DRAFT International Standard

ISO/IEC DIS 22237-7

Information technology — Data centre facilities and infrastructures —

Part 7: Management and operational information

Technologie de l'information — Installation et infrastructures de centres de traitement de données —

Partie 7: Informations de gestion et de fonctionnement

ICS: 35.020

ISO/IEC JTC **1**/SC **39**

Secretariat: **ANSI**

Voting begins on:
2026-06-29

Voting terminates on:
2026-09-21

This document is circulated as received from the committee secretariat.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/IEC DIS 22237-7:2026(en)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Foreword **9**
Introduction **10**
1 Scope **13**
2 Normative references **13**
3 Terms, definitions and abbreviations **14**
3.1 Terms and definitions 14
3.2 Abbreviations 16
4 Conformance **16**
5 Data centre strategy **17**
5.1 Purpose 17
5.1.1 General 17
5.1.2 Requirements 17
5.2 Activities 18
5.2.1 Assess current capabilities 18
5.2.2 Implement processes and KPI 18
5.2.3 Review of the strategy 19
5.2.4 Sourcing strategy 19
5.2.5 Strategy agreement 19
5.3 KPI: Actuality of agreed strategy 19
5.3.1 General 19
5.3.2 Recommendations 19
6 Organization **20**
6.1 Purpose 20
6.1.1 Requirements 20
6.1.2 Recommendation 20
6.2 Organizational duties, tasks and responsibilities 20
6.2.1 Requirements 20
6.2.2 Recommendations 20
6.3 Human resources 20
6.3.1 Requirements 20
6.3.2 Recommendation 20

© ISO/IEC 2026 – All rights reserved

6.4 Organizational Structure 20
6.4.1 Requirements 20
6.4.2 Recommendations 21
6.5 Management of processes 22
6.5.1 Purpose 22
6.5.2 Monitoring and control of Processes 22
7 Data centre management 23
7.1 Purpose 23
7.1.1 General 23
7.1.2 Requirements 23
7.2 Basic organization and role model 23
7.3 Management objectives 24
7.3.1 Management duties, tasks and responsibilities 24
7.3.2 Management objectives 25
7.3.3 Management of governance and compliance 25
7.3.4 Management of services and service levels 25
7.3.5 Management of processes 26
7.3.6 Management of key performance indicators 26
7.3.7 Management of quality 26
7.3.8 Management of threats and risks 26
7.3.9 Management of data centre continuity 27
7.3.10 Management of sustainability 27
7.3.11 Management of customer obligation 27
7.3.12 Supply management process 28
7.3.13 Management of providers, internal and external resources 28
8 Operational processes 29
8.1 Purpose 29
8.1.1 General 29
8.1.2 Requirements 29

© ISO/IEC 2026 – All rights reserved

8.2 Activities 29
8.2.1 Operational procedures 29
8.2.2 Standard operating procedures 30
8.2.3 Emergency operating procedures 30
8.2.4 Method of procedure 31
8.2.5 Work permit 31
8.2.6 Lock Out, Tag Out (LOTO) 32
8.2.7 Control of critical tasks 33
8.2.8 Setpoint and airflow control 34
8.2.9 Fire compartments 36
8.2.10 Maintenance 36
9 Operational information and parameters 43
9.1 Purpose 43
9.1.1 General 43
9.1.2 Requirements 43
9.1.3 Recommendations 43
9.2 Building construction as per ISO/IEC 22237-2 43
9.2.1 Requirements 43
9.2.2 Recommendations 44
9.3 Power distribution as per ISO/IEC 22237-3 44
9.3.1 General 44
9.3.2 Requirements 44
9.3.3 Recommendations 45
9.4 Environmental control as per ISO/IEC 22237-4 45
9.4.1 Requirements 45
9.4.2 Recommendations 45
9.4.3 Air flow parameters 46
9.4.4 Temperature parameters 46
9.4.5 Humidity parameters 46

