TECHNICAL SPECIFICATION

ISO/IEC TS 22237-1

First edition
2018-05

Information technology — Data centre facilities and infrastructures —

Part 1: General concepts

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

Partie 1: Concepts généraux



Reference number
ISO/IEC TS 22237-1:2018(E)

© ISO/IEC 2018



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018

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
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms, definitions and abbreviated terms ... **2**
3.1 Terms and definitions ... 2
3.2 Abbreviated terms ... 5

4 Conformance ... **6**

5 Business risk analysis ... **6**
5.1 General ... 6
5.2 Downtime cost analysis ... 6
5.3 Risk analysis ... 7

6 Data centre design overview ... **8**
6.1 General ... 8
6.2 Spaces and facilities ... 8

7 Classification system for data centres ... **11**
7.1 General ... 11
7.2 Availability ... 11
7.3 Physical security ... 13
7.3.1 General ... 13
7.3.2 Protection against unauthorised access ... 13
7.3.3 Protection against environmental events ... 13
7.4 Energy efficiency enablement ... 14
7.4.1 General ... 14
7.4.2 Power distribution system ... 15
7.4.3 Environmental monitoring and control ... 15

Annex A (informative) **General design principles** ... **16**

Bibliography ... **21**

© ISO/IEC 2018 – 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 39, *Sustainability for and by Information Technology.*

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

© ISO/IEC 2018 – 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 are housing and supporting 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 economical 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;

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

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 and physical security. Effective management and operational information is required to monitor achievement of the defined needs and objectives.

The ISO/IEC TS 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, facility managers, ICT managers, project managers, main contractors;

2) consultants, architects, building designers and builders, system and installation designers;

3) suppliers of equipment;

4) installers, maintainers.

At the time of publication of this document, the ISO/IEC TS 22237 series will comprise the following documents:

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

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

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

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

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

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

© ISO/IEC 2018 – All rights reserved

— ISO/IEC TS 22237-7: *Information technology — Data centre facilities and infrastructures — Part 7: Management and operational information*.

The inter-relationship of the specifications within the ISO/IEC TS 22237 series is shown in Figure 1.

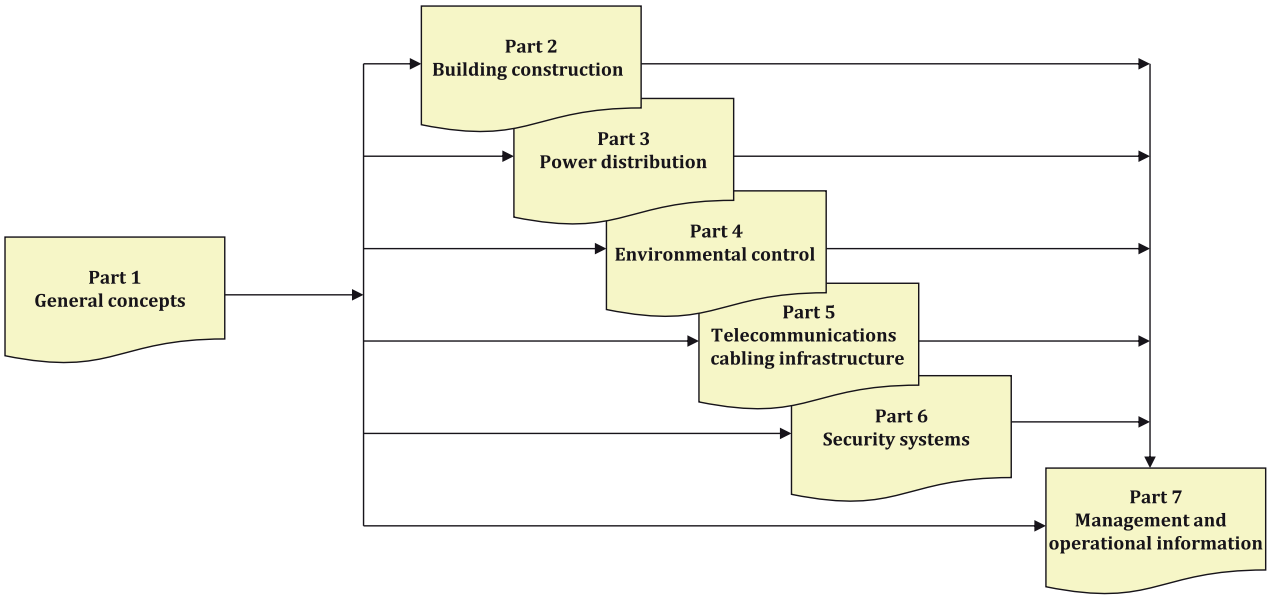


Figure 1 — Schematic relationship between the ISO/IEC TS 22237 series of documents

This document, defines the general concepts for the design and operation of data centres. This includes a business risk and operational cost analysis as well as a classification system for data centres with respect to "availability", "physical security" and "energy efficiency enablement".

