Rackhosting ApS

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 May 2025 to 30 April 2026 in relation to Rackhosting ApS's general services to customers

July 2026

Contents

1. Management's assertion

The accompanying description has been prepared by Rackhosting ApS (Rackhosting) for customers who have used the general services and their auditors who have a sufficient understanding to consider the description, along with other information, including information about controls operated by the customers themselves, when assessing the risks of material misstatements in their financial statements.

Global Connect and Cibicom A/S are service organisations that provides data centre and network to Rackhosting. This report uses the carve-out method, and the description in section 3 includes only the control objectives and related controls of Rackhosting and excludes the control objectives and related controls of Global Connect and Cibicom A/S. Our evaluation did not extend to controls of Global Connect and Cibicom A/S.

The description indicates that certain control objectives specified in the description can be achieved only if complementary customer controls contemplated in the design of our controls are suitably designed and operating effectively. This report does not comprise the suitability of the design or operating effectiveness of such complementary user entity controls.

Rackhosting confirms that:

a) The accompanying description in section 3 fairly presents the general services that have processed customers' transactions throughout the period from 1 May 2025 to 30 April 2026. The criteria used in making this statement were that the accompanying description:

   (i) Presents how IT general controls in relation to the general services 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 the general services, 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 IT general controls

   (ii) Includes relevant details of changes to IT general controls in relation to the general services during the period from 1 May 2025 to 30 April 2026

   (iii) Does not omit or distort information relevant to the scope of IT general controls in relation to the general services being described, while acknowledging that the description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of IT general controls in relation to the general services 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 May 2025 to 30 April 2026. The criteria used in making this statement were that:

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

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

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 May 2025 to 30 April 2026.

Taastrup, 8 July 2026
Rackhosting ApS

Martin Helms
CEO

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

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 May 2025 to 30 April 2026 in relation to Rackhosting's general services to customers

To: Rackhosting ApS (Rackhosting), its customers and their auditors

Scope

We have been engaged to report on Rackhosting's description in section 3 of IT general controls in relation to the general services which have processed customers' transactions throughout the period from 1 May 2025 to 30 April 2026 (the description) and on the suitability of the design and operating effectiveness of controls related to the control objectives stated in the description.

Global Connect and Cibicom A/S are service organisations that provides data centre and network to Rackhosting. This report uses the carve-out method, and the description in section 3 includes only the control objectives and related controls of Rackhosting and excludes the control objectives and related controls of Global Connect and Cibicom A/S. Our examination did not extend to controls of Global Connect and Cibicom A/S.

The description indicates that certain control objectives specified in the description can be achieved only if complementary customer controls contemplated in the design of Rackhosting's controls are suitably designed and operating effectively. This report does not comprise the suitability of the design or operating effectiveness of such complementary user entity controls.

Rackhosting's responsibilities

Rackhosting is responsible for: preparing the description and accompanying assertion in section 1, including the completeness, accuracy and method of presentation of the description and assertion; providing the services covered by the description; specifying the control objectives and stating them in the description; identifying the risks that threaten the achievement of the control objectives; identifying the criteria and designing, implementing and effectively operating controls to achieve the stated control objectives. The control objectives have been specified by Rackhosting and are stated in the description.

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 the fairness of Rackhosting's description and on the suitability of 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 3402, "Assurance Reports on Controls at a Service Organisation", issued by the International Auditing and Assurance Standards Board, and additional requirements applicable in Denmark. This standard requires that we comply with ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description of a service organisation's system and the suitability of the design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the description 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 also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein and the suitability of the criteria specified by Rackhosting and described in section 1.

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

Inherent limitations

Rackhosting's description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the general services that the individual customer may consider important in its own particular circumstances. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in the general services. Also, the projection to future periods of any evaluation of the fairness of the presentation of the description, or opinions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organisation may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the criteria including the control objectives described in Rackhosting's assertion in section 1:

a) The description fairly presents how IT general controls in relation to the general services were designed and implemented throughout the period from 1 May 2025 to 30 April 2026

b) The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls operated effectively throughout the period from 1 May 2025 to 30 April 2026 and user entities applied the complementary customer controls referred to in section 3

c) The controls tested, which together with the complementary customer controls referred to in section 3, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 May 2025 to 30 April 2026.

