INDEPENDENT AUDITOR'S ISAE 3402 ASSURANCE REPORT FOR THE PERIOD FROM 1 SEPTEMBER 2025 TO 31 AUGUST 2026 ON THE DESCRIPTION OF COLOCATION AND THE RELATED CONTROLS AND THEIR DESIGN AND OPERATING EFFECTIVENESS

Cibicom A/S

This English document is an unofficial translation of the original Danish assurance report, and in case of any discrepancy between the original Danish assurance report and the English translation, the Danish text shall prevail.



CONTENTS

1. AUDITOR'S REPORT 2

2. CIBICOM A/S'S STATEMENT 4

3. CIBICOM A/S' DESCRIPTION OF COLOCATION 5

A.5: Information security policies 10

A.6: Organization of information security and internal organization 11

A.7: Employee safety 12

A.11: Physical protection and environmental protection 14

A.18: Compliance 16

1. AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT FOR THE PERIOD FROM 1 SEPTEMBER 2025 TO 31 AUGUST 2026 ON THE DESCRIPTION OF COLOCATION AND THE RELATING CONTROLS AND THEIR DESIGN AND OPERATING EFFECTIVENESS

To: The Management in Cibicom A/S
Cibicom A/S' customers and their auditors

Scope

We have been engaged to report on the description prepared by Cibicom A/S (the service organization) in Section 3 for the period from 1 September 2025 to 31 August 2026 of its Colocation services and related controls, and on the suitability of the design and operating effectiveness of the controls that relate to the control objectives stated in the description.
The assurance report covers four locations: Ballerup, Copenhagen West (Hove), Søsterhøj (Aarhus), and Kappa (Hinnerup). The Taulov location is outside the scope of this report.

The Service Provider's Responsibilities

The service provider is responsible for preparing the description and accompanying statement in section 2, including the completeness, accuracy, and method of presentation of the description and the statement.

The service provider is responsible for providing the services covered by the description; stating the control objectives; and identifying the risks threatening achievement of the control objectives; designing and implementing effectively operating controls to achieve the stated control objectives.

Auditor's Independence and Quality Assurance

We have complied with the requirements of independence and other ethical requirements of the International Ethics Standards Board of Auditors' International Guidelines on the Conduct of Auditors (IESBA Code), which are based on the fundamental principles of integrity, objectivity, professional competence, and due diligence, confidentiality, and professional conduct, as well as ethical requirements applicable in Denmark.

BDO Statsautoriseret revisionspartnerselskab applies International Standard on Quality Management, 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.

Auditor's Responsibilities

Our responsibility is, on the basis of our actions, to express a conclusion about the service provider's description as well as about the design and operational efficiency of controls related to the control objectives set out in this description.

We have performed our work in accordance with the International Standard on Assurance Engagements 3402 on declaration duties with security checks at a service organisation. This standard requires that we plan and carry out our actions in order to obtain a high degree of certainty as to whether the description is correct in all material respects and whether the controls in all essential respects are appropriately designed and have operated effectively.

A declaration task with certainty to provide a statement about the description, design, and operational effectiveness of controls at a service provider includes performing actions to obtain evidence of the information in

the service provider's description as well as of the controls' design and operational effectiveness. The actions chosen depends on the assessment of the service provider's auditor, including the assessment of the risks that the description is not accurate and that the controls are not appropriately designed or do not operate effectively. Our actions have included tests of the operational effectiveness of such controls, which we consider necessary to provide a high degree of assurance that the control objectives set out in the description were achieved. A statement of assurance with certainty of this type further includes an assessment of the overall presentation of the description, the appropriateness of the control objectives set out therein and the appropriateness of the criteria specified and described by the service provider in section 2.

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

The service organisations' description is prepared to meet the common needs of a wide range of customers and their auditors and may not, therefore, include every aspect of Colocation that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions. Also, 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 report. The criteria we used in forming our opinion are those described in service providers statement in section 2. In our opinion, in all material respects:

a. The description of Colocation and related controls, as designed and implemented throughout the period from 1 September 2025 to 31 August 2026 is in all material aspects, accurate and

b. The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 September 2025 to 31 August 2026; 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 September 2025 to 31 August 2026.

Description of Tests of Controls

The specific controls tested, and results of those tests are listed in section 4.

Intended Users and Purpose

This report is intended only for customers, which have used the service providers Colocation, and their auditors who have a sufficient understanding to consider it, along with other information about controls operated by the customer themselves when obtaining an understanding of customers' information systems relevant to financial reporting.