© ISO/IEC 2026 – All rights reserved

9.5 Telecommunications cabling infrastructure as per ISO/IEC 22237-5 46
9.5.1 General 46
9.5.2 Requirements 47
9.5.3 Recommendations 47
9.6 Security systems as per ISO/IEC 22237-6 47
9.6.1 General 47
9.6.2 Requirements 47
9.7 Acceptance test 47
9.7.1 Purpose 47
9.7.2 Building construction (ISO/IEC 22237-2) tests 49
9.7.3 Power supply and distribution (ISO/IEC 22237-3) tests 49
9.7.4 Environmental control (ISO/IEC 22237-4) tests 50
9.7.5 Telecommunications cabling infrastructure (ISO/IEC 22237-5) tests 50
9.7.6 Security systems (ISO/IEC 22237-6) tests 50
9.7.7 Energy efficiency tests 51
9.8 Asset and configuration management 51
9.8.1 Purpose 51
9.8.2 Activities 51
9.8.3 KPI for asset and configuration management 52
9.9 Documentation 52
9.9.1 General 52
9.9.2 Recommendations 53
9.9.3 Design and construction documents 53
9.9.4 Insurance requirement reports 54
9.9.5 Security handbook 54
9.9.6 Building permit 54
9.9.7 Operational handbook 54
9.9.8 Installation handbook 55
9.9.9 Administration manual and software application settings 55

© ISO/IEC 2026 – All rights reserved

9.9.10 Housekeeping manual 56
9.9.11 Customer information portal 56
9.10 Incident management 56
9.10.1 Purpose 56
9.10.2 Activities 56
9.10.3 KPI for incident management 57
9.11 Problem management 58
9.11.1 Purpose 58
9.11.2 Activities 59
9.11.3 KPI: Ratio of solved problems 59
9.12 Change management 60
9.12.1 Purpose 60
9.12.2 Activities 60
10 Management Processes 61
10.1 Capacity management 61
10.1.1 Purpose 61
10.1.2 Activities 63
10.1.3 KPI: Balance of actual usage and capacity reserve 64
10.2 Availability management 65
10.2.1 Purpose 65
10.2.2 Activities 65
10.2.3 KPI for availability management 66
10.3 Security management 66
10.3.1 Purpose 66
10.3.2 Activities 66
10.3.3 KPI: number of security incidents 69
10.4 Resource management 69
10.4.1 Purpose 69
10.4.2 Activities 69

© ISO/IEC 2026 – All rights reserved

10.4.3 KPI for resource management 70
10.5 Energy management 70
10.5.1 Purpose 70
10.5.2 Activities 71
10.5.3 KPI for energy management 71
10.6 Product lifecycle management 73
10.6.1 Purpose 73
10.6.2 Activities 74
10.6.3 KPI: Deviation from expected product properties 75
10.7 Cost management 75
10.7.1 Purpose 75
10.7.2 Activities 75
10.7.3 KPI for cost management 77
10.8 Service level management 77
10.8.1 Purpose 77
10.8.2 Activities 77
10.8.3 KPI: Discrepancy between service quality and SLA 78
10.9 Customer management 78
10.9.1 General 78
10.9.2 Recommendations 78
10.9.3 Purpose 79
10.9.4 Activities 79
10.9.5 KPI for customer management 79
11 Risk management 80
11.1 Purpose 80
11.1.1 Requirements 80
11.1.2 Recommendations 80
11.2 Activities 80
11.2.1 General 80

© ISO/IEC 2026 – All rights reserved

178 11.2.2 Requirements 81
179 11.2.3 Recommendations 81
180 11.2.4 Risk list 82
181 11.2.5 Categorization 82
182 11.3 KPI for risk management 83
183 11.3.1 Number of open risks 83
184 11.3.2 Duration from register to completion 83
185 **12 Quality management 83**
186 12.1 Purpose 83
187 12.1.1 General 83
188 12.1.2 Requirements 83
189 12.2 Activities 84
190 12.2.1 Quality methodologies 84
191 12.2.2 Quality plan and objectives 84
192 12.2.3 Quality assessment 84
193 12.3 Quality improvement 84
194 **Annex A (informative) Example for process implementation 85**
195 **A.1 Prioritization of processes 85**
196 **Table A.1 — Prioritization of processes 85**
197 **A.2 Maturity 85**
198 **A.3 Relationship between the different types of maintenance (EN 13306:2017) 86**
199 **Table A.2 — Operational levels 87**
200 **Annex B (normative) Security systems 88**
201 **B.1 Access to the data centre premises 88**
202 **B.1.1 Manned guarding 88**
203 **B.1.1.1 General 88**
204 **B.1.1.2 Recommendations 88**
205 **B.1.2 Employees and other authorized personnel 88**
206 **B.1.2.1 Requirements 88**
207 **B.1.2.2 Recommendations 88**
208 **B.1.3 Visitors 89**
209 **B.1.3.1 Requirements 89**
210 **B.1.3.2 Recommendations 90**
211 **B.1.4 Deliveries 90**
212 **B.1.4.1 Requirements 90**

© ISO/IEC 2026 – All rights reserved

B.1.4.2 Recommendations 90
B.1.5 Examples for security controls 91
B.2 Fire suppression systems 92
B.2.1 Requirements 92
B.2.2 Recommendations 93
B.3 Management of electrical interference 93
B.3.1 Requirements 93
B.3.2 Recommendations 93
Bibliography 94

© ISO/IEC 2026 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 39, *Sustainability, IT and data centres*.