Emphasis of matter

Without giving rise to any modification of our opinion, we inform you that our audit has identified a number of weaknesses in control objective "15 Supplier relationships" regarding Global Connect A/S.

Description of test of controls

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

Additional information

The information included in section 5 is presented by Rackhosting to provide additional information and is not part of Rackhosting's description of controls that may be relevant to customers' internal control as it relates to financial reporting. Such information has not been subjected to the procedures applied in the examination of the description of Rackhosting's controls and, accordingly, we express no opinion on it.

Intended users and purpose

We were engaged to report by Rackhosting and, therefore, this report and the description of tests of controls and results thereof in section 4 are intended for the use of Rackhosting.

We permit the disclosure of this report in full only, including the description of tests of controls and results thereof by Rackhosting, at its discretion, to customers who have used Rackhosting's general services during some or all of the period of 1 May 2025 to 30 April 2026 and their auditors, who have a sufficient understanding to consider it, along with other information about controls operated by customers themselves when assessing the risks of material misstatements of customers' financial statements, without assuming or accepting any responsibility or liability to customers or their auditors on our part.

Our report is not to be used for any other purpose or to be distributed to any other parties.

Hellerup, 8 July 2026
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Michael Clement
State-Authorised Public Accountant
mne23410

3. System description

3.1. Introduction

Rackhosting ApS provides cloud infrastructure and hosting services to Danish private enterprises and public sector organisations, with a strong focus on high availability, performance, and information security.

Since 2006, the company has operated its sales, administration, Network Operations Centre (NOC), and primary operational facilities from Taastrup, Denmark.

Rackhosting utilises third-party data centre providers while retaining full operational responsibility for its infrastructure, networking, and information security within its own environments. This operating model provides flexibility in system design and reduces dependency on individual suppliers.

The company's core service is a standardised virtualised hosting platform from which the majority of customer services are delivered. The platform is designed to provide stable, energy-efficient operations, high performance, and effective data protection through redundancy, replication, and backup.

Rackhosting's customers range from small and medium-sized enterprises to large commercial organisations and public sector institutions.

There have not been any significant changes in the period of the audit statement.

3.2. Description of Services

Rackhosting's services are delivered through a standardised virtualisation platform based on OpenStack/KVM.

Services are provided either as standard offerings or as customer-specific solutions based on individual agreements (managed or unmanaged).

Operational service options include:
• Tiered Storage (SAN) with advanced backup and disaster recovery capabilities
• Agent-based and agentless backup solutions
• Network and security services (firewalls, IDS/IPS, antivirus)
• Email and anti-spam services
• Monitoring, patch management, server management, and on-call services

All services are supported by customer-specific Service Level Agreements (SLAs), a Service Desk, and technical support.

3.3. Data Protection and Backup

Storage
The hosting platform is based on a redundant enterprise storage architecture distributed across two geographically separate data centres.

Storage is divided into the following tiers:

• High Performance (Tier 1): Performance-critical workloads (Pure Storage FlashArray//X)
• General Purpose (Tier 2): Production workloads (Pure Storage FlashArray//C)
• Archive / S3 (Tier 3): Archive, backup, and object storage (Pure Storage FlashBlade//E)

Each storage tier consists of two identical systems located in separate geographical locations and supports the following data protection mechanisms, where agreed:

• Active/Active replication to a secondary site
• High-frequency local snapshots
• Replication of snapshots to a secondary site

• Immutable backups (SafeMode) with segregation of duties for deletion

The storage systems are designed for enterprise workloads requiring high performance, availability, data integrity, and rapid recovery following failures or operational incidents.

Rackhosting maintains a proactive 24×7×365 support and monitoring agreement with the storage vendor, including a four-hour response time for all storage systems.

Backup
In addition to the integrated backup and security capabilities of the Pure Storage platform, Rackhosting offers backup solutions based on either Acronis or Veeam, depending on customer requirements.

Backup recovery is performed on an ongoing basis upon customer request as part of the continuous verification of backup integrity and recovery capability.

3.4. Control Environment

Technical personnel are located in the company's Network Operations Centre (NOC), from which operational services and customer support are delivered.

The NOC includes monitoring systems providing a consolidated overview of operational status, incidents, and support cases.