Copenhagen, 22. October 2026

BDO Statsautoriseret Revisionspartnerselskab

Nikolai T. Visti
Partner, State Authorised Public Accountant

Mikkel Jon Larssen
Partner, chef for Risk Assurance, CISA, CRISC

2. CIBICOM A/S'S STATEMENT

Cibicom A/S operates and provides Colocations services.

The description has been prepared for Cibicom A/S' customers and their auditors who have a sufficient understanding to consider this description, along with other information, including information about controls operated by the customers themselves, when assessing the risks of material misstatements of customers' financial statements.
Cibicom A/S confirms that the accompanying description in section 3 fairly presents controls in relation to Colocations and associated controls throughout the period from 1 September 2025 to 31 August 2026. The criteria used in making this statement were that the accompanying description:

1. Explains the Colocation services, and how associated controls were designed and implemented, including explaining:
    - The Colocation services provided
    - The procedures and controls, which are part of the physical security related to Colocation.
    - The scope includes the four locations of Ballerup, Copenhagen West (Hove), Søsterhøj (Aarhus), and Kappa (Hinnerup). The Taulov location is excluded from the scope.
    - Relevant control objectives and controls designed to achieve those objectives.
    - Other aspects of our control environment, risk assessment process, information system (including the associated business processes) and communication, control activities and monitoring controls that have been relevant to the processing and reporting of customer transactions
2. Includes relevant details of changes to the controls relating to the service providers Colocation during the period from 1 September 2025 to 31 August 2026.
3. Does not omit or distort information relevant to the scope of the controls described relating to Colocation considering that the description is prepared to meet the general needs of a wide range of customers and their auditors and therefore cannot include every aspect of Colocations that the individual customer may consider of importance to their special environment.

Cibicom A/S confirms that controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 September 2025 to 31 August 2026. The criteria we used in making this statement were that:

1. The risks that threatened achievement of the control objectives stated in the description were identified.
2. The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved.
3. The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period from 1 September 2025 to 31 August 2026.

Ballerup, 22. October 2026

Cibicom A/S

Jakob Reichhardt
CISO

3. CIBICOM A/S' DESCRIPTION OF COLOCATION

OVERALL DECRIPTION OF CIBICOM A/S

Cibicom provides support to customers with different key services, making it necessary to manage such services in a structured and professional manner. Therefore, all services are maintained and operated on the basis of the same structure and standards.

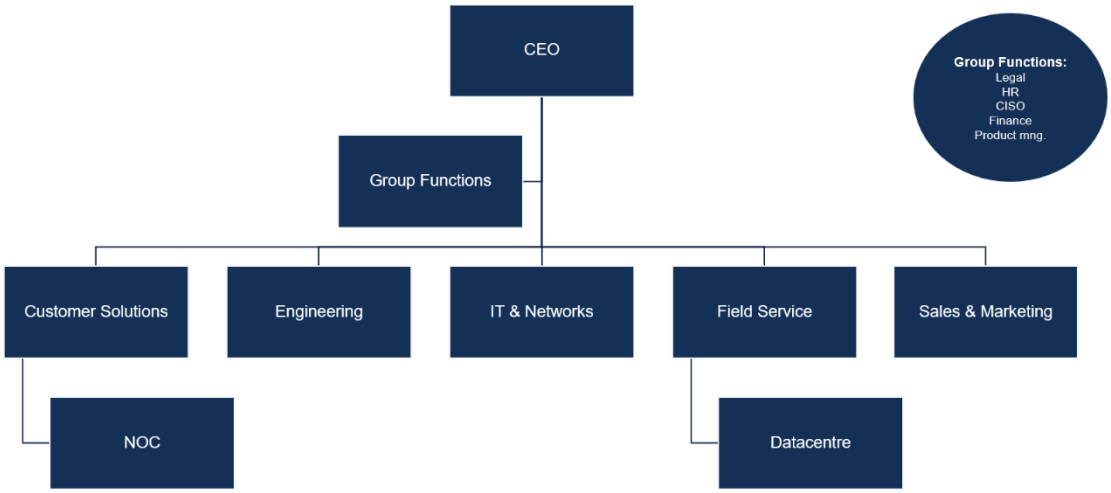
We ensure that our customers have access to the latest technology through professional consultancy, installation and service, and thus ensure the best foundation for competent, all-round solutions, one of which is Colocation.

The structure of our operating organisation is based on the international standards ISO 9001 and ISO 27001:2013, which Cibicom is certified for, and ITIL - IT Infrastructure Library®, on which all our operating procedures are based.

Such factors are incorporated into management's control of information security and supported by our Quality Management and Information Security Policy, which defines the framework for implementation of information security at Cibicom.

