INTERNATIONAL STANDARD

ISO/IEC 22237-1

First edition
2021-10

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 22237-1:2021(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).

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) or the IEC list of patent declarations received (see patents.iec.ch).

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 & Data Centres*.

This first edition cancels and replaces the first edition (ISO/IEC TS 22237-1:2018), which has been technically revised.

The main changes are as follows:

— reference to Key Performance Indicators of ISO/IEC 30134 series has been included;

— Clause 7 (Availability) has been revised;

— the design processes (Clause 8) and design principles (Clause 9) have been moved from an annex to the main body of the document;

— the existing Annex A has been removed;

— new Annexes A and B have been added.

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 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 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.

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

— ISO/IEC 22237-1 (this document), *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 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*;

— 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 22237 series is shown in Figure 1.

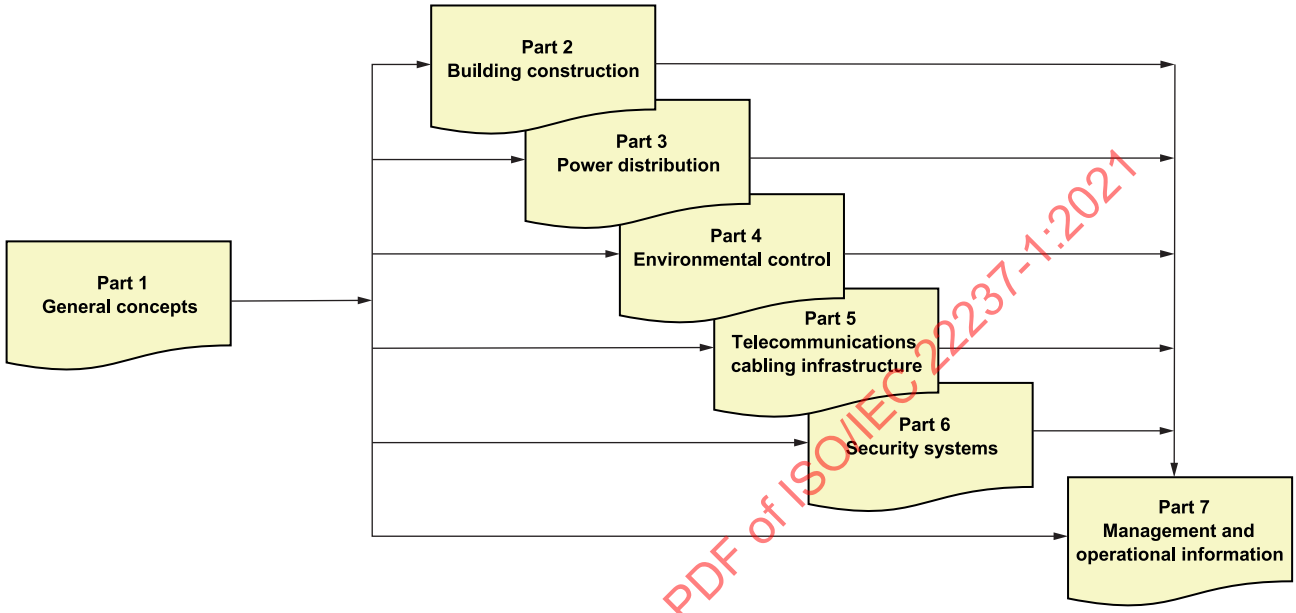


Figure 1 — Schematic relationship between the ISO/IEC 22237 series of documents

This document, ISO/IEC 22237-1, 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 22237-6 specify requirements and recommendations for particular facilities and infrastructures to support the relevant classification for "availability", "physical security" and "energy efficiency enablement" selected from ISO/IEC 22237-1 (this document).

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

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

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 1: General concepts

1 Scope

This document:

a) describes the general principles for data centres upon which the requirements of the ISO/IEC 22237 series are based;

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

f) provides a reference to the operation and management of data centres.

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

1) the selection of information technology and network telecommunications equipment, software and associated configuration issues are outside the scope of this International Standard;

2) quantitative analysis of overall service availability resulting from multi-site data centres;

3) safety and electromagnetic compatibility (EMC) requirements (covered by other standards and regulations. However, information given in this document can 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 22237-6, *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 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 http://www.electropedia.org/

3.1.1
availability
ability to be in a state to perform as required

[SOURCE: IEC 60050-192:2015, 192-01-23, modified — Note 1 to entry and Note 2 to entry deleted.]

3.1.2
building entrance facility
facility (3.1.16) that provides all necessary services, and which complies with all relevant regulations for the entry of specific *infrastructures* (3.1.21) or services into a building

3.1.3
building security
facilities (3.1.16) and *systems* (3.1.30) necessary to provide the required levels of security at the entrance to and within the building containing the *data centre* (3.1.8)

3.1.4
co-hosting data centre
data centre (3.1.8) 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* (3.1.21) of the building are provided as a service by the data centre operator.