ISO/IEC TS 22237-2 to ISO/IEC TS 22237-7 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 TS 22237-1.

ISO/IEC TS 22237-7 addresses the operational and management information (in accordance with the requirements of ISO/IEC TS 22237-1).

This document is intended for use by and collaboration between architects, building designers and builders, system and installation designers.

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

© ISO/IEC 2018 – All rights reserved

Information technology — Data centre facilities and infrastructures —

Part 1: General concepts

1 Scope

This document:

a) details the issues to be addressed in a business risk and operating cost analysis enabling application of an appropriate classification of the data centre;

b) defines the common aspects of data centres including terminology, parameters and reference models (functional elements and their accommodation) addressing both the size and complexity of their intended purpose;

c) describes general aspects of the facilities and infrastructures required to support effective operation of telecommunications within data centres;

d) specifies a classification system, based upon the key criteria of "availability", "security" and "energy-efficiency" over the planned lifetime of the data centre, for the provision of effective facilities and infrastructure;

e) describes the general design principles for data centres upon which the requirements of the ISO/IEC TS 22237 series are based including symbols, labels, coding in drawings, quality assurance and education.

The following topics are outside of the scope of the ISO/IEC TS 22237 series:

1) the selection of information technology and network telecommunications equipment, software and associated configuration issues;

2) safety and electromagnetic compatibility (EMC) requirements (covered by other standards and regulations). However, information given in the ISO/IEC TS 22237 series may be of assistance in meeting these standards and regulations).

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

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

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

© ISO/IEC 2018 – All rights reserved

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

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

3.1.1
availability
ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided

[SOURCE: IEC 60050-191:1990, 191-02-05]

3.1.2
building entrance facility
facility that provides all necessary mechanical and electrical services for the entry of telecommunications cables into a building and which may allow for transition from external to internal cable

3.1.3
building security
facilities and systems necessary to provide the required levels of security at the entrance to and within the building containing the data centre

3.1.4
cabinet
enclosed construction for housing closures and other information technology equipment

[SOURCE: ISO/IEC 14763-2:2012, 3.1.7, modified — removed the words "intended" and "components and".]

3.1.5
co-hosting data centre
data centre in which multiple customers are provided with access to network(s), servers and storage equipment on which they operate their own services/applications

Note 1 to entry: Both the information technology equipment and the support infrastructure of the building are provided as a service by the data centre operator.

3.1.6
co-location data centre
data centre in which multiple customers locate their own network(s), servers and storage equipment

Note 1 to entry: The support infrastructure of the building (such as power distribution and environmental control) is provided as a service by the data centre operator.

3.1.7
computer room space
area within the data centre that accommodates the data processing, data storage and telecommunication equipment that provides the primary function of the data centre

© ISO/IEC 2018 – All rights reserved

3.1.8
control room space
area within the data centre used to control the operation of the data centre and to act as a central point for all control and monitoring functions

3.1.9
data centre
structure, or group of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network telecommunications equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control together with the necessary levels of resilience and security required to provide the desired service availability

Note 1 to entry: A structure can consist of multiple buildings and/or spaces with specific functions to support the primary function.

Note 2 to entry: The boundaries of the structure or space considered the data centre, which includes the information and communication technology equipment and supporting environmental controls, can be defined within a larger structure or building.

[SOURCE: ISO/IEC 30134-1:2016, 3.1.4]

3.1.10
data centre security
necessary facilities and systems that provide the required levels of security at the entrance to and within the data centre

3.1.11
demarcation point
point where the operational control or ownership changes

3.1.12
electrical distribution space
area used for housing facilities to distribute electrical power between the transformer space and electrical spaces within the data centre or elsewhere within the premises or individual buildings within the premises

3.1.13
electrical space
area within the data centre used for housing facilities to deliver and control electrical power to the data centre spaces [including switchboards, batteries, uninterruptible power supplies (UPS) etc.]

3.1.14
enterprise data centre
data centre that is operated by an enterprise which has the sole purpose of the delivery and management of services to its employees and customers

3.1.15
external premises security
facilities and systems that provide the required levels of security for the area between the building and the boundary of the premises

3.1.16
energy efficiency enablement
ability to measure the energy consumption and to allow calculation and reporting of energy efficiency of the various facilities and infrastructures

3.1.17
facility
spaces and pathways that accommodate a specific infrastructure

© ISO/IEC 2018 – All rights reserved

3.1.18
functional capability
ability of the data centre (or system or sub-system) to deliver its intended function

3.1.19
generator space
area used for housing the installation of electrical power supply generation equipment together with associated storage of fuels or energy conversion equipment

3.1.20
holding space
area within the data centre used for the holding of equipment prior to being brought into service or having been taken out of service

3.1.21
infrastructure
technical systems providing functional capability of the data centre

EXAMPLE Power distribution, environmental control and physical security.