Services are operated under standard agreements unless otherwise agreed with the customer.

The control environment is based on documented policies, procedures, and controls managed centrally through the ComplyCloud GRC platform.

ComplyCloud is used for:
• Maintaining the control catalogue
• Follow-up of control activities
• Documentation of completed controls
• Risk assessments

Controls are performed with supporting evidence documented within the system. Roles and responsibilities are formally assigned to ensure accountability and traceability.

Employees sign confidentiality agreements as part of their employment, which remain in force after termination of employment.

Primary systems are hosted in dedicated server areas managed by Rackhosting within third-party data centres. Independent assurance reports covering these facilities are obtained annually.

3.5. Change Management

Procedures for changes to infrastructure, internal systems, and customer environments are documented in Rackhosting's operational documentation portal (docs.rackhosting.com) and managed operationally through the Service Desk. Changes are registered, assessed, risk evaluated, and documented, including their purpose and associated risks.

3.6. Risk Management

Risk management is performed through ComplyCloud, where risks are identified, assessed, and linked to relevant controls. Risks are reviewed at least annually and whenever significant changes occur to systems or the threat landscape.

3.7. Information and Communication

Customer communication is primarily handled through the Service Desk. Customer enquiries received by telephone or email are registered as support tickets. Tickets are prioritised according to the customer's SLA and handled in accordance with defined processes. Escalation is performed automatically or manually in accordance with established procedures. Tickets are assigned based on workload, competence, and areas of responsibility. Operational reporting is provided where contractually agreed.

3.8. Monitoring

Relevant system activities are logged to ensure traceability and follow-up. Monitoring of controls and operational activities is supported by ComplyCloud and technical monitoring tools. Processes are established to ensure follow-up on completed controls and overdue activities. Management is actively involved in ensuring that control activities are performed and appropriately prioritised.

3.9. Incident Management

Incidents are classified within the Service Desk according to four severity levels: Critical, High, Medium, and Low. This classification forms the basis for prioritisation, escalation, and handling throughout the incident lifecycle.

3.10. Control Activities

Control activities are performed within the following areas (some activities require a specific customer agreement):

- Capacity management and infrastructure monitoring
- Patch management
- Backup and restore procedures
- Access management and user administration
- Security event monitoring and logging
- Change management
- Incident management and follow-up

3.11. Documentation and Follow-up

Control activities are documented and followed up in ComplyCloud, ensuring traceability and audit evidence.

3.12. Subservice Organisations

Rackhosting uses GlobalConnect A/S as its primary data centre provider, leasing dedicated and secured server areas. GlobalConnect provides facility management, including power, cooling, and physical security.

Rackhosting uses Cibicom A/S as its secondary data centre provider for backup and disaster recovery purposes, providing equivalent facility management services.

Rackhosting retains responsibility for all networking and information security within its own environments.

Neither supplier has access to Rackhosting's systems or customer data and is therefore not considered a data processor in this context.

3.13. Complementary User Entity Controls

Customers are responsible for acquiring, developing, and maintaining their own applications.

Customers are responsible for ensuring appropriate access management for their own systems following organisational or personnel changes.

Customers are also responsible for maintaining adequate backup arrangements and regularly testing recovery procedures unless these services have been specifically agreed with Rackhosting.

3.14. Detailed Control Objectives and Controls

A detailed description of the control objectives and related control activities is provided in Section 4.

4. Control objectives, control activity, tests and test results

4.1. Purpose and scope

We conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organisation", and additional requirements applicable in Denmark.

Our testing of the design, implementation and operating effectiveness 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 included how the controls are performed.
Observation	We observed the execution of the control.
Reperformance of the control	Repetition of the relevant control. We repeated the execution of the control to verify whether the control functions as assumed.

4.3. Overview of control objectives, control activity, tests and test results

4. Risk assessment

Control objective 4: Risk assessment

That the company has a procedure for risk assessment and that a current risk analysis has been prepared and approved by management.

No.	Rackhosting's control activity	Tests performed by PwC	Result of PwC's tests
4.1.1	**Risk assessment** Rackhosting performs risk assessments of critical internal information assets. The risk assessment is systematised using a tool. Risk assessments are performed at least once a year. Responsibility for risk assessment rests with management, who initiate the assessment in collaboration with an assessment officer.	We have inquired of management about the procedures and control activities performed. We have inspected the risk assessment provided from the Control Manager. We have inspected that the risk assessment was performed within the past year.	No exceptions noted.