This first edition cancels and replaces ISO/IEC TS 22237-7:2018, which has been technically revised.

The main changes are as follows:

a) tbd

b) …

A list of all parts in the ISO/IEC 22237 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2026 – All rights reserved

Introduction

The unrestricted access to internet-based information demanded by the information society has led to an exponential growth of both internet traffic and the volume of stored/retrieved data. Data centres house and support the information technology and network telecommunications equipment for data processing, data storage and data transport. They are required both by network operators (delivering those services to customer premises) and by enterprises within those customer premises.

Data centres need to provide modular, scalable and flexible facilities and infrastructures to easily accommodate the rapidly changing requirements of the market. In addition, energy consumption of data centres has become critical, both from an environmental point of view (reduction of carbon footprint), and with respect to economic considerations (cost of energy) for the data centre operator.

The implementation of data centres varies in terms of:

a) purpose (enterprise, co-location, co-hosting or network operator facilities);

b) security level;

c) physical size; and

d) accommodation (mobile, temporary and permanent constructions).

NOTE Cloud services can be provided by all data centre types mentioned.

The needs of data centres also vary in terms of availability of service, the provision of security and the objectives for energy efficiency. These needs and objectives influence the design of data centres in terms of building construction, power distribution, environmental control, telecommunications cabling and physical security. Effective management and operational information are required to monitor achievement of the defined needs and objectives.

Most of the value of a data centre is created by proper operation.

During its decades-long operation, IT, business, society, and the technology of buildings and facilities themselves will change, so constant optimization is required.

Based on that, data centres must be planned, designed, and built based on business requirements and the operational requirements that must be realized. In that sense, this standard is also a design guide.

In addition, there are two basic facts to keep in mind when considering and understanding the operation of a data centre.

-Humans are fallible creatures.

-Things will break someday.

Based on these two points, it is important to recognize that proper operational management that compensates for them, increases availability and security, and reduces risks is the key to realizing the value of a data centre, and that the individual measures described in this standard will be effective.

The ISO/IEC 22237 series specifies requirements and recommendations to support the various parties involved in the design, planning, procurement, integration, installation, operation and maintenance of facilities and infrastructures within data centres. These parties include:

1) owners, operators, facility managers, ICT managers, project managers, main contractors;

2) consultants, architects, building designers and builders, system/installation designers, auditors, test and commissioning agents;

© ISO/IEC 2026 – All rights reserved

3) suppliers of equipment; and

4) installers, maintainers.

The inter-relationship of the various documents within the ISO/IEC 22237 series at the time of publication is shown in Figure 1.