3.1.5
co-location data centre
data centre (3.1.8) in which multiple customers locate their own network(s), servers and storage equipment

Note 1 to entry: The support *infrastructure* (3.1.21) of the building (such as power distribution and environmental control) is provided as a service by the data centre operator.

3.1.6
computer room space
area within the *data centre* (3.1.8) that accommodates the data processing, data storage and *telecommunication equipment* (3.1.33) that provides the primary function of the data centre

3.1.7
control room space
area within the *data centre* (3.1.8) used to control the operation of the data centre and to act as a central point for all control and monitoring functions

3.1.8
data centre
a structure, or group of structures, dedicated to the centralized accommodation, interconnection and operation of information technology and network *telecommunications* (3.1.31) equipment providing data storage, processing and transport services together with all the *facilities* (3.1.16) and *infrastructures* (3.1.21) for power distribution and environmental control together with the necessary levels of resilience and security required to provide the desired service *availability* (3.1.1)

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]

3.1.9
data centre security
necessary *facilities* (3.1.16) and *systems* (3.1.30) that provide the required levels of security at the entrance to and within the *data centre* (3.1.8)

3.1.10
demarcation point
point where the operational control or ownership changes

3.1.11
electrical distribution space
area used for housing facilities to distribute electrical power between the *transformer space* (3.1.36) and *electrical spaces* (3.1.12) within the *data centre* (3.1.8) or elsewhere within the premises or individual buildings within the premises

3.1.12
electrical space
area within the *data centre* (3.1.8) used for housing *facilities* (3.1.16) to deliver and control electrical power to the data centre spaces (including switchboards, batteries, *uninterruptible power systems* (3.1.37) (UPS), etc.)

3.1.13
enterprise data centre
data centre (3.1.8) that is operated by an enterprise which has the sole purpose of the delivery and management of services to its employees and customers

3.1.14
external premises security
facilities (3.1.16) and *systems* (3.1.30) that provide the required levels of security for the area between the building and the boundary of the premises

3.1.15
energy efficiency enablement
ability to measure the energy consumption and to allow calculation and reporting of energy efficiency of the various *facilities* (3.1.16) and *infrastructures* (3.1.21)

3.1.16
facility
spaces and pathways that accommodate a specific *infrastructure* (3.1.21)

3.1.17
functional capability
ability of the *data centre* (3.1.8) (or *system* (3.1.30) or sub-system) to deliver its intended function

3.1.18
functional element
source of supply, device or path

3.1.19
generator space
area used for housing the installation of electrical power supply generation equipment together with control *systems* (3.1.30), storage of associated fuels or energy conversion equipment

3.1.20
holding space
area within the *data centre* (3.1.8) 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* (3.1.30) providing *functional capability* (3.1.17) of the *data centre* (3.1.8)

Note 1 to entry: Examples are power distribution, environmental control and *physical security* (3.1.25).

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, 3.1.11, modified — removed "as specified in ISO/IEC 11801-1".]

3.1.23
mechanical space
area that is used for housing mechanical equipment and *infrastructure* (3.1.21) that provides environmental control for the *data centre* (3.1.8) spaces (including chillers and water treatment, air handling and fire suppression *systems* [3.1.30])

3.1.24
network operator data centre
data centre (3.1.8) that has the primary purpose of the delivery and management of broadband services to the operator's customers

3.1.25
physical security
measures (combining physical and technological controls), procedures and responsibilities to maintain the desired level of *availability* (3.1.1) for the *facilities* (3.1.16) and *infrastructures* (3.1.21) of the *data centres* (3.1.8) in relation to access control and environmental events

3.1.26
planned downtime
period of time during which a *system* (3.1.30) or sub-system does not provide *functional capability* (3.1.17) 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
facility (3.1.16) that provides all necessary services, and which complies with all relevant regulations, for the entry of specific *infrastructures* (3.1.21) or services into premises

3.1.28
reliability
ability to perform as required, without failure, for a given time interval, under given conditions

[SOURCE: IEC 60050-192:2015, 192-01-24, modified — Note 1 to entry to Note 3 to entry deleted.]

3.1.29
storage space
secured area where general goods and/or *data centre* (3.1.8) goods to be used in the premises and data centre are stored

3.1.30
system
set of interrelated *functional elements* (3.1.18) considered in a defined context as a whole and separated from their environment

3.1.31
telecommunications
branch of technology concerned with the transmission, emission, and reception of signs, signals, writing, images, and sounds, that is, information of any nature by cable, radio, optical, or other electromagnetic *systems* (3.1.30)

[SOURCE: ISO/IEC 11801-1:2017, 3.1.51, modified.]

