International Standard

ISO/IEC 22237-2

First edition
2024-02

Information technology — Data centre facilities and infrastructures —

Part 2: Building construction

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

Partie 2: Construction des bâtiments

Reference number
ISO/IEC 22237-2:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 39, *Sustainability, IT and data centres*.

This first edition cancels and replaces ISO/IEC TS 22237-2:2018, which has been technically revised.

The main changes are as follows:

— the interrelationship between this document and ISO/IEC 22237-6 concerning constructional prerequisites for the implementation of security concepts and desired security systems has been more clearly presented;

— the document has been restructured;

  — Clause 6, “Site configuration”, has been split and relevant subclauses have been moved into a new Clause 7, “Outside spaces”;

  — Clause 7, “Building construction”, has been completely revised to present all requirements and recommendations in a single Clause 8;

  — Clause 8, “Data centre spaces and access routes”, has been revised to focus on the design of data centre spaces (now Clause 9);

  — a new Clause 10, “Construction of data centre spaces”, has been added;

  — the content of Clause 9, “Fire compartments, fire barriers and fire suppression systems”, has been revised (now Clause 11);

  — Annex A on additional requirements and recommendations has been removed;

  — Annex B on physical protection against external hazards has been revised as Annex A “Building materials”;

— a new Annex B summarizing the requirements and recommendations of Clause 5 has 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 house and support the information technology and network telecommunications equipment for data processing, data storage and data transport. They are required both by network operators (delivering those services to customer premises) and by enterprises within those customer premises.

Data centres need to provide modular, scalable and flexible facilities and infrastructures to easily accommodate the rapidly changing requirements of the market. In addition, the 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 and main contractors;

2) consultants, architects, building designers and builders, system/installation designers, auditors, test and commissioning agents;

3) suppliers of equipment; and

4) installers and maintainers.

The inter-relationship of the various documents within the ISO/IEC 22237 series at the time of publication is shown in Figure 1.

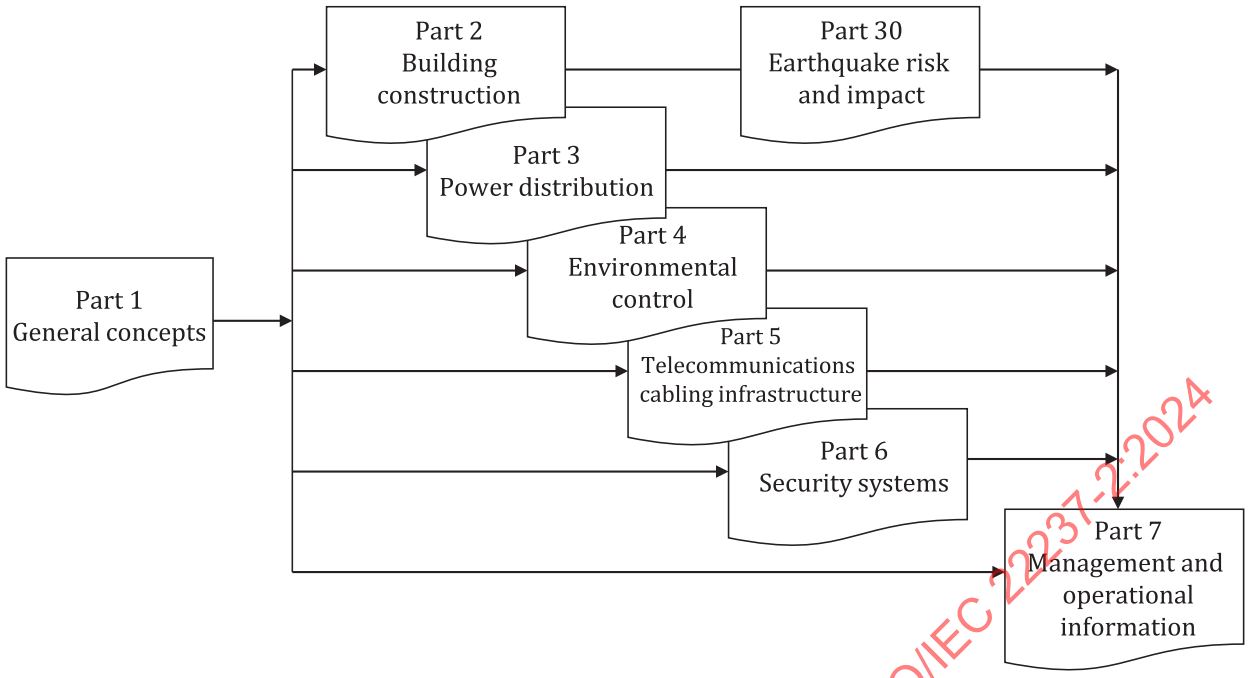


Figure 1 — Schematic relationship between the documents of the ISO/IEC 22237 series

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

This document, ISO/IEC 22237-2, addresses the building design of data centres. It addresses physical security issues from a construction point of view, as opposed to ISO/IEC 22237-6, which specifies the pertinent security system requirements of those facilities and infrastructures (in accordance with the requirements of ISO/IEC 22237-1).