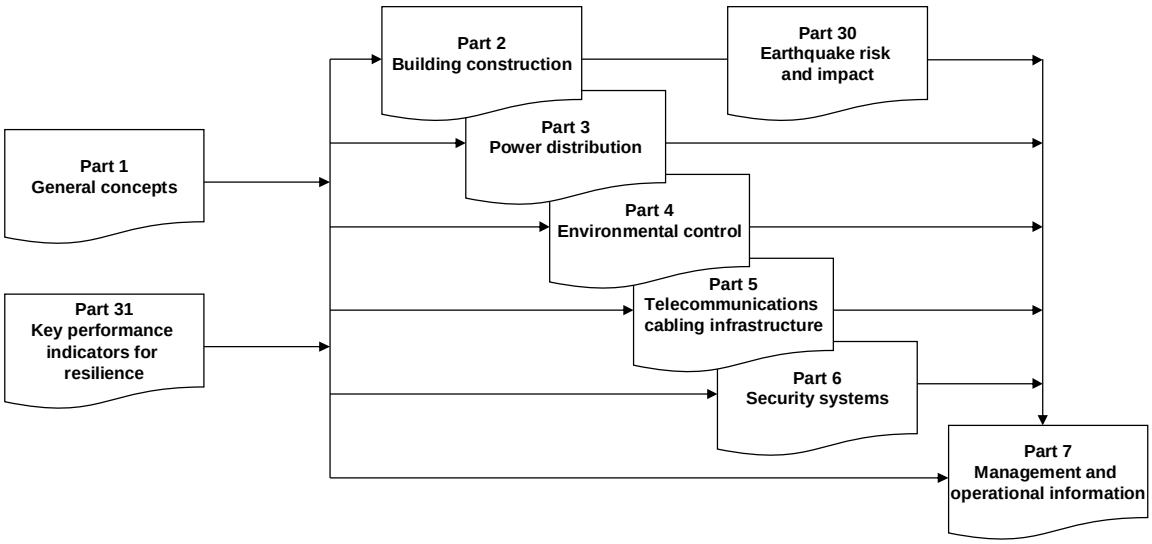


Figure 1 — Schematic relationship between the documents of the ISO/IEC 22237 series

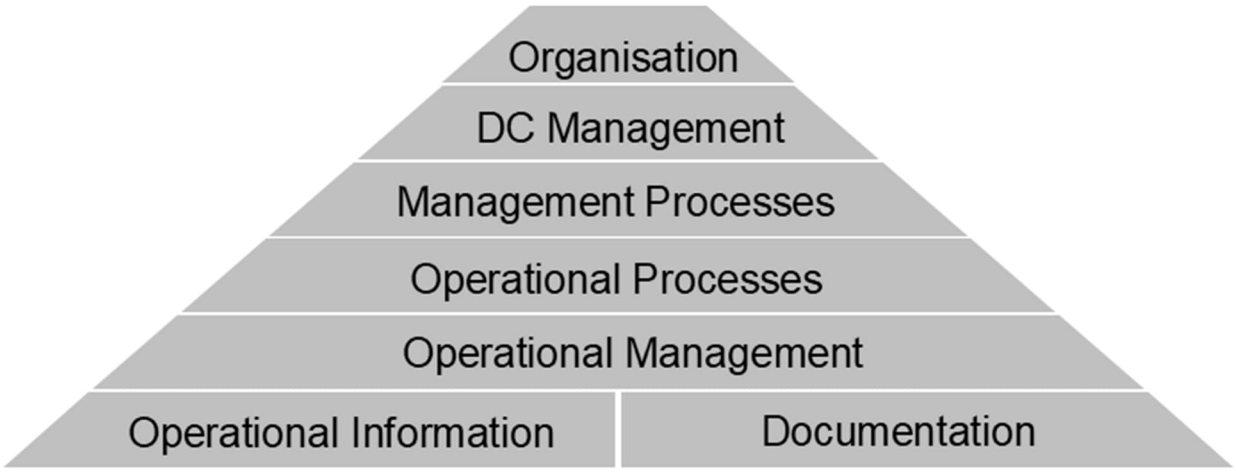
The ISO/IEC 22237-X documents specify requirements and recommendations for particular facilities and infrastructures to support the relevant classification for “availability”, “physical security” and “energy efficiency enablement” selected from ISO/IEC 22237-1.

This International Standard addresses the operational and management information (in accordance with the requirements of ISO/IEC 22237-1). A data centre’s primary function typically is to house large quantities of computer and telecommunications hardware which affects the construction, operation, and physical security. Most of the data centres may impose special security requirements. Therefore, the planning of a data centre by the designer and the various engineering disciplines that will assist in the planning and implementation of the design of the data centre i.e. electrical, mechanical, security, etc. shall be carried out in cooperation with the IT and telecommunications personnel, network professionals, the facilities manager, the IT end users, and any other personnel involved.

Figure 2 shows an overview of the document:

- The organization provides the data centre strategy and resources for data centre management and operation.
- Data Centre management organizes all process and resources for data centre operation.
- Operational information and documentation support all data centre activities.

© ISO/IEC 2026 – All rights reserved



318

319 **Figure 2 — Data centre management overview**

320 The transition from planning and building to operation of a data centre is considered as part of the acceptance
321 test process in Clause 9.7.

322 This document is intended for use by and collaboration between facility managers, ICT managers, and main
323 contractors.

324 The ISO/IEC 22237 series does not address the selection of information technology and network
325 telecommunications equipment, software and associated configuration issues.

© ISO/IEC 2026 – All rights reserved

1 Scope

This document specifies processes for the management and operation of data centres. The primary focus of this standard is the processes necessary to deliver the expected level of resilience, availability, risk management, risk mitigation, capacity planning, security and resource and energy efficiency.