5. Information security policies

Control objective 5: Guidelines for the management of information security

To provide guidelines for and support information security in accordance with business requirements and relevant laws and regulations.

No.	Rackhosting's control activity	Tests performed by PwC	Result of PwC's tests
5.1.1	**Information security policies** Rackhosting's information security policy is documented and maintained through the ControlManager by means of regular reviews and updates. The information security policy has been approved by management. The information security policy is made available to employees via the ControlManager.	We have inquired of management about the procedures and control activities performed. We have inspected that management has approved the security policy and that it is updated on an ongoing basis. Furthermore, that it is readily available to employees.	No exceptions noted.

6. Organisation of information security

Control objective 6: Internal organisation

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

No.	Rackhosting's control activity	Tests performed by PwC	Result of PwC's tests
6.1.1	**Information security roles and responsibilities** The organisational responsibility for information security is documented and implemented. In addition, rules have been established for confidentiality agreements and the reporting of information security incidents, and comprehensive inventories of significant assets have been prepared.	We have inquired of management about the procedures and control activities performed. We have inspected that the organisational responsibility for information security is documented and implemented. We have furthermore inspected that confidentiality agreements, the reporting of information security incidents and the inventory of assets have been prepared.	No exceptions noted.
6.1.2	**Segregation of duties** Management has implemented policies and procedures to ensure satisfactory segregation of duties at Rackhosting. These policies and procedures include requirements that: • administrators responsible for production do not have access to applications and transactions; Backup administrators do not have administrative rights to both the primary and secondary backup locations.	We have inquired of management about the procedures and control activities performed. During interviews, IT staff have been asked about their competencies, areas of work and responsibilities. We have inspected that there is segregation of duties between finance and IT operations. We have inspected that there is segregation of duties between the primary and secondary backup locations.	No exceptions noted.

9. Access control

Control objective 9:

To ensure access for authorised users and prevent unauthorised access to systems and services.

No.	Rackhosting's control activity	Tests performed by PwC	Result of PwC's tests
9.1.1	**Access to networks and network services, data communication** Data communication is appropriately organised and adequately secured against the risk of loss of authenticity, integrity, availability and confidentiality. Furthermore, the network has been segmented where this has been deemed necessary or agreed with the customer.	We have inquired of management about the procedures and control activities performed and inspected that an appropriate authentication process is used for the operating environment. We have, on a sample basis, inspected that users are identified and verified before access is granted, and that remote access is protected by VPN. We have inspected that unified threat management is used, which continuously and actively provides information about possible threats that may affect the "confidentiality, integrity and availability of data." We have inspected that the network is configured with separate VLANs.	No exceptions noted.
9.2.2	**User access provisioning** All users must be registered with a unique user ID, and their rights to networks and systems must comply with Rackhosting's policies. Furthermore, it must be ensured that rights are based on a business-related need and are properly approved and set up in the systems.	We have inquired of management about the procedures and control activities performed. We have inspected the procedure for user administration and that the control activities adequately cover Rackhosting's needs. We have obtained an overview of user accounts on systems and networks. We have, on a sample basis, inspected that access requests were documented and approved in accordance with the relevant security policy, and that unique and personally identifiable user IDs are used.	No exceptions noted.

9. Access control

Control objective 9:

To ensure access for authorised users and prevent unauthorised access to systems and services.

