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 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

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 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 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.

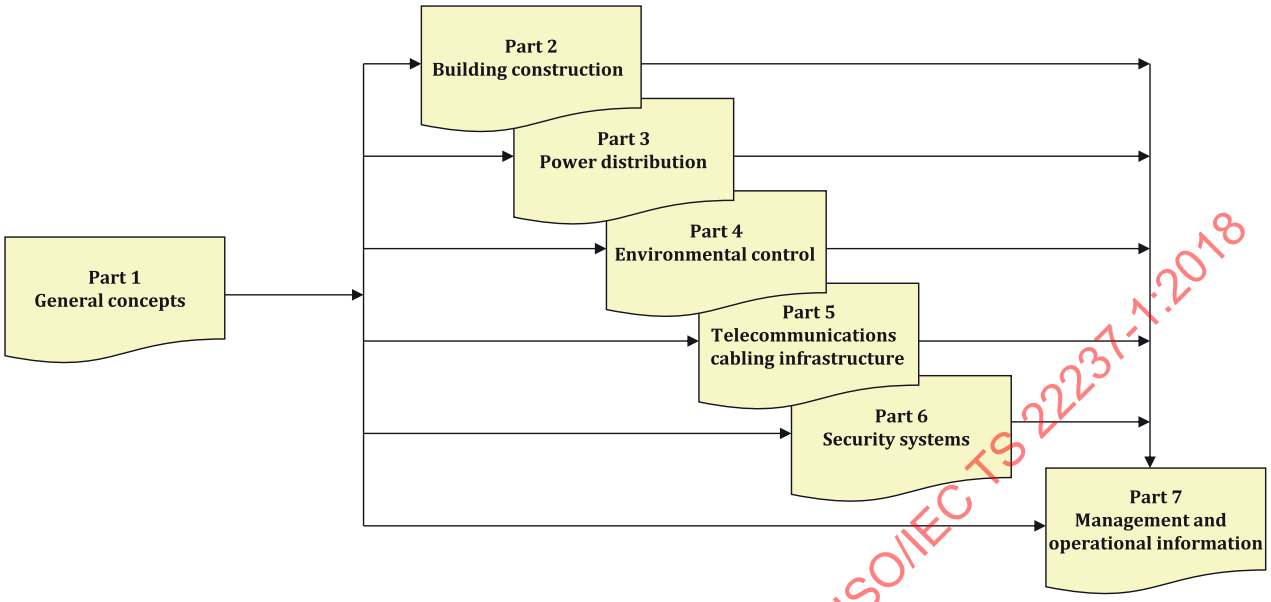

Figure 1 — Schematic relationship between the ISO/IEC TS 22237 series of documents

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.

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 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

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

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

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

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.

Although cost is often considered when analysing downtime, other impacts should also be considered. Data Centres containing life safety, legal, medical and criminal information may have individually recognised consequences from un-scheduled downtime.

5.3 Risk analysis

This standard does not define methods of risk analysis. Standards such as IEC 31010 provide useful guidance.

Risk analysis may be used as a management tool allowing the comparison with the acceptable total risk and showing trends resulting from mitigation activity. For the purposes of this standard the risk associated with an event concerning the facilities and infrastructures of the data centre which disrupts the provision of service of the data centre is defined as event risk which is a function of impact and probability where:

a) impact is the magnitude or severity of adverse incidents or impacts, expressed numerically or nominally expected duration of loss of service (availability) of the event;

b) probability is the likelihood of the event.

The impact of risk may be assessed using different units of measure e.g. cost, safety etc.

The total risk to the functional capability of the data centre is a function of the event risks associated with each facility and infrastructure provided that those risks are quantified on the same basis. If related to the output of the downtime cost analysis (see 5.2) the financial value of the total risk can be estimated.

The risks considered should include external threats which may affect the facilities and infrastructures including in particular the location, which could be geographical (air traffic, flooding etc.), political (wars, trouble spots, terror etc.) or affecting neighbourhood relations (if, for example, fire hazards exist due to filling stations, chemical storage etc.) and thus influence the likelihood of a potential downtime. In addition, potential risks resulting from attacks from the company's own staff and from outside should be part of the overall risk evaluation.

Impact can be categorised as:

1) low: Loss of non-critical services;

2) medium: Failure of critical system components but no loss of redundancy;

3) high: Loss of critical system redundancy but no loss of service to clients;

4) critical: Loss of critical service to one or more clients or loss of life (which may be extended to address personal injury).

