FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEC
FDIS
22237-6**

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

Secretariat: **ANSI**

Voting begins on:
2023-11-09

Voting terminates on:
2024-01-04

Information technology — Data centre facilities and infrastructures —

Part 6: Security systems

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

Partie 6: Systèmes de sécurité

Reference number
ISO/IEC FDIS 22237-6:2023(E)

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

Contents

Page

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 22237-6:2018, which has been technically revised.

The main changes are as follows:

— a new Clause 7, "Protection against intrusion to data centre spaces", has been added. Clause 6 has been restructured accordingly;

— references to relevant provisions of ISO/IEC 22237-2 have been added to highlight the respective links to constructional requirements;

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.

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.

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;

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.

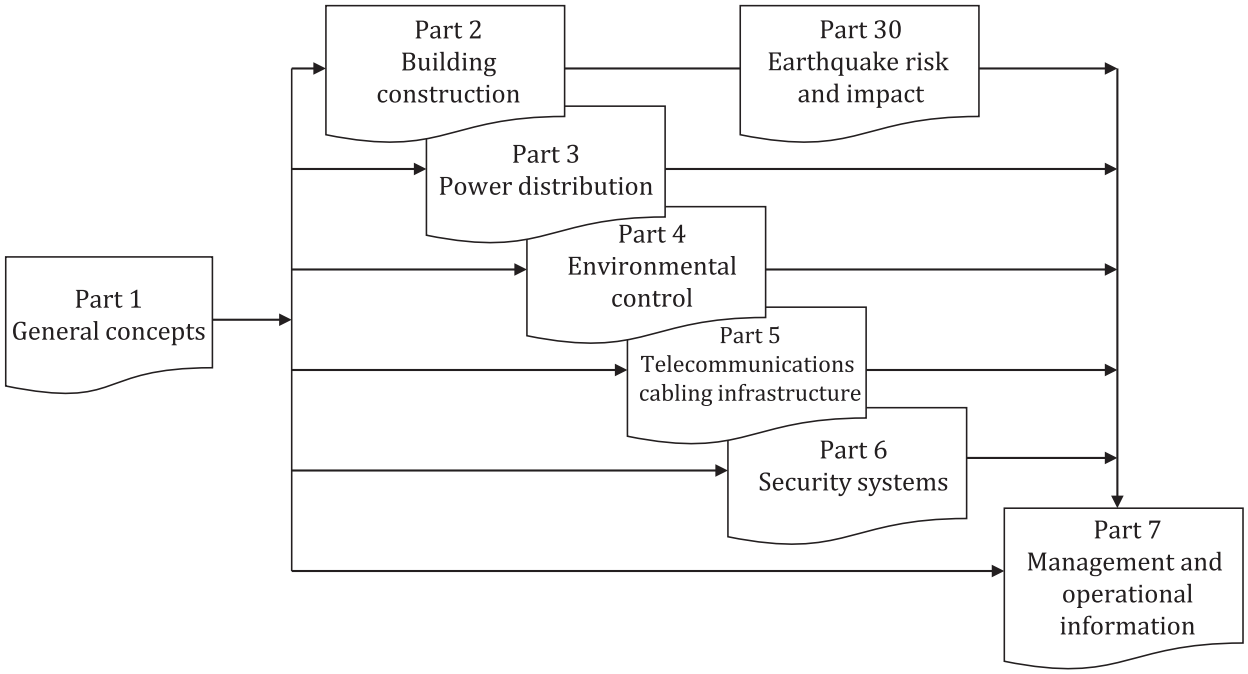

Figure 1 — Schematic relationship between the documents of the ISO/IEC 22237 series

ISO/IEC 22237-2 to ISO/IEC 22237-6 specify requirements and recommendations for particular facilities and infrastructures to support the relevant classification for “availability”, “physical security” and “energy efficiency enablement” according to ISO/IEC 22237–1.

This document, ISO/IEC 22237-6, addresses the physical security of facilities and infrastructure within data centres together with the interfaces for monitoring the performance of those facilities and infrastructures in line with ISO/IEC TS 22237-7 (in accordance with the requirements of ISO/IEC 22237-1).

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

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

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

Information technology — Data centre facilities and infrastructures —

Part 6: Security systems

1 Scope

This document specifies requirements and recommendations concerning the physical security of data centres based on the criteria and classifications for "availability", "security" and "energy efficiency enablement" within ISO/IEC 22237-1.

This document provides designations for the data centres spaces defined in ISO/IEC 22237-1.

This document specifies requirements and recommendations for such data centre spaces, and the systems employed within those spaces, in relation to protection against:

a) unauthorized access addressing organizational and technological solutions;

b) intrusion;

c) internal fire events igniting within data centres spaces;

d) internal environmental events (other than fire) within the data centre spaces which would affect the defined level of protection;

e) external environmental events outside the data centre spaces which would affect the defined level of protection.

NOTE Constructional requirements and recommendations are provided by reference to ISO/IEC 22237-2.

Safety and electromagnetic compatibility (EMC) requirements are outside the scope of this document and are covered by other standards and regulations. However, information given in this document can be of assistance in meeting these standards and regulations.

Conformance of data centres to the present document is covered in Clause 4.