3.1.22
main distributor
distributor used to make connections between the main distribution cabling subsystem, network access cabling subsystem and cabling subsystems and active equipment

[SOURCE: ISO/IEC 11801-5:2017, 3.1.6, modified — removed "as specified in ISO/IEC 11801-1".]

3.1.23
mechanical space
area that is used for housing mechanical equipment and infrastructure that provides environmental control for the data centre spaces (including chillers and water treatment, air handling and fire suppression systems)

3.1.24
network operator data centre
data centre that has the primary purpose of the delivery and management of broadband services to the operators customers

3.1.25
physical security
measures (combining physical and technological controls), procedures and responsibilities to maintain the desired level of availability for the facilities and infrastructures of the data centres in relation to access control and environmental events

3.1.26
planned downtime
period of time during which a system or sub-system does not provide functional capability whilst it undergoes maintenance or is switched off to test the response of a related system or sub-system

3.1.27
premises entrance facility
space that provides all necessary mechanical and electrical services for the entry of cables into the premises

3.1.28
storage space
secured area where general goods and/or data centre goods can be stored

© ISO/IEC 2018 – All rights reserved

3.1.29
telecommunications
branch of technology concerned with the transmission, emission and reception of signs, signals, writings, images and sounds, that is, information of any nature by cable, radio, optical or other electromagnetic systems

[SOURCE: ISO/IEC 11801-1:2017, 3.1.78, modified — Note 1 to entry deleted.]

3.1.30
telecommunications cabling
telecommunications cabling infrastructure from the telecommunications space(s) to the premises entrance facility

3.1.31
telecommunication equipment
equipment within the data centre that provides telecommunication services within the data centre

3.1.32
telecommunications space
area which may house demarcation points and telecommunication equipment associated with the building entrance facility and which may allow service providers restricted access to the data centre

3.1.33
testing space
area within the data centre used for the testing and configuring of equipment prior to being brought into service

3.1.34
transformer space
area used for housing equipment necessary to convert primary electrical circuits to levels appropriate for connection to the equipment within the premises or individual buildings within the premises

3.1.35
uninterruptible power system
combination of convertors, switches and energy storage devices (such as batteries), constituting a power system for maintaining continuity of load power in case of input power failure

Note 1 to entry: Continuity of load power occurs when voltage and frequency are within rated steady-state and transient tolerance bands and with distortion and interruptions within the limits specified for the load. Input power failure occurs when voltage and frequency are outside rated steady-state and transient tolerance bands or with distortion or interruptions outside the limits specified for the UPS.

[SOURCE: IEC 62040-1:2008, 3.1.1]

3.1.36
unplanned downtime
time taken, following a failure of functional capability, to repair the relevant infrastructure together with the “re-boot” time necessary to recover functional capability following that repair

3.2 Abbreviated terms

For the purposes of this document the following abbreviated terms apply.

CRAC	Computer Room Air Conditioner/Conditioning
ffs	for further study
MTBF	Mean Time Between Failures

© ISO/IEC 2018 – All rights reserved

MTTR	Mean Time To Recovery
NOC	Network Operating Centre
UPS	Uninterruptible Power Supply

4 Conformance

For a data centre design to conform to this document:

a) a business risk analysis according to Clause 5 shall be completed;

b) an appropriate Availability Class in 7.2 shall be selected using a business risk analysis in Clause 5;

c) an appropriate Protection Class in 7.3 shall be selected using a business risk analysis in Clause 5;

d) an appropriate energy efficiency enablement level in 7.4 shall be selected;

e) the general design principles in Annex A shall be applied.

5 Business risk analysis

5.1 General

The overall availability of a data centre is a measure of the continuity of its data processing, storage, and transport functions. The acceptable level of the overall availability of a data centre is determined by a number of factors including:

a) a downtime cost analysis (see 5.2) - the cost associated with a failure of service provision, which depends upon a number of factors including the function and importance of the data centre;

b) externally applied commercial pressures (e.g. insurance costs).

The availability of each of the facilities and infrastructures of the data centre required to support the desired overall availability is described by an availability classification (see 7.2). The design of each of the data centre infrastructures shall take account of their impact on overall availability and the costs associated with the predicted downtime associated with failure or planned maintenance. The design and physical security of the facilities and infrastructures of the data centre may be subjected to a risk analysis (see 5.3) which maps identified risk events against the requirements of the availability classification (see 7.2). This analysis identifies the aspects of the facilities and infrastructures that require investment in terms of design improvements to reduce their impact and/or probability of those risk events.

5.2 Downtime cost analysis

This standard does not define methods of analysis for the cost of downtime. Standards such as IEC 31010 provide useful guidance.

The elements to be considered within such an analysis will depend upon the purpose of the data centre. Some organisations may be able to assign a monetary value (or range) to loss of service which may include the following:

a) immediate financial penalties;

b) consequential losses;

c) an assessment of longer term damage to business reputation e.g. an Internet Service Provider or a financial institution.

 © ISO/IEC 2018 – All rights reserved