The probability of an event occurring can be defined in a similar way, that is:

— very low;

— low;

— medium;

— high.

Each risk can be quantified on a risk map as shown in Figure 2. High risk events inhabit the top right hand corner of the figure and low risk events inhabit the bottom left hand corner.

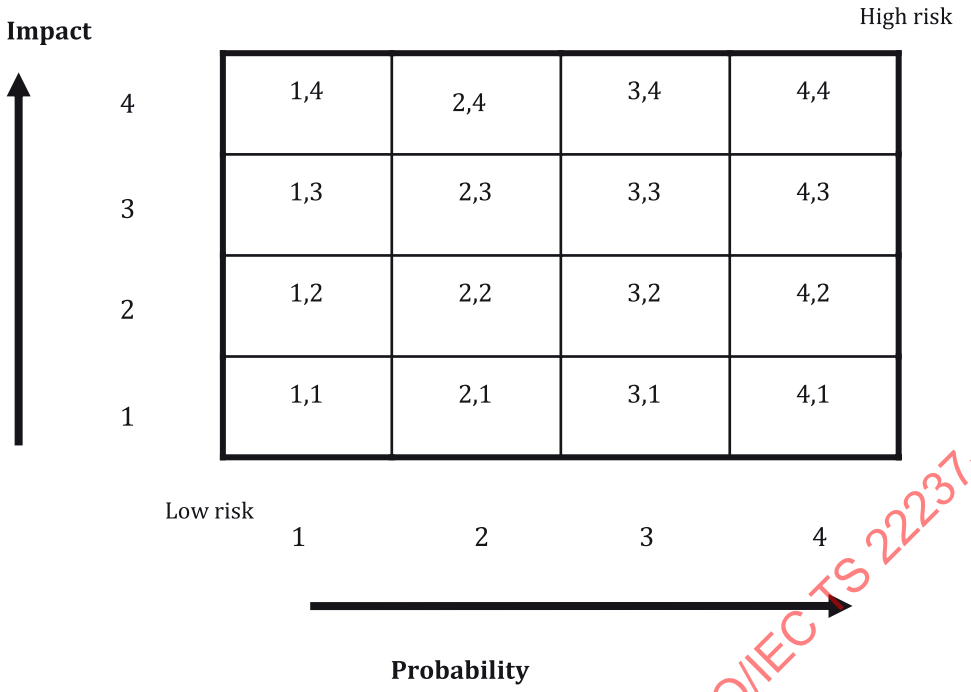

Figure 2 — Example of risk map

Having identified the risk of the possible events associated with data centre facilities and infrastructures, the downtime cost with that event shall be determined to enable design decisions to be made that reduce the risk (by means of reducing the impact or probability of the event).

6 Data centre design overview

6.1 General

A data centre comprises one or more buildings or one or more spaces within those buildings, whose primary function is to accommodate equipment that processes, delivers and/or stores information. Similarly, data centres have a variety of purposes including co-hosting, co-location, enterprise and network operator services.

Data centres can differ significantly with respect to their physical size. At the lower end of the size range, they can house a small quantity of storage and server equipment to provide information technology services to a building cabling infrastructure. At the upper end of the size range, they can house a large quantity of such equipment requiring sophisticated power distribution and environmental control facilities housed in one or more buildings dedicated to ensuring the operation of the data centre.

This clause provides a general design overview for data centres independent of their size.

NOTE The design of generic cabling is covered by ISO/IEC TS 22237-5, whereas the installation of such cabling is specified in ISO/IEC 14763-2.

6.2 Spaces and facilities

Figure 3 shows a schematic representation of the spaces required by a large data centre within a building and within premises containing one or more building.

The data centre may share certain spaces with the rest of the building including:

a) building entrance facilities;

b) personnel entrance(s);

c) docking/loading bay(s);

d) generators space(s) including fuel storage;

e) transformer space(s);

f) electrical distribution space(s);

g) telecommunications spaces(s).

The need for the above spaces and facilities within the building depends upon the purpose of both the building and the data centre. Any sharing of these spaces and facilities will depend on the size but also on the defined Availability and Protection Classes of the data centre and the functions of the remainder of the building. For example, in buildings housing large data centres, the facilities and spaces supporting the data centre may be dedicated to the data centre with separate spaces being provided for the remainder of the building.