3.1.32
telecommunications cabling
infrastructure (3.1.21) from the *telecommunications space(s)* (3.1.34) to the *premises entrance facility* (3.1.27)

3.1.33
telecommunication equipment
equipment within the *data centre* (3.1.8) that provides telecommunication services within the data centre

3.1.34
telecommunications space
area which may house *demarcation points* (3.1.10) and *telecommunication equipment* (3.1.33) associated with the *building entrance facility* (3.1.2) and which may allow service providers restricted access to the *data centre* (3.1.8)

3.1.35
testing space
area within the *data centre* (3.1.8) used for the testing and configuring of equipment prior to being brought into service

Note 1 to entry: Testing space is sometimes called staging area.

3.1.36
transformer space
area used for housing equipment necessary to convert voltage levels and/or provide necessary isolation for the connection to the equipment within the premises or individual buildings within the premises

3.1.37
uninterruptible power system
combination of convertors, switches and energy storage devices (such as batteries), constituting a power *system* (3.1.30) 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 output port. 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 62040-1:2017, 3.101]

3.1.38
unplanned downtime
unexpected time taken, following a failure of *functional capability* (3.1.17), to repair the relevant *infrastructure* (3.1.21) 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

CRAH	computer room air handling unit
MDT	mean downtime
MTBF	mean time between failures
MTTR	mean time to repair
NOC	network operating centre
UPS	uninterruptible power system

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 accordance with Clause 5;

c) appropriate Protection Classes for the data centre spaces and pathways shall be in accordance with 7.3.1;

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

e) the design process of Clause 8 (or equivalent) shall be applied;

f) the design principles of Clause 9 shall be applied.

NOTE The application of the design process in Clause 8 is not mandatory for an assessment of existing data centres.

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 business impact 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).

There is a link between the availability of the infrastructures specified in the ISO/IEC 22237 series and the overall availability, but it should be recognized that the recovery of intended data processing, storage, and transport functionality following the repair of an infrastructure failure depends on many factors related to the configuration of the hardware and software providing that functionality.

As a result, the role of the infrastructure is to support overall availability objectives but this is not the sole factor in their attainment.

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 downtime for maintenance.

The design and physical security of the facilities and infrastructures of the data centre shall be subjected to a risk analysis (see 5.3) which maps identified risk events against the requirements of the availability classification (see 7.2). The availability classification for each infrastructure is described as providing low, medium, high and very high availability. Clause 7 further describes the situations (risk events) for which each infrastructure is protected against failure. Other approaches are to apply "% availability" to infrastructures but this is not supported by the ISO/IEC 22237 series for reasons explained in Annex A.

A business risk 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 Business impact analysis

This document does not define methods of analysis for the cost of downtime. Standards such as IEC 31010, ISO/TS 22317 or ISO 22301 provide useful guidance.

The parameters to be considered within such an analysis will depend upon the purpose of the data centre. Some organizations can 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 can have individually recognized consequences from unplanned downtime.

5.3 Risk analysis

This document does not define methods of risk analysis. Standards such as ISO 31000 and IEC 31010 provide useful guidance on this topic.

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 document, 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 business impact analysis (see 5.2) the financial value of the total risk can be estimated.

The risks considered should include external threats which can 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 internal and external attacks by the staff or others should be part of the overall risk evaluation.

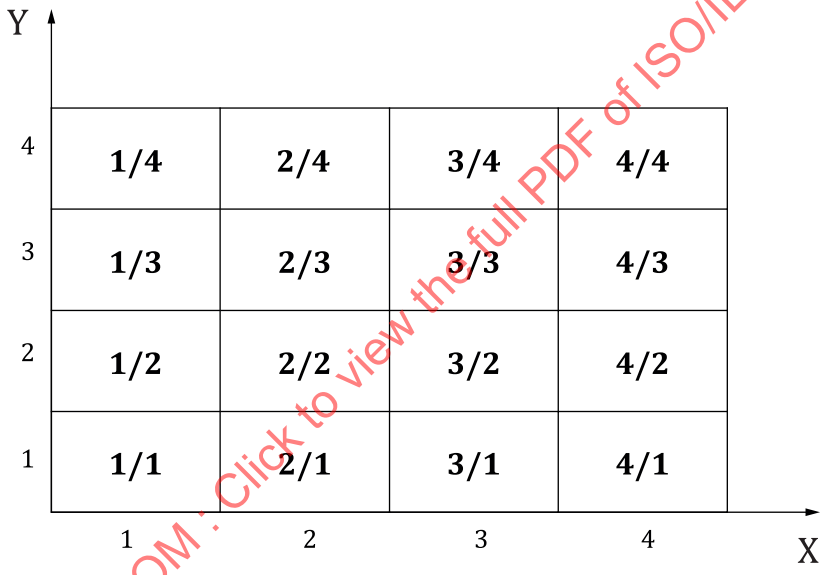
Impact can be categorized as:

1) low: Loss of non-critical services;
2) medium: Failure of critical system functional elements but no loss of redundancy;
3) high: Loss of critical system redundancy but no loss of service;
4) critical: Loss of critical service 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:

1) very low;
2) low;
3) medium;
4) 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.