The secondary focus is on organization and data centre management to align the actual and future demands. Only processes specific for data centres are in the scope of this document.

Business processes like people management, financial management, etc. are out of scope.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 14763-2, *Information technology — Implementation and operation of customer premises cabling - Part 2: Planning and installation*

ISO/IEC 22237-1, *Information technology — Data centre facilities and infrastructures — Part 1: General concepts*

ISO/IEC 22237-2, *Information technology — Data centre facilities and infrastructures — Part 2: Building construction*

ISO/IEC 22237-3:2021, *Information technology — Data centre facilities and infrastructures — Part 3: Power distribution*

ISO/IEC 22237-4, *Information technology — Data centre facilities and infrastructures — Part 4: Environmental control*

ISO/IEC 22237-5, *Information technology — Data centre facilities and infrastructures — Part 5: Telecommunications cabling infrastructure*

ISO/IEC 22237-6, *Information technology — Data centre facilities and infrastructures — Part 6: Security systems*

ISO/IEC 30134-3, *Information technology — Data centre facilities and infrastructures — Part 3: Renewable Energy Factor*

ISO/IEC 30134-6, Information technology — *Data centre facilities and infrastructures — Part 6: Energy Reuse Factor*

ISO/IEC 30134-7, *Information technology — Data centre facilities and infrastructures — Part 7: Cooling Efficiency Ratio*

ISO/IEC 30134-8, *Information technology — Data centre facilities and infrastructures — Part 8: Carbon usage effectiveness*

ISO/IEC 30134-9, *Information technology — Data centre facilities and infrastructures — Part 9: Water Usage Effectiveness*

© ISO/IEC 2026 – All rights reserved

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 22237-1, ISO/IEC 22237-2 to ISO/IEC 22237-6 and the following apply.

3.1.1
availability management
process for monitoring, analysis, reporting and improvement of availability

3.1.2
capacity management
process for monitoring, analysis, reporting and improvement of capacity

3.1.3
change management
process for recording, coordination, approval and monitoring of all changes

3.1.4
configuration item
entity managed by configuration management

3.1.5
configuration management
process for logging and monitoring of configuration items

3.1.6
cost distribution model
model to distribute costs that cannot be directly related to an infrastructure item

3.1.7
cost management
process for monitoring, analysis and reporting of all infrastructure related costs

3.1.8
customer management
process for management of customers responsibilities

3.1.9
data centre strategy
process for alignment of actual data centre’s capabilities and future demands of data centre’s users and owners

3.1.10
energy management
process for monitoring, analysis, reporting and improvement of energy efficiency

3.1.11
event
something that happens and leads to one or more failures or faults

[SOURCE: ISO/IEC TS 22237-31:2023, 3.1.7]

3.1.12
incident management
process for responding to unplanned events and recovery of normal operation condition

© ISO/IEC 2026 – All rights reserved

3.1.13
incident severity
incident category, e.g. based on categories of the risk map described in ISO/IEC 22237-1

3.1.14
key performance indicator
parameter used to evaluate performance

3.1.15
operations management
process for infrastructure maintenance, monitoring and event management

3.1.16
product lifecycle management
process for managing the timely renewal of infrastructure components and review of product lifecycle costs

3.1.17
provisioned capacity
capacity of the data centre's actual installed infrastructure

3.1.18
resilience
ability to withstand and reduce the magnitude and/or duration of disruptive events, including the capability to anticipate, absorb, adapt to, and/or rapidly recover from such an event

[SOURCE: IEEE Task Force on Definition and Quantification of Resilience, PES-TR65:2018-04]

3.1.19
resilience level
enumeration of attributes for the determination of resilience aspects of a defined service at a defined operation point (OP)

[SOURCE: ISO/IEC TS 22237-31:2023, 3.1.26]

3.1.20
security incident
unplanned event resulting in an actual or potential breach of security

3.1.21
security management
process for design and monitoring of security policies, analysis, reporting and improvement of security

3.1.22
service level management
process for monitoring, analysis and reporting of service level compliance

3.1.23
service level agreement
agreement defining the content and quality of the service to be delivered and the timescale in which it is to be delivered

3.1.24
total capacity
maximum capacity the data centre was designed for at full use in terms of e.g. space, power and cooling

3.1.25
used capacity
data centre's current capacity used by the IT and facility in terms of e.g. space, power and cooling

© ISO/IEC 2026 – All rights reserved