TECHNICAL SPECIFICATION

ISO/IEC TS 22237-6

First edition
2018-05

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 TS 22237-6:2018(E)

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

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.

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);

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

3) facility and infrastructure integrators, 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 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.

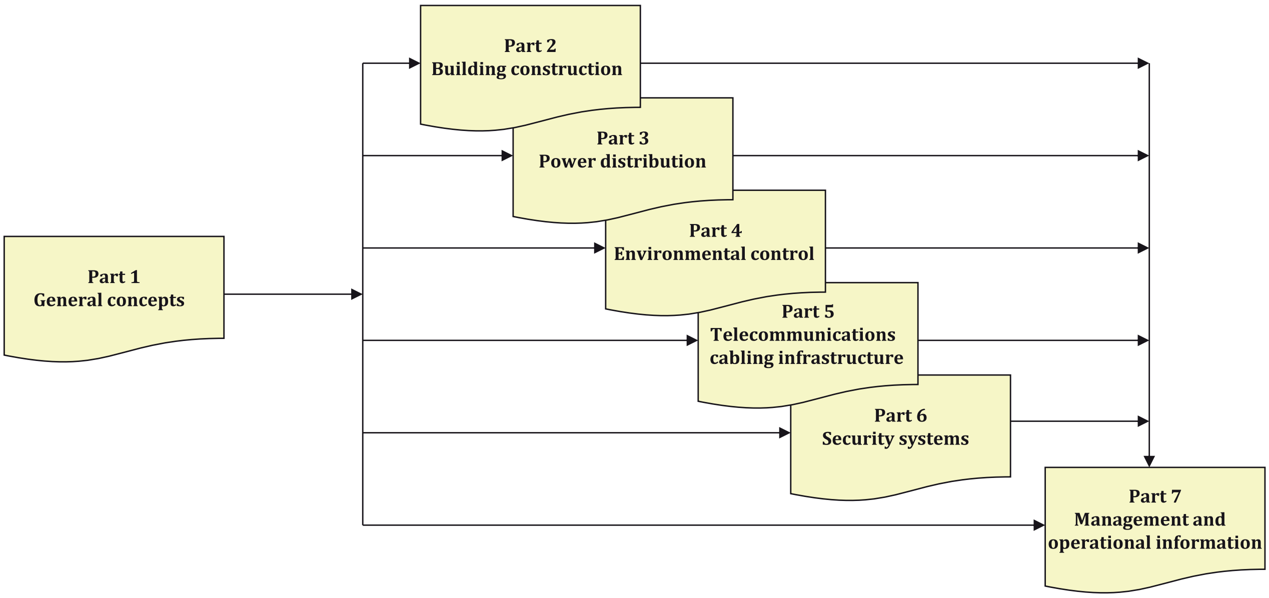

Figure 1 — Schematic relationship between the ISO/IEC TS 22237 series of documents

ISO/IEC TS 22237-2 to ISO/IEC TS 22237-6 specify requirements and recommendations for particular facilities and infrastructures to support the relevant classification for “availability”, “physical security” and “energy efficiency enablement” selected from EN 50600-1.

This document, 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 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 and security managers among others.

The ISO/IEC TS 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 addresses the physical security of data centres based upon the criteria and classifications for “availability”, “security” and “energy efficiency enablement” within ISO/IEC TS 22237-1.

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

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

a) unauthorized access addressing constructional, organizational and technological solutions;

b) fire events igniting within data centre spaces;

c) other events within or outside the data centre spaces, which would affect the defined level of protection.

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 may be of assistance in meeting these standards and regulations.

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

ISO/IEC TS 22237-2:2018, *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*

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

IEC 62676-1-1:2014, *Video surveillance systems for use in security applications — Part 1-1: System requirements — General*

EN 3 (all parts), *Portable fire extinguishers*

EN 54 (all parts), *Fire detection and fire alarm systems*

EN 54-13, *Fire detection and fire alarm systems — Part 13: Compatibility assessment of system components*

EN 54-20:2006, *Fire detection and fire alarm systems — Part 20: Aspirating smoke detectors*

EN 1047-2, *Secure storage units — Classification and methods of test for resistance to fire — Part 2: Data rooms and data container*

EN 1366-3, *Fire resistance tests for service installations — Part 3: Penetration seals*

EN 1627:2011, *Pedestrian doorsets, windows, curtain walling, grilles and shutters — Burglar resistance — Requirements and classification*

EN 1634 (all parts), *Fire resistance and smoke control tests for door and shutter assemblies, openable windows and elements of building hardware*

EN 12845, *Fixed firefighting systems — Automatic sprinkler systems — Design, installation and maintenance*

EN 13565-2, *Fixed firefighting systems — Foam systems — Part 2: Design, construction and maintenance*

CEN/TS 14816, *Fixed firefighting systems — Water spray systems — Design, installation and maintenance*

CEN/TS 14972, *Fixed firefighting systems — Watermist systems — Design and installation*

EN 16750, *Fixed firefighting systems — Oxygen reduction systems — Design, installation, planning and maintenance*

EN 50131 (all parts), *Alarm systems — Intrusion and hold-up systems*

EN 50136 (all parts), *Alarm systems — Alarm transmission systems and equipment*

EN 50518 (all parts), *Monitoring and alarm receiving centre*

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 TS 22237-1 and the following 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
forcible threat
threat exhibited by physical force

3.1.2
hold time
time during which a concentration of fire extinguishant is maintained at an effective level with the space being protected

3.1.3
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

3.1.4
residual risk
remaining risk(s) posed to the data centre assets requiring protection following the deployment of appropriate countermeasures

3.1.5
security manager
individual with overall responsible for all operational security aspects of the data centre, including logical and physical control mechanisms or processes

3.1.6
surreptitious attack
compromise of an asset via logical or physical means with the objective that the attack remains undetected

3.1.7
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 TS 22237-1 and the following apply.