The area within the building designated as a data centre may contain the following spaces:

1) personnel entrance(s);

2) main distributor space(s);

3) computer room space(s) and associated testing space(s);

4) electrical space(s);

5) mechanical space(s);

6) control room space(s);

7) office space(s);

8) storage and holding space(s).

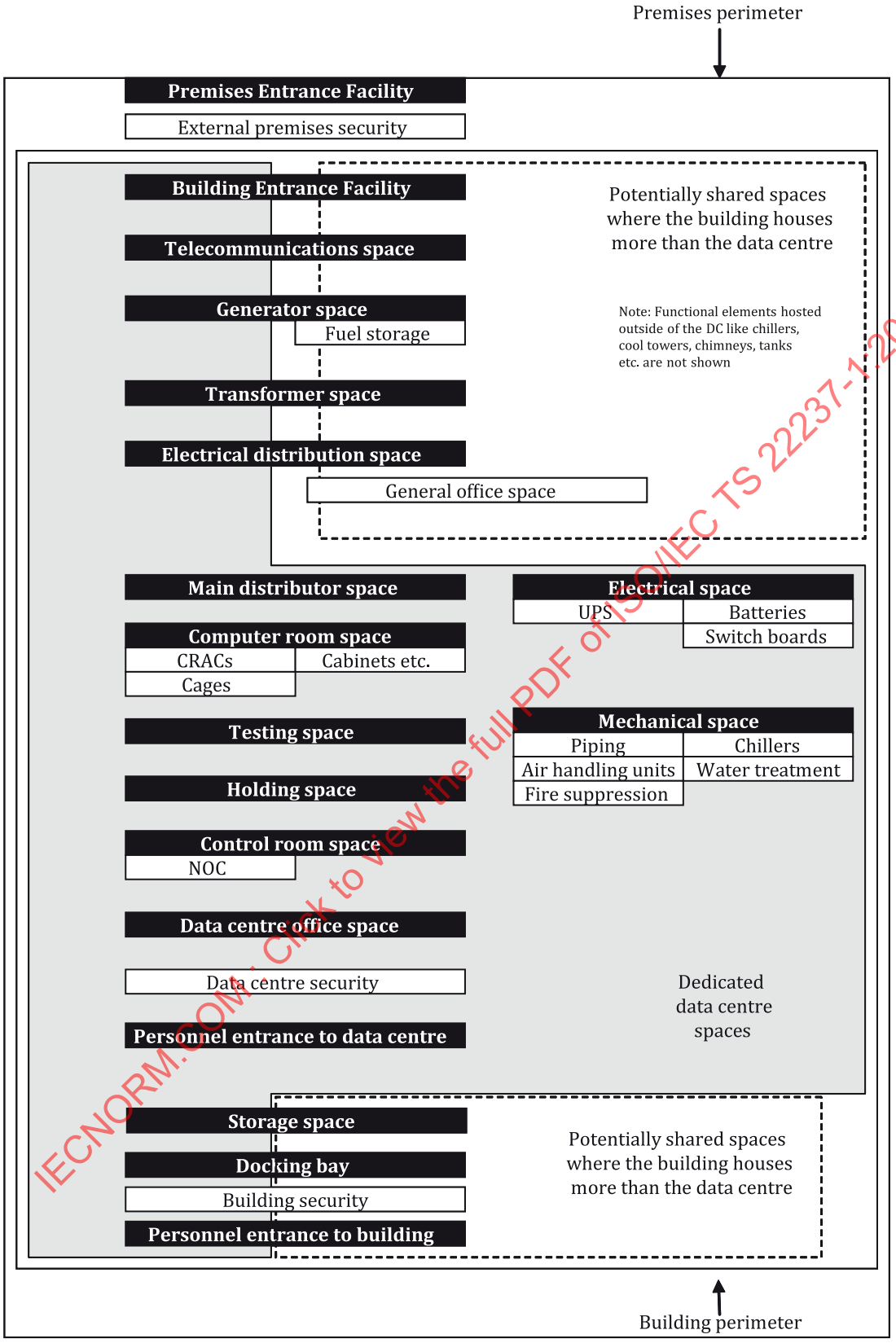

Figure 3 — Typical schematic diagram of premises containing a data centre

Within the area of the building designated as a data centre, the need for, and contents of, the spaces depends upon the purpose of the data centre, its anticipated power consumption and the need for environmental control.