Key

X probability of an event
Y impact

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

Data centres differ in terms of their purpose e.g. co-hosting data centre, co-location data centre, enterprise data centre, network operator data centre. Data centres can also differ significantly with respect to their physical size, ranging from:

a) a data centre in a building housing a small quantity of storage and server equipment to provide information technology services to the occupants of that building; to

b) a data centre housing a large quantity of such equipment providing information technology services via diverse internal and external telecommunications networks and 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 purpose and their size.

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 buildings.

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 not only 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 can 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 can 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) (which accommodate(s) e.g. CRAC and CRAH);

6) control room space(s) (which accommodate(s) the NOC);

7) office space(s);

8) storage space(s) and holding space(s).

The spaces and facilities also address building security, data centre security and external premises security.

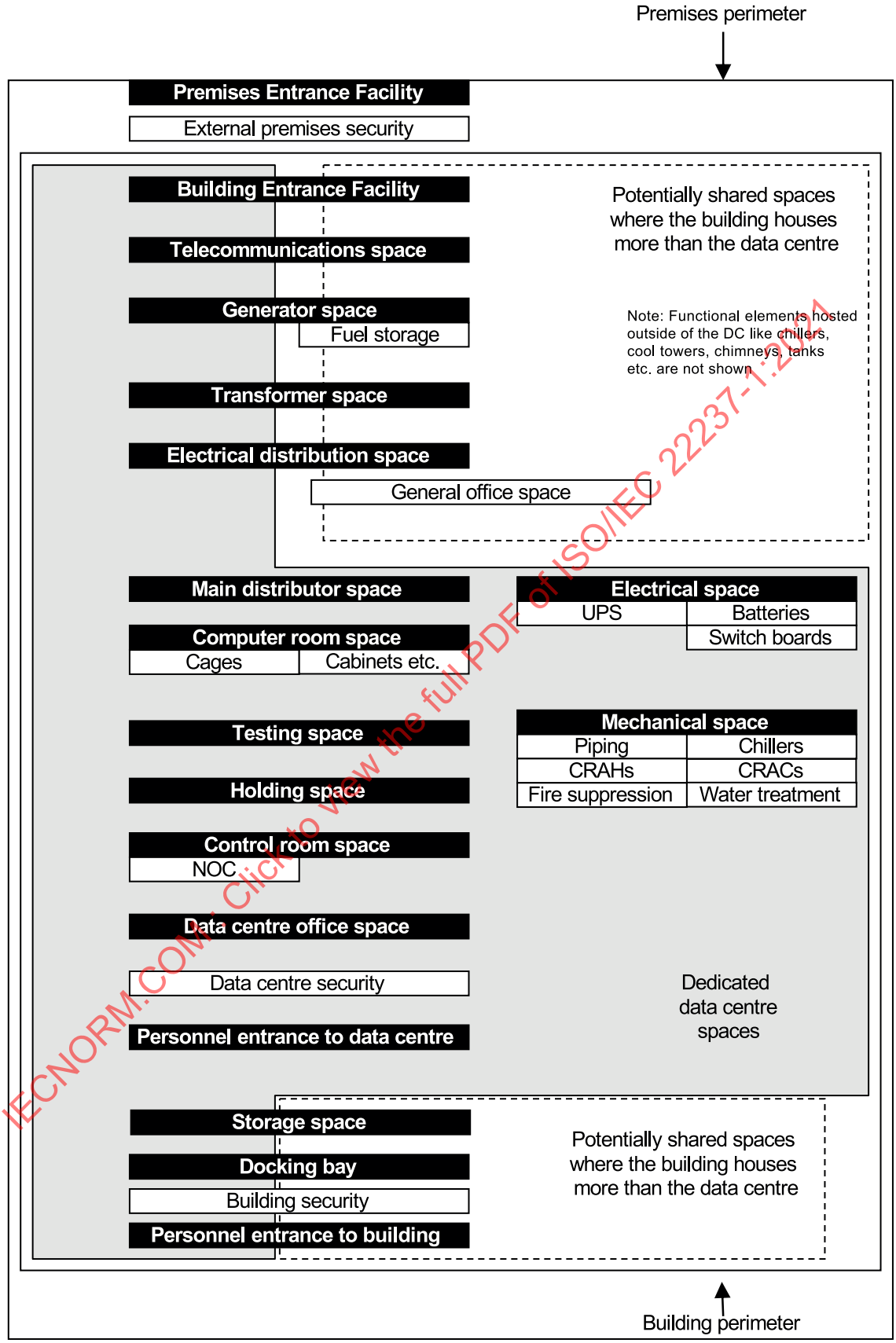


Figure 3 — Typical schematic diagram of premises containing a data centre

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 availability and fire protection considerations, requirements for security and upon the need for environmental control.