No.	Rackhosting's control activity	Tests performed by PwC	Result of PwC's tests
9.2.6	**Removal or adjustment of access rights** Upon termination of employment, all user rights to systems, networks, databases and data files are deactivated.	We have inquired of management about the procedures and control activities performed to ensure that the removal of access rights is carried out in accordance with sound business procedures, and that follow-up is performed in accordance with the business procedures for the access rights granted. We have furthermore, on a sample basis, inspected that terminated employees had been deleted from the AD and that the users did not appear in the overview of current user accounts.	We have found for 2 out of 2 samples of user terminations that the users' access rights were not removed or disabled in a timely manner. For one user, we have been informed that this is because he has helped after after his last working day. For both samples, we have inspected that they have not been logged in after resigning. No further exceptions found.
9.4.2	**Secure log-on procedures** Access to systems, networks, databases and data files is protected by passwords. Quality requirements have been set for passwords, requiring a minimum length, complexity and maximum validity period, and password settings prevent passwords from being reused. Furthermore, the user is locked out after repeated incorrect log-on attempts.	We have inquired of management about the procedures and control activities performed in connection with password controls and inspected that appropriate authentication of users is applied across all access paths. We have inspected that an appropriate password quality is applied in Rackhosting's operating environment. Furthermore, we have, on a sample basis, inspected that access to the company's systems takes place using a username and password.	We have found that the build version on the sampled SQL database has not been updated with a new version since November 16, 2022. No further exceptions found.

11. Physical and environmental security

Control objective 11: Secure areas

To prevent unauthorised physical access to, and damage and interference with, the organisation's information and information processing facilities.

No.	Rackhosting's control activity	Tests performed by PwC	Result of PwC's tests
11.1.2	**Physical security perimeter** Access to secured areas (for both new and existing employees) is restricted (including using a security pass and personal code) to authorised employees. Persons without authorisation to secured areas must be accompanied by an employee with the appropriate authorisation.	We have inquired of management about the procedures and control activities performed. We have performed a physical inspection of Rackhostings office.	No exceptions noted.

12. Operations security

Control objective 12:

To ensure correct and secure operation of information processing facilities, protected against malware and loss of data and to record events and provide evidence.

No.	Rackhosting's control activity	Tests performed by PwC	Result of PwC's tests
12.1.1	**Documented operating procedures** Documented and management-approved operating procedures exist for all significant areas of Rackhosting's quality management system.	We have inquired of management about the procedures and control activities performed. In connection with the audit of the individual operational areas, we have inspected that documented procedures exist and that there is consistency between the documentation and the actions actually performed.	No exceptions noted.
12.1.2	**Change management** New systems and significant upgrades are tested, including user acceptance testing by qualified staff prior to implementation in the production environment. Subsequent testing of implementations is also performed. Issues identified during the development and implementation of new systems and significant updates are resolved satisfactorily. Testing/assessment of changes to systems and networks is approved before transfer to production. Emergency changes to systems and networks outside the normal business procedures are tested and approved subsequently.	We have inquired of management about the procedures and control activities performed, as well as the adequacy of the change management procedures. We have inspected that an appropriate change management system has been established to support the technical infrastructure. We have, on a sample basis, inspected change requests for the following: • documented testing of changes, including approval; • approval must be obtained prior to implementation (verbal management approval is considered sufficient for emergency changes but must be documented subsequently); • rollback plan, via snapshot where relevant.	We have found for 2 out of 2 samples that due to personnel changes, they have not followed the change management procedure. We have not been able to see documentation of tests performed and timely approval of the changes. No further exceptions found.

12. Operations security

Control objective 12:

To ensure correct and secure operation of information processing facilities, protected against malware and loss of data and to record events and provide evidence.

No.	Rackhosting's control activity	Tests performed by PwC	Result of PwC's tests
12.2.1	**Controls against malware** Antivirus software has been implemented and is updated regularly.	We have inquired of management about the procedures and control activities performed. We have, on a sample basis, inspected that antivirus software is installed where relevant and that it is updated.	No exceptions noted.
12.3.1	**Information backup** Data is backed up at appropriate intervals. Periodic testing is performed to ensure that data can be restored from backups.	We have inquired of management about the procedures and control activities performed. We have inspected that backup procedures are updated and formally documented. We have, on a sample basis, inspected that backups have been completed successfully, or alternatively that remediation is performed in the event of failed backups. In addition, we have, on a sample basis, inspected that restore tests have been performed.	No exceptions noted.
12.4.3	**Administrator and operator logs** Transactions or activity, as well as users with privileged rights (e.g. superusers), are logged. This also includes databases. Anomalies are investigated and resolved in a timely manner.	We have inquired of management about the procedures and control activities performed. We have, on a sample basis, inspected that the system configuration of logging parameters is set up so that actions performed by users with elevated rights on servers and significant network devices are logged. We have furthermore, on a sample basis, inspected that adequate follow-up is performed on logs from critical systems.	No exceptions noted.