The need for segregation of spaces depends on safety considerations, requirements for security and upon the need for environmental control.

As examples, a small enterprise data centre may comprise a single room having the function of a computer room space and an electrical space without physical segregation whereas a large data centre may require one or more segregated spaces of each type identified in Figure 3.

7 Classification system for data centres

7.1 General

For the purposes of the ISO/IEC TS 22237 series, data centres are classified with respect to:

a) Availability Classes (see 7.2);

b) Protection Classes (see 7.3);

c) Energy efficient enablement levels (see 7.4).

Combinations of the three classifications are used to determine the relevant requirements and recommendations for the following facilities and infrastructures according to the risk analysis in Clause 5:

1) building construction (see ISO/IEC TS 22237-2);

2) power distribution (see ISO/IEC TS 22237-3);

3) environmental control (see ISO/IEC TS 22237-4);

4) telecommunications cabling infrastructure (see ISO/IEC TS 22237-5);

5) security systems (see ISO/IEC TS 22237-6).

7.2 Availability

The required availability of the facilities and infrastructures that support the functionality of the data centre is of the utmost significance. The data centre owner/user shall determine the desired availability of the overall set of facilities and infrastructures using business risk analysis and downtime cost analysis (Clause 5). It is recognised that availability requirements may vary with time of day, week or month.

Different qualitative Availability Classes for the overall set of data centre facilities and infrastructures are defined as shown in Table 1. The availability of the entire data centre depends on the Availability Classes of its individual infrastructures such as power sourcing and distribution, environmental control and security. The requirements for a specific facility or infrastructure of a given Availability Class are specified in ISO/IEC TS 22237-3, ISO/IEC TS 22237-4 and ISO/IEC TS 22237-6, respectively.

In order for the set of facilities and infrastructures of data centre to be considered to be of a given Availability Class, the design of each individual facility and infrastructure listed in Table 1 shall meet or exceed that Availability Class.

NOTE Where the design of the environmental control facility and infrastructure is of Enhanced Class 4 as described in ISO/IEC TS 22237-4, the set of facilities and infrastructures of data centre may be considered to be of Enhanced Class 4 provided that all other facilities and infrastructures of Table 1 are of Class 4.

The provision of higher Availability Classes generally requires greater investment, for example in design, construction, components, systems and human resources. For example, greater investment in components can result in greater Mean Time between Failures (MTBF) or Reduced Mean Time to Recovery (MTTR). MTBF of a particular infrastructure provides information in relation the event

probability as discussed in 5.3. MTTR of a particular infrastructure provides an indication of the event impact as discussed in 5.3.

Table 1 — Availability Classes and example implementations

	Availability Class 1	Availability Class 2	Availability Class 3	Availability Class 4
Availability of overall set of facilities and infrastructures	Low	Medium	High	Very high
Example for power distribution (see ISO/IEC TS 22237-3)	Single-path (no redundancy of components)	Single-path (resilience provided by redundancy of components)	Multi-path (resilience provided by redundancy of systems)	Multi-path (fault tolerant even during maintenance)
Example for environ-mental control (see ISO/IEC TS 22237-4)	No specific requirements	Single-path (no redundancy of components)	Single-path (resilience provided by redundancy of components)	Multi-path (resilience provided by redundancy of systems), allows maintenance during operation
Example for telecommunications cabling (see ISO/IEC TS 22237-5	Single-path using direct connections	Single-path using fixed infrastructure	Multi-path using fixed infrastructure	Multi-path using fixed infrastructure with diverse pathways

NOTE 1 Requirements and recommendations for data centre construction that provide the desired Protection Classes to ensure availability of the facilities and infrastructures are addressed in ISO/IEC TS 22237-2.

NOTE 2 Enhanced Class 4 providing a multi-path solution (fault tolerant even during maintenance) is specified in ISO/IEC TS 22237-4.

NOTE 3 Requirements and recommendations for physical security of data centre spaces to ensure availability of the facilities and infrastructures are addressed in ISO/IEC TS 22237-6.

If possible, the determination of the availability for sub-systems and components should include possible future expansions in the data centre for resilience purposes.

Additional attention shall be given to the physical security of the facilities and infrastructures outlined in 7.3, describing other important factors for the overall availability of the entire data centre.