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

Functional spaces can be accommodated in one or more physical spaces and in one or more buildings and premises and subject to multiple ownership.

7 Classification system for the design of data centre facilities and infrastructures

7.1 General

For the purposes of the ISO/IEC 22237 series, data centres facilities and infrastructures are designated with respect to:

a) Availability Classes (see 7.2);

b) Protection Classes (see 7.3);

c) Energy efficiency enablement levels (see 7.4).

These designations are used in combination to determine the relevant requirements and recommendations for the following facilities and infrastructures:

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

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

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

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

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

7.2 Availability

7.2.1 General

Data centres can be single-site or configured to operate across multiple sites.

7.2.2 describes the availability concepts and requirements for a single-site data centre.

7.2.3 describes the use of a multi-site data centre to improve the overall service availability.

Annex B summarizes the availability classification specified in this document.

7.2.2 Single-site data centres

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 business impact analysis (Clause 5). It is recognized that availability requirements can vary with time of day, week or month.

The ISO/IEC 22237 series defines four Classes of availability. Based on the outcome of the business risk analysis in Clause 5 an Availability Class shall be selected for the following infrastructures:

— power supply and distribution;

— environmental control;

— telecommunications cabling.

The availability of the entire data centre depends on the Availability Classes of its infrastructures.

The selection of the Availability Class shall be made based on the following design objectives (for requirements and recommendations specific to each infrastructure see the appropriate part of the ISO/IEC 22237 series).

For the set of facilities and infrastructures of a data centre to be considered to be of a given Availability Class, the design of each facility and infrastructure shall meet or exceed the design objectives of that Availability Class defined below.

A Class 1 solution (single path) is appropriate where the outcome of the risk assessment deems it acceptable that:

— a single fault in a functional element can result in loss of functional capability;

— planned maintenance can require the load to be shut-down.

A Class 2 solution (single path with redundancy) is appropriate where the outcome of the risk assessment deems it necessary that:

— a single fault in a device shall not result in loss of functional capability of that path (via redundant devices);

— routine planned maintenance of a redundant device shall not require the load to be shut down.

NOTE Failure of the path can result in unplanned load shutdown and routine maintenance of non-redundant devices can require planned load shutdown.

A Class 3 solution (multiple paths providing a concurrent/repair operate solution) is appropriate where the outcome of the risk assessment deems it necessary that:

— a fault of a functional element shall not result in loss of functional capability;

— for environmental control: although a failure of a path can result in unplanned load shutdown, maintenance routines shall not require planned load shutdown as the passive path serves to act as the concurrent maintenance enabler as well as reducing the recovery of service time (minimizing the mean downtime) after the failure of a path;

— planned maintenance shall not require the load to be shut-down.

All paths shall be designed to sustain the maximum load.

A Class 4 solution (fault-tolerant solution except during maintenance) is appropriate where the outcome of the risk assessment deems it necessary that:

— a fault of a functional element shall not result in loss of functional capability;

— for power supply and distribution: any single event impacting a functional element shall not result in load shut-down;

— for environmental control: a failure of one path shall not result in unplanned load shutdown;

— planned maintenance shall not require the load to be shut-down.

All paths shall be designed to sustain the maximum load.

Technical solutions supporting different qualitative Availability Classes for the overall set of data centre facilities and infrastructures are shown in Table 1.

Table 1 — Availability Classes and technical solutions

Infrastructure of the ISO/IEC 22237 series	Availability Class 1	Availability Class 2	Availability Class 3	Availability Class 4
Power supply (see ISO/IEC 22237-3)	Single path to primary distribution equipment — Single source	Single path to primary distribution equipment — Redundant sources	Multiple paths to primary distribution equipment — Redundant sources	Multiple paths to primary distribution equipment — Multiple sources
Power distribution (see ISO/IEC 22237-3)	Single path	Single path with redundancy	Multiple paths — Concurrent repair/operate solution	Multiple paths — Fault tolerant except during maintenance
Environmental control (see ISO/IEC 22237-4)	Single path	Single path with redundancy	Multiple paths — Concurrent repair/operate solution	Multiple paths — Fault tolerant except during maintenance
Telecommunications cabling (see ISO/IEC TS 22237-5)	Single path — direct connections or fixed infrastructure with single access network connection	Single path — fixed infrastructure with multiple access network connections	Multiple paths — fixed infrastructure with diverse pathways with multiple access network connections	Multiple paths — fixed infrastructure with diverse pathways and redundant distribution zones and multiple access network connections
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 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.				