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 Class of Clause 5 shall be applied to each of the spaces of the data centre;

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

3) the systems to support the requirements of Clause 6 shall be in accordance with Clause 10;

4) local regulations, including safety, shall be met.

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 function of, and the integrity/security of the data stored and processed within, the data centre.

5.3 provides minimum requirements for the data centres spaces defined in ISO/IEC TS 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) fire events originating within data centres spaces (Clause 7);

c) other events within (see Clause 8) or outside (see Clause 9) the data centre spaces, which would affect the defined level of protection.

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

In order for a space within the data centre to be considered to be of a given Protection Class the architectural and engineering design of the space (or entry to that space) shall meet or exceed that Protection Class for all aspects detailed above.

5.2 Risk assessment

The requirements for operational security should be determined by the organization responsible for data centre assets. The requirements should be determined following a risk assessment based on the threats posed to the data, and the “classification” of that data. See ISO/IEC TS 22237-1 for further information regarding risk assessment methodologies.

Figure 2 illustrates the concept of the risk assessment which is described as follows:

a) asset value: the classification of the material should be determined at an early stage, so that is possible to deploy appropriate protection countermeasures. The nature of the “classification” maybe “native”, or “raised” due to the effects of data aggregation;

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

c) threat (forcible or surreptitious) 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.

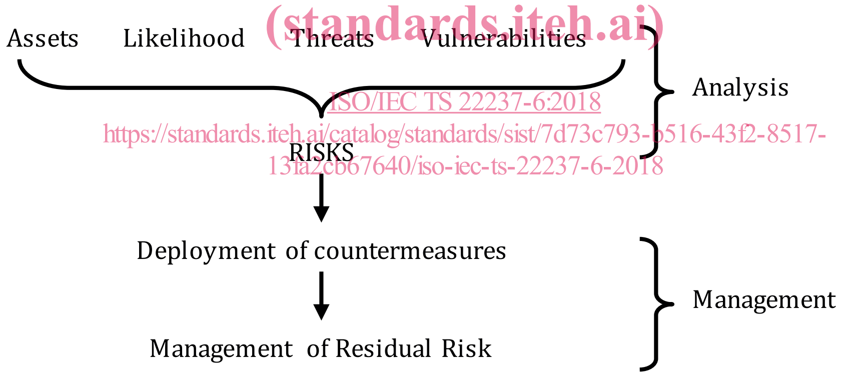

Figure 2 — Risk assessment concepts

These four items are analysed during the risk assessment process, 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.

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 the mitigate the risk(s);

4) termination — the activity posing the risk is terminated.

5.3 Designation of data centre spaces — Protection Classes

Each of the data centre spaces, independent of the size or purpose of the data centre, is designated as being of a particular Protection Class. There is no concept of a data centre of a given Protection Class.

The requirements for the Protection Class to be applied to the elements of the following facilities and infrastructures within the data centre are defined in:

a) ISO/IEC TS 22237-3 for the power distribution system;

b) ISO/IEC TS 22237-4 for the environmental control system.

All telecommunications equipment and connections to the telecommunications cabling infrastructure shall be in areas of Protection Class 3. Where pathways containing telecommunication cabling are routed in areas of a lower Protection Class they shall be monitored for unauthorized access.

In addition, the risk assessment of 5.2 together with the construction and configuration of the data centre described in 6.2 will require other spaces to be defined in terms of Protection Class. An example of this is shown in Table 1.

Table 1 — Examples of Protection Classes for data centre spaces

Protection Class 1	Protection Class 2	Protection Class 3	Protection Class 4
Personnel entrances to buildings or structures containing data centre spaces	The internal access to docking bays (the barrier of the docking bay providing the interface between Protection Classes 1 and 2) External premises security spaces Personnel entrances to the data centre spaces Storage spaces Holding spaces Testing spaces Data centre office spaces	Premises entrance facility[a,b] Building entrance facilities[b] Computer room spaces Control room space Data centre security spaces	Cabinets, cages or rows of cabinets within the computer room space

[a] This applies to premises entrance facilities which are within the control of the data centre.

[b] Access restrictions apply to pathways leading to areas of Protection Classes of a lower Protection Class.

6 Protection Class against unauthorized access

6.1 General

This document applies the four Protection Classes in relation to access to spaces accommodating the elements of the different facilities and infrastructures as detailed in Table 2 (in accordance with ISO/IEC TS 22237-1).