13. Communications security

Control objective 13: Network security management

To ensure the protection of information in networks and of supporting information processing facilities.

No.	Rackhosting's control activity	Tests performed by PwC	Result of PwC's tests
13.1.1	**Securing network services** Penetration tests are performed regularly to secure the network.	We have inspected that periodic penetration tests have been performed and that identified weaknesses have been addressed and remediation measures initiated.	No exceptions noted.

15. Supplier relationships

Control objective 15: Supplier service delivery management

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

No.	Rackhosting's control activity	Tests performed by PwC	Result of PwC's tests
15.1.2	**Supplier agreements** Cooperation with suppliers is based on approved contracts.	We have inquired of management about the procedures and control activities performed. We have furthermore, on a sample basis, inspected that cooperation with external parties is based on approved contracts.	No exceptions found.
15.2.1	**Monitoring and review of supplier services** A review of services from service providers has been performed, including consideration of obtaining assurance reports from these, e.g. an ISAE 3402 report. For type 2 reports, user controls are reviewed and compared with existing controls and processes. New reports are reviewed periodically to ensure that they cover the correct period. In addition, identified control weaknesses are reviewed. Matters are investigated and resolved in a timely manner.	We have inquired of management about the procedures and control activities performed. We have inspected that ISAE 3402 reports have been received and reviewed from relevant service providers for the relevant period.	We have found that there is no documentation that supplier reports have been reviewed in accordance with the described control. We have found from the audit statement regarding GlobalConnect A/S that the auditor has not been able to obtain documentation for the performed half year review of external access cards that have not been used within the last six months. Further, that not all repeater sites comply with the requirements for physical security. No further exceptions found.

17. Information security aspects of business continuity management

Control objective 17.1: Information security continuity

That information security continuity should be embedded in the organisation's business continuity management systems.

No.	Rackhosting's control activity	Tests performed by PwC	Result of PwC's tests
17.1.1	**Planning information security continuity** The overall disaster recovery plan consists of an overarching disaster management procedure as well as operational disaster recovery plans for the specific disaster areas. The operational disaster recovery plan contains a description of the disaster recovery organisation, including management role descriptions, contact information, alert lists and instructions for the necessary response teams. For each platform, detailed response team instructions have been prepared for recovery to emergency operations.	We have inquired of management about the procedures and control activities performed. We have inspected that the organisational and operational IT disaster recovery plan contains management role descriptions, contact information, alert lists and instructions.	No exceptions noted.
17.1.2	**Verify, review and evaluate information security continuity** The disaster recovery capability is tested annually through both desktop tests and actual test scenarios.	We have inquired of management about the procedures and control activities performed. We have inspected that contingency plans are tested through desktop tests or realistic test scenarios, to the extent possible.	No exceptions noted.

5. Additional information from Rackhosting ApS

The information included in this section is prepared by Rackhosting to provide its customers 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 is fairly presented, whether the controls supporting the control objectives presented in section 4 have been appropriately designed and whether the controls operated effectively throughout the period. Thus, PwC's opinion in section 2 does not cover the information in section 5.

No.	Rackhosting's control activity	Result of PwC's tests	Management comments
9.2.6	**Removal or adjustment of access rights** Upon termination of employment, all user rights to systems, networks, databases and data files are deactivated.	We have found for 2 out of 2 samples of user terminations that the users' access rights were not removed or disabled in a timely manner. For one user, we have been informed that this is because he has helped after after his last working day. For both samples, we have inspected that they have not been logged in after resigning. No further exceptions found.	Management acknowledges the observation. We agree that access rights should be removed or adjusted in a timely manner upon termination of employment. In the two samples identified, the accounts were not disabled within the expected timeframe. We note that PwC inspected that the users did not log in after their resignation dates. For one of the users, continued access related to post-employment assistance. Going forward, any such access will be handled as a documented, approved and time-limited exception with defined scope and subsequent removal. Management has strengthened the offboarding process to ensure that all employee terminations trigger a documented access review and removal process across relevant systems. The process includes a checklist, responsible owner, deadline for completion, evidence of access removal and separate approval of any exceptions.