The provision of higher Availability Classes generally requires greater investment. More information about availability can be found in Annex A.

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 organizational structures to manage the operation of those technical solutions including, but not limited to:

1) the availability of trained service personnel;

2) storage of spare parts;

3) the establishment of maintenance contracts and service level agreements;

4) rapid access to precise instructions defining the actions and communications required in any case of failure.

7.2.3 Multi-site data centres

In some cases, data centres configured across multiple sites can feature individual sites of low availability class infrastructures while maintaining the overall service availability objectives provided by the group of data centre sites. This document does not provide a mapping between the overall service availability of the multi-site data centre and that of the availability class of the infrastructures

in any individual site. This concept requires additional capabilities of the IT services which are out of the scope of this document.

7.3 Physical security

7.3.1 General

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 physical security provided for the data centre influences both the probability and impact of risk events (see 5.3) since the objective of physical security is to protect against:

a) unauthorized access (see 7.3.2);

b) intrusion (see 7.3.3);

c) internal environmental events (see 7.3.4);

d) external environmental events (see 7.3.4).

The required Protection Classes for the data centre spaces shall be selected according to ISO/IEC TS 22237-6 for each of these objectives.

7.3.2 Protection against unauthorized access

The areas of the data centre and its surroundings shall be protected against unauthorized access.

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

ISO/IEC TS 22237-6 specifies the requirements of and provides recommendations for active and passive measures in support of the Protection Classes for unauthorized access.

ISO/IEC TS 22237-2 specifies requirements and recommendation for the construction of boundaries between spaces of a given Protection Class.

7.3.3 Protection against intrusion

The areas of the data centre and its surroundings shall be protected against intrusion.

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

For a particular Protection Class the intrusion delay time provided by an intrusion barrier should be longer than the time it takes to stop the intruder. If the intrusion delay is created by multiple barriers, the summation of the individual delay times results in the total intrusion delay time.

All intrusion related requirements and recommendations for the construction of data centres are for further study and are the subject of the revision of ISO/IEC TS 22237-2.

All intrusion related requirements and recommendations for active and passive measures in support of the Protection Classes are for further study and are the subject of the revision of ISO/IEC TS 22237-6.

7.3.4 Protection against environmental events

The areas of the data centre and its surroundings shall be protected against environmental events.

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 22237-3 specifies the Protection Classes applicable to spaces accommodating power supply and distribution systems.

ISO/IEC 22237-4 specifies the Protection Classes applicable to spaces accommodating environmental control systems.

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

ISO/IEC TS 22237-2 specifies requirements and recommendations for the:

a) construction of boundaries between spaces of a given Protection Class to minimize the impact of internal environmental events;

b) location and construction of data centres to mitigate external environmental events.

7.4 Energy efficiency enablement

7.4.1 General

The ability to measure the energy consumption and to allow calculation and reporting of resource management (e.g. energy efficiency, source diversity and mix) and of the various facilities and infrastructures supporting the operation of a data centre is critical to the achievement of any related objectives.

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 can be determined by:

1) an operating cost analysis;

2) The application of resource and energy management processes according to ISO/IEC TS 22237-7;

3) the selection and application of one or more appropriate KPIs for resource management according to the ISO/IEC 30134 series;

4) external regulatory or legislative requirements;

5) user-defined rules.

Three levels of granularity for the measurement 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 providing detailed information for specific facilities and infrastructures within the data centre;

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

NOTE These three granularity levels are not related to any classes of a given KPI.

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

7.4.2 Power distribution system

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

7.4.3 Environmental monitoring and control

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

7.4.4 Operational processes and KPIs

ISO/IEC TS 22237-7 describes processes and Key Performance Indicators (KPIs) for resource and energy management which analyse data provided by monitoring of power distribution and environmental control infrastructures. Standards in the ISO/IEC 30134 series specify the detailed requirements for this type of KPI.

8 Design and implementation process

8.1 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 4 lists all phases in their sequential order including phase descriptions and responsibilities.

Data centre owners should be aware of the impact of operational strategy on data centre availability, security concept, data centre management and operation. An operational concept should be discussed and decided upon to ensure that room layouts and security zones and protection class boundaries provide the necessary function to protect the data centre against unauthorized access according to the security concept.

The operational concept should also describe process interfaces between owner, operator, customers and suppliers. Processes, roles and responsibilities shall be defined prior to the beginning of operation. Operational staff shall be instructed on technical infrastructure and trained on operational procedures at latest during acceptance test phase (see ISO/IEC TS 22237-7 for more information about acceptance tests).