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 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, *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*

IEC 60839-11-1, *Alarm and electronic security systems — Part 11-1: Electronic access control systems — System and components requirements*

IEC 60839-11-2, *Alarm and electronic security systems - Part 11-2: Electronic access control systems - Application guidelines*

IEC 62305 (all parts), *Protection against lightning*

IEC 62676-1-1, *Video surveillance systems for use in security applications — Part 1-1: System requirements — General*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

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

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

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

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

3.1.1
authorized person
person having been assessed and subsequently provided with access credentials to specific areas within the data centre

3.1.2
forcible threat
threat exhibited by physical force

3.1.3
frame
open construction, typically wall-mounted, for housing closures and other information technology equipment

3.1.4
free-standing barrier
wall, fence, gate, turnstile or other similar self-supporting barrier, and their associated foundations, designed to prevent entry to a space of a given Protection Class

[SOURCE: ISO/IEC 22237-2:2023, 3.1.2]

3.1.5
hold time
time during which a concentration of fire extinguishant is maintained at an effective level with the space being protected

3.1.6
information technology equipment
equipment providing data storage, processing and transport services together with equipment dedicated to providing direct connection to core and/or access networks

3.1.7
make-up air
air introduced into a data centre space to replace air that is exhausted through ventilation or combustion processes

3.1.8
rack
open construction, typically self-supporting and floor-mounted, for housing closures and other information technology equipment

3.1.9
residual risk
remaining risk(s) posed to the data centre assets requiring protection following the deployment of appropriate countermeasures

3.1.10
surreptitious attack
compromise of an asset via logical or physical means with the objective that the attack remains undetected

3.1.11
surreptitious threat
threat of a surreptitious attack by entities via logical or physical means leading to the compromise of that asset

3.2 Abbreviated terms

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

EMC	electromagnetic compatibility
I&HAS	intruder and holdup alarm systems
VSS	video surveillance system

4 Conformance

For a data centre to conform to this document:

1) the required Protection Classes of Clause 5 shall be applied to each of the spaces of the data centre according to the risk analysis of 5.2;

2) the requirements of the relevant Protection Class of Clauses 6, 7, 8, 9 and 10 shall be applied;

3) the systems to support the requirements of Clause 6 shall be in accordance with Clause 11.

5 Physical security

5.1 General

The degree of physical security applied to the facilities and infrastructures of a data centre has an influence on both the availability of the data centre and the integrity/security of the data stored and processed within, the data centre.

Subclause 5.3 provides minimum requirements for the data centres spaces defined in ISO/IEC 22237-1. The requirements and recommendations for those data centre spaces, and the systems employed within those spaces, address protection against:

a) unauthorized access (see Clause 6);

b) intrusion (see Clause 7);

c) fire events originating within data centres spaces (see Clause 8);

d) environmental events (other than fire) within the data centre spaces which would affect the defined level of protection (see Clause 9);

e) environmental events outside the data centre spaces which would affect the defined level of protection (see Clause 10).

Constructional requirements for walls and penetrations are provided in ISO/IEC 22237-2 and relevant cross-references are provided throughout this document.

5.2 Risk analysis and management

The requirements for security should be determined:

— by the organization responsible for data centre assets;

— following a risk assessment based on the threats posed to the data (and the "classification" of the data) and the processes hosted by the data centre. See ISO/IEC 22237-1 for further information regarding risk assessment methodologies.

Figure 2 illustrates the concept of the risk analysis and management and is described as follows:

a) asset value analysis: a classification ("native", or "raised" due to the effects of data aggregation) of the assets should be determined at an early stage, so that it is possible to deploy appropriate protection countermeasures;

b) likelihood analysis: the probability of some form of attack against the protected assets;

c) forcible threat and surreptitious threat analysis: for example, posed by unauthorized access to the assets resulting in loss or unavailability of the assets;

d) vulnerability analysis: for example, inadequate physical security or technical controls of the hosted data.

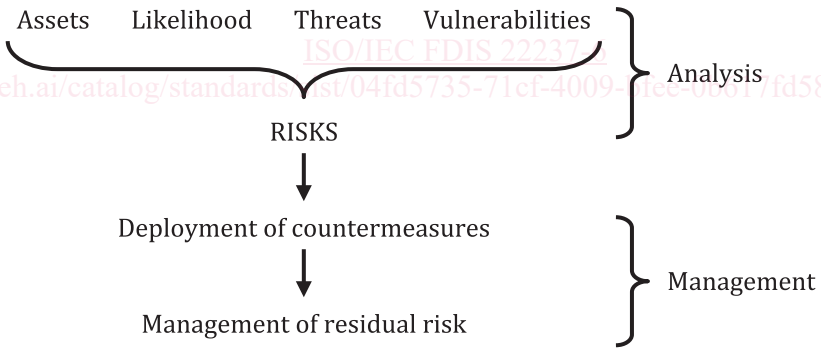

Figure 2 — Risk analysis and management concepts

These four items are analysed to identify the baseline risk posed to the data centre. Management of the identified baseline risk employs appropriate technical, physical and procedural countermeasures or a combination thereof at the appropriate security level.

Following the deployment of baseline countermeasures, further decisions shall be taken relating to the residual risk(s) as follows, driven by the acceptance of risk of the asset owner:

1) toleration — the remaining risk(s) are accepted and no additional countermeasures deployed;

2) treatment — additional measures are deployed to counter the remaining risk(s);

3) transferral — the risk(s) are transferred to another party, for example obtaining additional insurance cover to mitigate the risk(s);