No.	Rackhosting's control activity	Result of PwC's tests	Management comments
9.4.2	**Secure log-on procedures** Access to systems, networks, databases and data files is protected by passwords. Quality requirements have been set for passwords, requiring a minimum length, complexity and maximum validity period, and password settings prevent passwords from being reused. Furthermore, the user is locked out after repeated incorrect log-on attempts.	We have found that the build version on the sampled SQL database has not been updated with a new version since November 16, 2022. No further exceptions found.	Management acknowledges the observation. The observation relates to the build version of the sampled SQL database. Management notes that the observation concerns patch and version management rather than the password and lock-out requirements described in the control activity. Management will review the SQL database version, including vendor support status, relevant security updates and operational dependencies. Based on this review, the database will either be updated through the change management process or handled as a documented risk-based exception with relevant compensating controls. Going forward, SQL database build levels will be included in the regular patch and vulnerability management process to ensure periodic review, documented assessment and follow-up on required updates.

No.	Rackhosting's control activity	Result of PwC's tests	Management comments
12.1.2	**Change management** New systems and significant upgrades are tested, including user acceptance testing by qualified staff prior to implementation in the production environment. Subsequent testing of implementations is also performed. Issues identified during the development and implementation of new systems and significant updates are resolved satisfactorily. Testing/assessment of changes to systems and networks is approved before transfer to production. Emergency changes to systems and networks outside the normal business procedures are tested and approved subsequently.	We have found for 2 out of 2 samples that due to personnel changes, they have not followed the change management procedure. We have not been able to see documentation of tests performed and timely approval of the changes. No further exceptions found.	Management acknowledges the observation. We agree that changes to systems and networks must be documented, assessed, tested and approved in accordance with the change management procedure. In the two samples identified, the required documentation of testing and timely approval was not available. The exceptions occurred during a period with personnel changes and operational transition. Management recognises that the change management process must remain consistently applied regardless of organisational changes. Management has therefore already reinforced the change management process by requiring that significant changes are registered in the Service Desk, linked to a documented change record, risk assessed, approved before implementation where possible, and completed with evidence of testing and rollback considerations. Emergency changes must be documented and approved retrospectively. Compliance with the change management process will be monitored on an ongoing basis.

No.	Rackhosting's control activity	Result of PwC's tests	Management comments
15.2.1	**Monitoring and review of supplier services** A review of services from service providers has been performed, including consideration of obtaining assurance reports from these, e.g. an ISAE 3402 report. For type 2 reports, user controls are reviewed and compared with existing controls and processes. New reports are reviewed periodically to ensure that they cover the correct period. In addition, identified control weaknesses are reviewed. Matters are investigated and resolved in a timely manner.	We have found that there is no documentation that supplier reports have been reviewed in accordance with the described control. We have found from the audit statement regarding GlobalConnect A/S that the auditor have not been able to obtain documentation for the performed half year review of external access cards that not have been used within the last six months. Further, that not all repeater sites comply with the requirements for physical security. No further exceptions found.	Management acknowledges the observation. Rackhosting obtains and read the received assurance reports from relevant service providers; however, documentation of the formal review of supplier reports was not available in accordance with the described control. Management has strengthened the supplier review process to ensure that relevant assurance reports are obtained, reviewed, documented and followed up on at least annually. The review will include assessment of report period coverage, auditor's opinion, identified exceptions, complementary user entity controls and any required follow-up actions. Regarding the observations in the GlobalConnect A/S assurance report, Management notes that the observations relate to controls operated by the subservice organisation and not to Rackhosting's own systems or customer data. Rackhosting have noted that the error, has been rectified and strengthened controls has been implemented at GlobalConnect Going forward, supplier report reviews and follow-up actions will be documented as part of Rackhosting's supplier management process.

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

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

Martin Helms
CEO
På vegne af: Rackhosting ApS
Serienummer: 695570c4-3c3a-4885-a3f2-5478783dca70
IP: 109.56.xxx.xxx
2026-07-08 07:34:42 UTC

Michael Clement
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
På vegne af: PricewaterhouseCoopers Statsautoriseret…
Serienummer: 232c5786-309c-4897-93ea-5c2a6741c1d3
IP: 83.136.xxx.xxx
2026-07-08 07:39:19 UTC