In addition to the design and installation of more sophisticated technical solutions, the implementation of higher Availability Classes implies the application of effective organisational structures to manage the operation of those technical solutions including, but not limited to:

a) the availability of trained service personnel;

b) storage of spare parts;

c) the establishment of maintenance contracts;

d) rapid access to precise instructions defining the actions and communications required in case of a system failure.

Annex A provides an overview of the design requirements to achieve a certain Availability Class.

7.3 Physical security

7.3.1 General

The physical security provided for the facilities and infrastructures of a data centre has an influence on both the probability and impact of risk events (see 5.3) since the objective of physical security is to protect against:

a) unauthorised access (see 7.3.2);

b) internal environmental events (see 7.3.3);

c) external environmental events (see 7.3.3).

7.3.2 Protection against unauthorised access

The areas of the data centre and its surroundings shall be defined in terms of Classes of protection against unauthorised access as shown in Table 2. Depending on the protection aim definition the data centre owner/user shall select the appropriate Protection Class.

Table 2 — Protection Classes

Type of protection	Protection Class 1	Protection Class 2	Protection Class 3	Protection Class 4
Protection against unauthorised access	Public or semi-public area	Area that is accessible to all authorised personnel (employees and visitors)	Area restricted to specified employees and visitors (other personnel with access to Protection Class 2 have to be accompanied by personnel authorised to access Protection Class 3 areas)	Area restricted to specified employees who have an identified need to have access (other personnel with access to Class 2 or Class 3 areas have to be accompanied by personnel authorised to access Class 4 areas)

Within the data centre, the access restrictions are dependent on the purpose of the data centre (e.g. enterprise vs. co-location). The design criteria are based upon an analysis of needs defining appropriate requirements and recommendations.

ISO/IEC TS 22237-2 specifies the requirements of and provides recommendations for the location and construction of data centres in support of the desired Protection Class zoning.

ISO/IEC TS 22237-3 specifies the requirements of and provides recommendations for power distribution systems in support of the desired Protection Class.

ISO/IEC TS 22237-4 specifies the requirements of and provides recommendations for environmental control systems in support of the desired Protection Class.

ISO/IEC TS 22237-6 specifies the requirements of and provides recommendations for security and protection systems in support of the desired Protection Class.

7.3.3 Protection against environmental events

The areas of the data centre and its surroundings shall be defined in terms of Classes of Protection against environmental events as shown in Table 3. Depending on the protection aim definition the data centre owner/user shall select the appropriate Protection Class for each type of protection shown in Table 3.

Table 3 — Protection against environmental events

Type of protection	Protection Class 1	Protection Class 2	Protection Class 3	Protection Class 4
Protection against internal fire	No special protection applied	The area requires to be protected against fire by a detection and suppression system, which maintains the function of that area during a fire in that area or one in a Class 1 area.	The area requires to be protected against fire by a detection and suppression system, which maintains the function of that area during a fire in that area or one in a Class 1 or Class 2 area.	The area requires to be protected against fire by a detection and suppression system, which enables critical data centre function to be secured during a fire in that area or one elsewhere in the data centre.
Protection against other internal events	No special protection applied	Mitigation applied	Mitigation applied	Mitigation applied
Protection against external environmental events	No special protection applied	Mitigation applied	Mitigation applied	Mitigation applied

Protection against internal and external environmental events includes all measures required to ensure the desired Availability Class for the facilities and infrastructures of the data centre including building construction, protection systems and organisational measures.

Internal environmental events include overheating, fire, electrostatic discharge, water etc. impacting the function of the data centre infrastructures.

External environmental events include fire, flood, earthquake, explosion and other forms of natural disaster (lightning and other electromagnetic effects).

Under optimal conditions, the risks posed by external environmental events are mitigated by the selection of the data centre location (see ISO/IEC TS 22237-2). However, in most situations alternative design solutions have to be applied to the data centre facilities and infrastructures to provide them with an acceptable degree of security against such events.

ISO/IEC TS 22237-2 specifies the requirements of and provides recommendations for the location and construction of data centres in support of the desired Protection Class against environmental events.

ISO/IEC TS 22237-3 specifies the requirements of and provides recommendations for power distribution systems in support of the desired Protection Class against environmental events.

ISO/IEC TS 22237-4 specifies the requirements of and provides recommendations for environmental control systems in support of the desired Protection Class against environmental events.