At appropriate points before final approval (phase 7), assessment(s) shall verify that the design, the operation and management processes and the KPIs meet the project objectives.

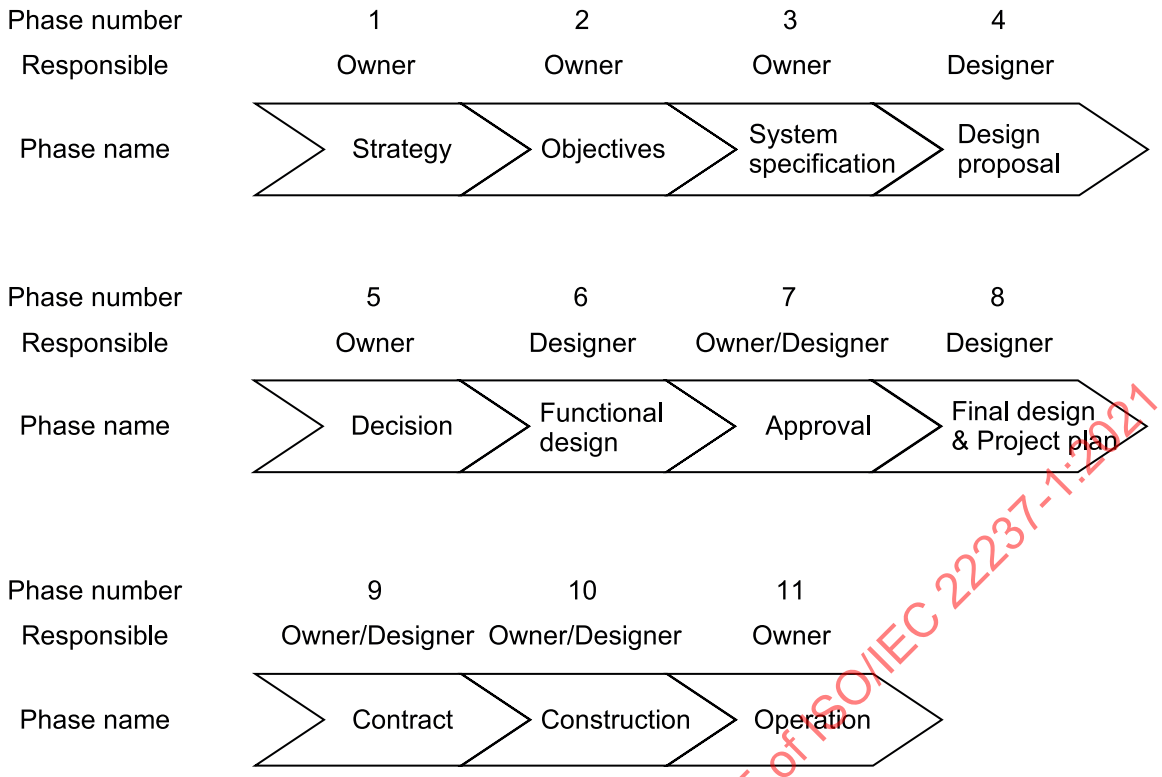


Figure 4 — Design phases

8.2 Design phases

8.2.1 Phase 1 — Strategy

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

a) business risk analysis;

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;

g) "forecast" of future facility and infrastructure demand (space, power and locations);

h) operational strategy.

8.2.2 Phase 2 — Objectives

This phase is used by the owner to convert the strategy into objectives. The results are the following:

a) correlation with corporate data centre strategy;

b) design benchmarks (size/performance levels/budgets);

c) project risk analysis (internal and external);

d) selecting location options;

e) definition of work flow;

f) timelines and impact of delays;

g) selection of location options;

h) general floor plan and materials catalogue.

8.2.3 Phase 3 — System specifications

This phase defines the target specifications for all infrastructures with the following output:

a) target specification for power supply (sources);

b) target specification for power distribution;

c) target specification for environmental control;

d) target specification for physical security;

e) target specification for fire detection and firefighting;

f) target specifications for telecommunications infrastructure;

g) target specification for data centre operation and management;

h) target specification for construction.

8.2.4 Phase 4 — Design proposal

The designer uses the target specifications and objectives to create a design proposal for all infrastructures offering several options to the owner. The design proposal contains:

a) design proposal for power supply (sources);

b) design proposal for power distribution;

c) design proposal for environmental control;

d) design proposal for physical security;

e) design proposal for fire detection and firefighting;

f) design proposal specifications for telecommunications infrastructure;

g) design proposal for data centre operation and management;

h) design proposal for construction;

i) cost models and timelines for proposed options;

j) final location selection.