Cibicom supplies reliable and secure distribution of IP, TV and radio services through professional consultancy, installation and service. Cibicom runs the Coastal Radio Network in Denmark, along with other broadcast ser-vices for the major TV operators in the country.
Such services are based on Cibicom's mast infrastructure, in which our 35 masts and backbone network are some of the key elements.

Cibicom is structured as shown below, in which the overall running of Cibicom's services come under the Chief Operating Officer – COO in Operations.



CONTROL ENVIRONMENT FOR THE COLOCATION SERVICE

Cibicom A/S's Colocation service is operated from four locations: Ballerup, Copenhagen West (Hove), Søsterhøj (Aarhus), and Kappa (Hinnerup). All data centres are built and operated based on the same infrastructure standards and operating procedures.

On 1 June 2025, Cibicom A/S acquired an additional data centre in Taulov. The Taulov data centre is currently being upgraded to meet Cibicom's standards but has not yet been commissioned for Colocation services. Consequently, the Taulov location is not included within the scope of this report..

A.5: Policies for Information Security
Our Information Security Management System (ISMS) provides an overview of the policies, procedures, processes, rules, organisational chains of command and activities, along with their related resources that comprise the components of the organisation’s management of information security.
Our quality and information security committee meets regularly, and at least twice annually.

A.6: Organisation of information security and internal organisation
Cibicom A/S has devised an ISMS policy and organisation chart to ensure that roles and areas of responsibility for information security are clearly defined and allocated.

A.7: Personnel
Cibicom A/S has procedures designed to ensure that the recruitment of personnel or leaving procedures comply with our criteria, including screening, references, security clearance (if required) and our procedure for termination/change of employment and sanctions in the event of non-compliance with procedures.

A.11: Procedure for site access
Security is a key element for Cibicom A/S, and we have therefore compiled access procedure for:
• Employees
• Subcontractors/engineers
• Colocation customers

A.11: Security of supply
A range of security measures have been implemented for Cibicom’s Colocation.
Firefighting equipment including fire and smoke detectors have been installed, and security of supply is ensured in the form of a battery uninterrupted power supply (UPS) and diesel generator (DG), controlled via electrical cabling equipment linking UPS, DG and mains electricity supply.

A.11: Monitoring
To ensure a high level of operational stability, monitoring of supply provision to Colocation sites and to the actual Colocation service has been implemented, in accordance with the SLA.
Monitoring includes:
• Electricity supply
• Fire
• Access
• Temperature

A.11: Access control
All access to Cibicom’s Colocation locations is controlled by Automatic Door Control (ADC) using card readers.

A.11: Perimeter security
Perimeter security is provided at all Colocation locations, along with procedures for classifying Colocation locations and areas.

Perimeter security consists of fencing around the building with remotely controlled gates (may be remotely controlled by NOC). Cards can also be used. Moreover, intruder alarms are also installed on all exterior doors and windows and these sites have CCTV surveillance.

A.18: Service Level Agreement (SLA)
An SLA has been compiled for the Colocation service designed to ensure provision of all contractual services. The SLA is part of the established contractual agreement with Colocation customers.

Errors (incidents) are registered in Cibicom's ITSM system, providing the data for an SLA report.

Changes since the 31 August 2025

Cibicom A/S has not made any significant or relevant changes of the Colocations or the relating technical and organisational security measures and other controls during the period from 1 September 2025 to 31 August 2026.

4. CONTROL OBJECTIVES, CONTROLS, TEST AND RESULTS OF TESTS

Objective and scope

BDO has carried out the work in accordance with ISAE 3402 on assurance engagements relating to controls at a service organisation.

BDO has performed procedures to obtain evidence of the information in Cibicom A/S description of Colocation and the design and the operating effectiveness of these controls. The procedures performed depend on BDO's assessment, including the assessment of the risks that the description is not fairly presented and that the controls are not suitably designed or operating effectively.

BDO's test of the design and operating effectiveness of controls has included the control objectives and related control activities selected by Cibicom A/S, and which are described in the following.

In the check form, BDO has described the tests performed which were considered necessary to obtain a reasonable degree of assurance that the stated control objectives were achieved and that the related controls were suitably designed and operated effectively throughout the period from 1 September 2025 to 31 August 2026.

Test procedures

Tests of the design of technical and organisational security measures and other controls, the implementation and effectiveness hereof were performed by inquiry, inspection, observation, and re-performance.

