectives are not compromised.	We have inquired about how B4Restore ensures that suppliers follow B4Restore's security policy. We have inspected a sample of supplier agreements.	No exceptions noted.
15.2.1	**Monitoring and review of supplier services** A mutual service delivery agreement is made regarding the service level, for example through formal service level agreements (SLAs) as part of the signed operating agreement. B4Restore ensures that agreed security and control measures, services and service targets are established, delivered and maintained. B4Restore regularly monitors the service provider. This is done by reviewing agreed reports and performing actual audits to ensure compliance with the agreement and that security incidents and issues are handled satisfactorily. B4Restore has monthly reporting meetings with GlobalConnect which include status on information security.	We have inquired of Management about security and control measures in regard to suppliers, including GlobalConnect. We have inspected minutes from the monthly meeting with GlobalConnect and observed that information security status is addressed. We have inspected the housing agreement with GlobalConnect.	No exceptions noted.

15. Supplier relationships

Control objective: *Sufficient controls are designed and implemented to ensure that:*

- *written agreements are made with relevant suppliers, indicating agreed level of information security*
- *company assets to which suppliers and subsuppliers have access are protected.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
15.2.2	**Managing changes to supplier services** The COO ensures that change management of service provider services follows the same guidelines as B4Restore.	We have inquired about how change management of the suppliers is managed and controlled. We have inspected that changes handled by the supplier are handled within B4Restore's change management system.	No exceptions noted.

16. Information security incident management

Control objective: *Sufficient controls are designed and implemented to ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
16.1.1	**Responsibilities and procedures** Management responsibilities and necessary procedures are established to ensure a quick, effective and orderly response to information security incidents and breaches. An information security committee holds a monthly meeting addressing security matters.	We have inquired of Management about its responsibilities for managing security breaches. We have inquired of Management about the monthly information security forum meetings. We have inspected procedures for incident management.	No exceptions noted.
16.1.2	**Reporting information security events** Security incidents are reported to Management as soon as possible.	We have inquired of Management about how information on security incidents is obtained. We have inspected security incidents reported within the period.	No exceptions noted.
16.1.3	**Reporting information security weaknesses** All employees, collaborators and other users of systems and services are obliged to note and report any observed weaknesses or suspected weaknesses in systems and services.	We have inquired of a sample of employees about how security weaknesses are reported. We have inquired about how information and evidence regarding security weakness are obtained and managed.	No exceptions noted.
16.1.6	**Learning from information security incidents** B4Restore has a process that quantifies and monitors types, scope and costs of handling security breaches and avoiding repetitions.	We have inquired about how the process for monitoring security breaches is managed.	No exceptions noted.

17. Business continuity management

Control objective: *Sufficient controls are designed and implemented to ensure resilience against business interruptions, to protect critical business processes against the effects of major crashes of information systems as well as crisis or disasters, and to ensure timely recovery.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
17.1.1	**Planning information security continuity** A cross-organisational business continuity management process is established and maintained that addresses the information security requirements necessary for recovery of continued operation.	We have inquired of Management about business continuity management. We have inspected the business continuity management plan.	No exceptions noted.
17.1.2	**Implementing information security continuity** Plans for maintenance and recovery of business activities are prepared within the stipulated time frame after a disruption or failure of the critical business processes. Plans are updated annually.	We have inquired of Management about business continuity management. We have inspected the business continuity management plan. We have inspected that the business continuity plan is updated annually.	No exceptions noted.
17.1.3	**Verifying, reviewing and evaluating information security continuity** The disaster recovery plan and business continuity plan are tested and updated to ensure they are currently effective and include information security.	We have inquired of Management about test of business continuity. We have inspected the annual test of the business continuity management plan. We have inspected that lessons learned are captured and actions items established.	No exceptions noted.

18. Compliance

Control objective: *Sufficient controls are designed and implemented to avoid breaches of legal statutory, regulatory or contractual obligations and of any security requirement.*

No.	B4Restore's control activity	Tests performed by PwC	Result of PwC's tests
18.1.1	**Identification of applicable legislation and contractual requirements** B4Restore makes an annual assessment of the legal, regulatory and contractual requirements that apply to backup services. These requirements are identified and documented.	We have inquired of Management about which relevant legal statutory, regulatory or contractual obligations B4Restore has to comply with.	No exceptions noted.
18.2.1	**Independent review of information security** B4Restore's ISMS is ISO 27001-certified and is independently audited annually.	We have inquired of Management about B4Restore's ISO 27001 certification. We have observed that an annual independent audit has been executed in 2023.	No exceptions noted.

5 Additional information from B4Restore

The information included in this section is prepared by B4Restore to provide the customer with further information. The section should not be regarded as a part of the system description. The information in this section is not covered by audit procedures performed to assess whether the system description gives a true and fair view, whether the controls supporting the control objectives presented in section 4 have been suitably designed and whether they operated effectively throughout the period. Thus, PwC's conclusion in section 2 does not cover the information in section 5.

The individual customer is responsible for data transmission between B4Restore and the individual Spectrum Protect clients at the customer. It is thus the responsibility of the individual customer to ensure the controls in connection with this.

All user management, including the allocation of access rights and the protection of access through servers and equipment located at customer locations, is the responsibility of the customer. This also applies to Spectrum Protect-Backup clients. Customers thus need to control user administration.

Acquisition, development and implementation of systems on Spectrum Protect-Backup clients at customers are the customers' own responsibility. Controls related to system development, procurement and change management are also the responsibility of the customers.

The customers themselves are responsible for physical and environmental security of storage and backup devices located elsewhere than at B4Restore's data centre in Skanderborg or Viby.

B4Restore's Spectrum Protect solution supports IBM's encryption facility in a Spectrum Protect environment. Customers are responsible for setting up encryption on individual Spectrum Protect clients.

Controls related to emergency plans and contingency plans of customer backup services, including Spectrum Protect-Backup clients and associated server as well as restore and regular backup controls, are the responsibility of the customers.

As a controller and responsible of its own IT environment, the individual customer must enter into a contract with B4Restore as a processor to ensure that B4Restore acts only on instructions from the individual customer and that B4Restore takes all necessary technical and organisational security mechanisms and measures to process personal data and business-critical information.

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

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

Jørgen Pedersen
COO/CISO
På vegne af: B4Restore A/S
Serienummer: be0b4b32-eabf-4605-bffd-f9ef6835126a
IP: 212.98.xxx.xxx
2024-02-08 10:25:33 UTC

Henrik Lind
CEO
På vegne af: B4Restore A/S
Serienummer: 016d91cc-e102-40e6-8079-7e9c019c673c
IP: 212.98.xxx.xxx
2024-02-08 10:56:36 UTC

Rico Lundager
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Senior manager
På vegne af: Pricewaterhousecoopers Statsautoriseret…
Serienummer: 2e75390a-f48a-4123-b26c-3fd3e97823aa
IP: 83.136.xxx.xxx
2024-02-08 11:26:29 UTC

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
På vegne af: Pricewaterhousecoopers Statsautoriseret…
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 80.62.xxx.xxx
2024-02-08 11:28:40 UTC