8.2.5 Phase 5 — Decision

The owner selects the design from the available design options and cost models (supported by the designer).

8.2.6 Phase 6 — Functional design

The designer converts the owner selection into functional design. The functional design contains:

a) functional design for power supply (sources);

b) functional design for power distribution;

c) functional design for environmental control;

d) functional design for physical security;

e) functional design for fire detection and firefighting;

f) functional design for telecommunications infrastructure;

g) functional design for data centre operation and management;

h) functional design for construction;

i) cost model "fine tuning" for selected option.

8.2.7 Phase 7 — Approval

The owner approves the functional design and cost models, taking into account the risks and scheduling constraints of the project.

8.2.8 Phase 8 — Final design and project plan

The designer defines volume and/or pieces for all the infrastructures approved under 8.2.7. Furthermore, the project workflow and all project milestones and timelines are defined and subject to change control, resulting in an overall implementation plan.

8.2.9 Phase 9 — Contract

The owner (with support of the designer/consultant) issues a tender and selects the contractor(s).

8.2.10 Phase 10 — Construction

The owner and/or the designer supervise(s) the construction over the entire construction time. Acceptance verification (testing and commissioning) for all infrastructures and for the entire data centre is executed until the data centre is put into service. Further details on testing and commissioning can be found in ISO/IEC TS 22237-7.

8.2.11 Phase 11 — Operation

Hand over to owner for operation. See ISO/IEC TS 22237-7 for further details.

9 Design principles

9.1 Design reference documentation

The outcome of the steps of Clauses 5 to 7 shall be collected in a design reference document which contains as a minimum:

— the outcome of business impact analysis in accordance with 5.2;

— the outcome of risk analysis in accordance with 5.3;

— the description of a base data centre strategy and the selected Availability Class according to 7.2 selected using a business risk analysis;

— the application of physical security in accordance with 7.3;

— the selection of energy efficiency enablement level in accordance with 7.4;

— the operational concept in accordance with 8.1.

9.2 Design principles to support energy efficiency

The design of data centres shall consider energy efficiency (and wider aspects of resource efficiency) as a principle objective independent of the Availability Class to be applied.

ISO/IEC 30134 provides a series of Key Performance Indicators, some of which can be employed at the design stage to assess the predicted energy efficiency.

Best practices for energy-efficient data centre design and more information about resource and energy efficiency in data centres can be found in the following documents:

a) ISO/IEC TR 30133:—[1)],

b) CLC/TR 50600-99-1,

c) ETSI TS 105 174-2-2.

9.3 Design principles for electromagnetic interference

The design of data centres shall consider EMI as a principle objective. Additional information can be found in:

a) ISO/IEC TS 22237-2;

b) ISO/IEC 22237-3;

c) ISO/IEC TS 22237-5;

d) ISO/IEC TS 22237-6.

9.4 Design principles to support operational excellence

The design of data centres shall consider operational excellence as a principle objective independent of the Availability class to be applied.

The design of data centres should enable the provision of management and operational information required by ISO/IEC TS 22237-7.

9.5 Design principles for availability, reliability and resilience

The data centre industry places an emphasis on the importance of Availability of the IT applications, IT systems supporting the applications, and facility systems supporting the IT systems. In addition to Availability, the data centre industry should also recognize the importance of Reliability and Resilience. Throughout the ISO/IEC 22237 series, the term Availability is used to represent the general ability of an element to perform its intended function. This includes not only the Availability of an element, but also the Reliability of an element and Resilience of the data centre. Also, throughout the ISO/IEC 22237 series, the four Availability Classifications are defined on an abstract level from Availability Class 1 to Availability Class 4 to represent increasing ability of a data centre to function as intended without disruption.

1) Under preparation. Stage at the time of publication: ISO/IEC DTR 30133.3:2021.

Availability is the ability of an element to be in a state to perform its intended function at a specific instant of time. Also, Availability is often used to represent past performance of an element through measurement of the time an element is operating as intended, and measurement of time an element is not operating as intended. Reliability is the ability of an element to be in a state to perform its intended function for a given time interval. Resilience is the ability of a data centre to withstand failure in one or more elements, and the ability for the data centre to meet its specified service level during the failure of one or more elements.

The design and implementation of data centres shall consider Resilience as a principle objective independent of the applied Availability Class. Resilience can be improved by structural optimization, the use of more resilient functional elements, and operational excellence. To determine different aspects of Resilience, dedicated KPIs are required. For the optimization of Resilience, quantitative analyses based on KPIs should be involved in the design and implementation process.

Availability and Reliability are briefly discussed in Annex A. A detailed discussion on Availability, Reliability and Resilience is to be the topic of a future document within the ISO/IEC 22237 series.