Type	Description
Inquiry	Inquiries of relevant personnel at Cibicom A/S have been performed for all significant control activities. The purpose of the inquiries was to obtain knowledge and further information about implemented policies and procedures, including how the control activities are performed, and to obtain confirmed evidence of policies, procedures, and controls.
Inspection	Documents and reports, which include information about the performance of the control, have been read for the purpose of assessing the design and monitoring of the specific controls, i.e., whether the design of the controls is such that they are expected to be effective if implemented, and whether the controls are sufficiently monitored and checked at suitable intervals. Tests have been performed of significant system structures of technical platforms, databases, and network equipment to ensure that controls have been implemented, including for example assessment of logging, back-up, patch management, authorisations and access controls, data transmission, and inspection of equipment and locations.
Observation	The use and existence of specific controls have been observed, including tests to ensure that the control has been implemented.
Re-performance	Controls have been re-performed to obtain additional evidence that the controls operate as assumed.

Result of test

The result of the test made of technical and organisational measures and other controls has resulted in the conclusions specified on the following pages.

An exception exists when:

- Technical and organisational measures and other controls have not been designed or implemented to fulfil a control objective,
- Technical and organisational measures and other controls related to a control objective are not suitably designed and implemented or did not operate effectively throughout the period.

A.5: Information security policies

Control objectives

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

Control activity	Test performed by BDO	Result of test
Information security policies ▶ Management defines and approves procedures for information security, which are made available and communicated to employees. ▶ Cibicom A/S has implemented procedures, which ensures a periodic review of the ISMS-policy and approvement of the management. ▶ All procedures are reviewed and updated at least once a year or if significant changes are done to these.	We have made inquiries with relevant personnel at Cibicom A/S. We have inspected Cibicom A/S ISMS-policy and observed that Cibicom A/S has distributed their information security policy in multiple procedures. We have further ensured documentation that change in procedure and new procedures are communicated to relevant parties. We have observed that Cibicom A/S has reviewed and approved the individual procedures that make up the information security policy. We have inspected the Control Manager and observed that all procedures are reviewed on an ongoing basis and at least once a year and that these are approved by management.	No deviations noted.

A.6: Organization of information security and internal organization

Control objectives

- *To establish a managerial basis to initiate and control the implementation and operation of information security in the organization.*

Control activity	Test performed by BDO	Result of test
Roles and responsibility areas for information security ▶ All responsibility areas for information security have been defined and allocated.	We have made inquiries with relevant personnel at Cibicom A/S. We have inspected Cibicom A/S' ISMS-policy and observed that a number of roles have been defined and that powers are separated into specific groups.	No deviations noted.
Segregation of duties ▶ Conflicting functions and responsibilities are separated to reduce the possibility of unauthorized or unintentional use, changes, or misuse of organizational assets.	We have made inquiries with relevant personnel at Cibicom A/S. We have inspected Cibicom A/S' organizational diagram, as well as relevant policies and observed that roles and responsibilities support segregation of duties. We have inspected samples of accesses in AD and observed that accesses are differentiated.	No deviations noted.

A.7: Employee safety

Control objectives

- *Secure staff conditions before, during and after employment.*

Control activity	Test performed by BDO	Result of test
Screening ▶ HR ensures that there is an assessment of new employment which requires security clearance. ▶ HR ensures that references are collected from employees.	We have made inquiries with relevant personnel at Cibicom A/S. We have for a sample of new employees inspected the employment contract and observed that there is a paragraph regarding whether a position requires security clearance. We have for a sample of new employees observed that security clearance process was initiated. We have for a sample observed that HR obtained references according to the recruitment process.	No deviations noted.
Terms and conditions of employment ▶ HR ensures that at the end of an employee's employment the nearest manager is informed of handed over effects and these are recovered. ▶ Cibicom A/S has implemented a procedure for education and training of employees including awareness campaigns. ▶ Cibicom A/S has implemented a procedure for sanctions for employees who violates applicable information security rules	We have made inquiries with relevant personnel at Cibicom A/S. We have inspected Cibicom A/S' procedure for termination and changes and observed that there is a fixed process for settlements of effects. We have taken a sample of the above and observed that the nearest manager receives an e-mail regarding the termination of employment and that the Customer Solution Manager confirms the return of delivered effects. We have inspected Cibicom A/S' procedure for education and training in information security. We have observed that employees are tested annually in relevant information security topics and the awareness campaigns are held on an ongoing basis.	We have determined that a procedure for sanctions has been established. We have not been able to comment on the implementation and effectiveness of the control, as there have been no sanctions during the declaration period. No deviations noted.

A.7: Employee safety

Control objectives

- *Secure staff conditions before, during and after employment.*

Control activity	Test performed by BDO	Result of test
	We have inspected Cibicom A/S' procedure for sanctions and observed that there is a formal process for sanction of employees who violate current information security rules. We have been informed that during the declaration period there have been no situations that have activated the sanction process. Therefore, it has not been possible to verify the efficiency of the procedure.	