ISO/IEC TS 22237-6 specifies the requirements of and provides recommendations for security and protection systems in support of the desired Protection Class.

7.4 Energy efficiency enablement

7.4.1 General

The ability to measure the energy consumption and to allow calculation and reporting of energy efficiency of the various facilities and infrastructures supporting the operation of a data centre is critical to the achievement of any energy efficiency objectives.

Three levels of granularity are defined:

a) Level 1: a measurement regime providing simple global information for the data centre as a whole;

b) Level 2: a measurement regime provides detailed information for specific facilities and infrastructures within the data centre;

c) Level 3: a measurement regime provides granular data for elements within the spaces of the data centre.

Moving from one complexity level to a higher level requires an increased level of measurement/monitoring infrastructure.

The data centre owner/user shall define the appropriate energy efficiency enablement level prior to the data centre design.

The desired energy efficiency enablement level may be determined by:

1) an operating cost analysis;

2) external regulatory or legislative requirements;

3) user defined rules.

7.4.2 Power distribution system

ISO/IEC TS 22237-3 describes the elements of the power distribution systems for data centres and defines the requirements and recommendations for the measurement/monitoring infrastructures of the power distribution systems in support of the desired complexity level.

7.4.3 Environmental monitoring and control

ISO/IEC TS 22237-4 describes the elements of the environmental control systems for data centres and defines the requirements and recommendations for the measurement/monitoring infrastructures of the environmental control systems in support of the desired complexity level.

Annex A
(informative)

General design principles

A.1 Design process

A.1.1 Introduction

Effective data centre design requires the splitting of the project into phases. Each phase has its own input and output. All these phases follow a sequential timeline, resulting in the final project plan, leading to the issuing of a contract for the installation of the data centre enabling the operational phase to commence. Phases can be executed several times if required to achieve the agreed or defined objectives. Figure A.1 lists all phases in their sequential order including phase descriptions and responsibilities.

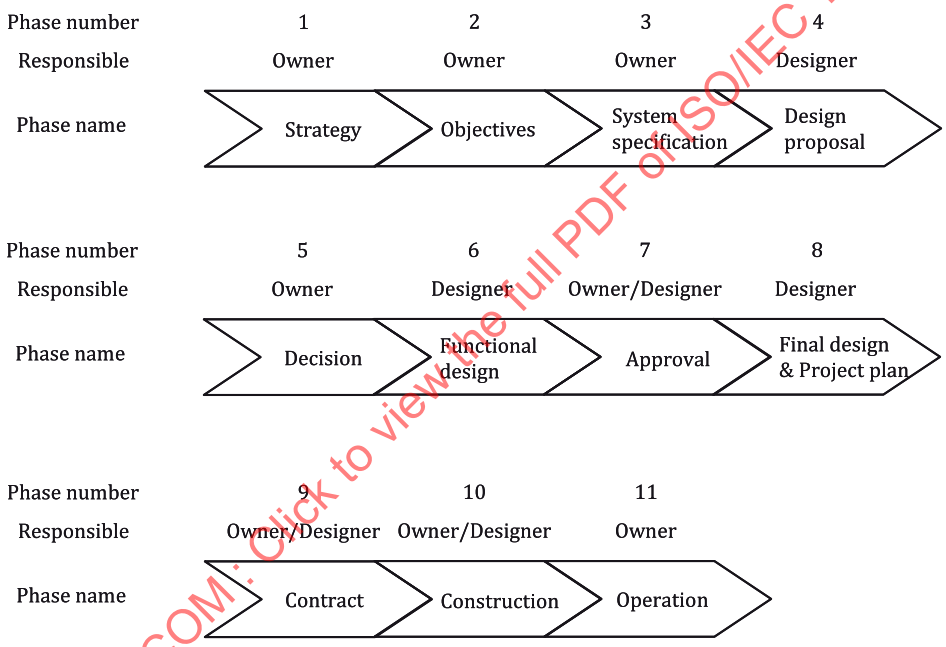

Figure A.1 — Design phases

A.1.2 Phase 1 — Strategy

This phase is for information collection in order to define the project objectives. The following information is required:

a) business continuity strategy;

b) IT strategy;

c) corporate data centre strategy;

d) general customer requirements/expectations;

e) analysis of current load/demand/costs;

f) expected infrastructure technology roadmap;