A.11: Physical protection and environmental protection

Control objectives

- *To ensure that procedures exist for accessing Colocation sites and that sites are classified.*
- *To ensure a stable supply to Cibicom A/S's locations.*
- *To ensure that there is no unauthorized access to Colocation sites.*

Control activity	Test performed by BDO	Result of test
Physical access control ▶ Cibicom A/S has implemented procedures for handling access control and access limitations to Colocation. ▶ NOC controls that customers are data centre customers.	We have made inquiries with relevant personnel at Cibicom A/S. We have inspected Cibicom A/S' procedures for access control and access limitations of Colocation. We have observed that Cibicom A/S has divided their sites so that only pre-approved employees and customers with a work-related need have access to them. Logical access is managed through Active Directory (AD). The relevant controls are tested in section A6. We have observed that Cibicom A/S has divided suppliers who want access to Colocations into four categories based on which licenses they have.	No deviations noted.
Supportive security of supply ▶ NOC receives and records incidents for alarms on supply CI's (Configuration items), that fail. ▶ Incidents are included in Cibicom A/S' annual risk assessment of the Colocation service. ▶ Cibicom A/S supervises services within emergency supply.	We have made inquiries with relevant personnel at Cibicom A/S. We have by inquiry been informed that all configuration items will be monitored by HP Openview and that in the event of an alarm in HP a case will be created as well as an event in Service Now. We have sampled incidents and observed that NOC monitors CI as well as receives alerts and creates these as incidents in Service Now. We have inspected the annual risk assessment of Colocation and have observed that incidents are included as part of this.	No deviations noted.

A.11: Physical protection and environmental protection

Control objectives

- *To ensure that procedures exist for accessing Colocation sites and that sites are classified.*
- *To ensure a stable supply to Cibicom A/S's locations.*
- *To ensure that there is no unauthorized access to Colocation sites.*

Control activity	Test performed by BDO	Result of test
	We have inspected the procedures for backup supply systems and UPS systems and observed that these undergo a regular inspection at least once a year. We have carried out service inspections on automatic fire alarm systems, automatic room extinguishing systems, generators, UPS and electricity supply. We have observed that an inspection of the facilities has been carried out at all four locations.	
Securing offices, premises, and facilities ▶ IT extracts in relation to whether there are attempts at unauthorized access to Colocation sites. ▶ Data from extracts is included in the information security committee meetings. ▶ An incident is created if shell protection on doors and windows is activated.	We have made inquiries with relevant personnel at Cibicom A/S. We have inspected the log for Colocation access control and observed that there have been no attempts at unauthorized access during the declaration period. We have inspected the latest information security committee meeting and observed that relevant incidents are reviewed in the meeting. We have by inquiry been informed that if perimeter security is activated, an incident is created in Service Now. We have inspected incidents on perimeter security being logged and created as incidents.	No deviations noted.

A.18: Compliance

Control objectives

- *Ensure compliance of Service Level Agreement.*

Control activity	Test performed by BDO	Result of test
Compliance - That alarms are received if there are errors. - NOC creates incident based on alarms affecting the Colocation service. - Incidents are handled according to the general service management procedure. - Incidents are included in Cibicom A/S' annual risk assessment of the Colocation service.	We have made inquiries with relevant personnel at Cibicom A/S. We have sampled HP Openview and observed that alarms are received in the event of a system failure. We observed that NOC creates incidents and that these incidents have been dealt with in accordance with relevant procedures. We have inspected the service management procedure and incident management flow. We have observed that events are created according to these. We have inspected the annual risk assessment of Colocation and observed that incidents are included as a part of this.	No deviations noted.

BDO STATSAUTORISERET REVISIONSPARTNERSELSKAB

VESTRE RINGGADE 28
8000 AARHUS C

www.bdo.dk

BDO Statsautoriseret Revisionspartnerselskab, danskejet rådgivnings- og revisionsvirksomhed, er medlem af BDO International Limited - et UK-baseret selskab med begrænset hæftelse - og del af det internationale BDO-netværk bestående af uafhængige medlems-firmaer. BDO er varemærke for både BDO-netværket og for alle BDO medlemsfirmaerne. BDO i Danmark beskæftiger mere end 1.800 medarbejdere, mens det verdensomspændende BDO-netværk har ca. 120.000 medarbejdere i mere end 166 lande.

Copyright - BDO Statsautoriseret Revisionspartnerselskab, cvr.nr. 45719375.