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

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

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 2: Building construction

1 Scope

This document specifies requirements and recommendations for the construction of buildings and other structures which provide accommodation for data centres based on the criteria and classification for "physical security" within ISO/IEC 22237-1 in support of availability.

This document specifies requirements and recommendations for the following:

a) location and site selection (taking in to account natural environment and adjacencies);

b) protection from environmental risks;

c) site configuration;

d) building construction;

e) building configuration;

f) provision of access;

g) physical intrusion protection;

h) physical fire protection;

i) protection against damage from water;

j) quality construction measures.

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

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

2 Normative references

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

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

ISO/IEC 22237-3, *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 22237-6, *Information technology — Data centre facilities and infrastructures — Part 6: Security systems*

ISO/IEC 30129, *Information technology — Telecommunications bonding networks for buildings and other structures*

IEC 62305-3, *Protection against lightning – Part 3: Physical damage to structures and life hazard*

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

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

ISO/IEC TS 22237-30, *Information technology — Data centre facilities and infrastructures — Part 30: Earthquake risk and impact analysis*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

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

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

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

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

3.1.1
effective height of free-standing barrier
h_e
shortest distance between any point on the top of the permanent part of the free-standing barrier (excluding any toppings) and the surface of the supporting ground when measured in the plane of the barrier

3.1.2
free-standing barrier
wall, fence, gate, turnstile or other similar self-supporting barrier, and their associated foundations, designed to prevent entry to a space of a given Protection Class

3.1.3
topping
construction, added to the top of a free-standing barrier, and designed to be an effective intruder-deterrent or for a decorative display of security

3.1.4
pathway
defined route of different media between identified points

Note 1 to entry: Examples of media are bus bars, cables, conduits, ducts, pipes.

3.1.5
raised access floor
system consisting of completely removable and interchangeable floor panels that are supported on an adjustable substructure to allow the area beneath the raised access floor panels to be used by building services

3.2 Abbreviated terms

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

AHU	air handling unit
ffs	for further study
HVAC	heating, ventilation, air conditioning
IT	information technology
M&E	mechanical and electrical
PDU	power distribution unit
RC	resistance class
UPS	uninterruptible power system

4 Conformance

For a data centre to conform to this document:

a) its location shall have been selected following a site assessment as required in Clause 5 (see also Annex B);

b) it shall conform to the site requirements of Clause 6;

c) it shall meet the requirements of Clause 7 where the data centre spaces are outside buildings;

d) it shall meet the building construction requirements of Clause 8 where the data centre spaces are within buildings;

e) it shall meet the building configuration and construction requirements detailed in Clause 9 and Clause 10;

f) it shall meet the requirements of physical fire protection of Clause 11.

5 Location

5.1 Assessment of location

5.1.1 Requirements

The location of a site for a data centre can be assessed either for a “green field” construction of a new data centre or the evaluation of a “brown field” existing site. The location shall be assessed against the following criteria:

a) geographical location (see 5.2);

b) natural environment and adjacencies (see 5.3);

c) utility provision (see 5.4);

d) budgetary factors such as site costs and cost to bring utilities to the site.

5.1.2 Recommendations

Availability of personnel (operational personnel, security personnel) and public transport opportunities should be considered.

5.2 Geographical location

5.2.1 Requirements

The impact of the elevation above sea level, which can have a direct influence on the performance of equipment, shall be considered. If equipment is being installed outside, the impact of ambient temperature and other environmental factors on performance and functionality shall also be considered.

5.2.2 Recommendations

When choosing the location of a new data centre, the following points should be considered:

a) assessment of its impact on the environment;

b) acceptance by the local community;

c) any opportunities to take advantage of renewable sources of energy (e.g. wind, solar, aerothermal, geothermal, hydrothermal and ocean energy, hydropower, biomass, landfill gas, sewage treatment plant gas and biogas);

d) any opportunities to take advantage of the reuse of energy (e.g. thermal) produced by the data centre;

e) any opportunities to take advantage of reclaimed water sources.

5.3 Environmental risk analysis

5.3.1 General

An environmental risk analysis shall be undertaken addressing the natural environment (see 5.3.2) and adjacencies (see 5.3.3).

The results of the environmental risk analysis shall be considered during the design of the data centre. Where the placement of a data centre in a location with negative environmental influences is unavoidable, these influences shall be mitigated by protective constructional, technical, and/or organizational measures.

5.3.2 Natural environment

5.3.2.1 Requirements

An environmental risk analysis shall be conducted which, as a minimum, considers the following natural environment items:

a) flooding, precipitation and surface waters, including the failure of any man-made flood protection systems;

b) seismic activity and earthquakes (requirements and recommendations of ISO/IEC TS 22237-30 shall apply);

c) high wind velocities;

d) lightning;

e) air contamination by natural causes [volcanic activities (e.g. ashes), smoke from wildfires, dust and sand, excessive pollen, etc.];

f) proximity to coast lines;

g) lower than sea level;

h) special purpose flood plains;

i) wildfires;

j) hurricanes, cyclones, typhoons, etc.

5.3.2.2 Recommendations

The environmental risk analysis should take into account the effects of climate change.

5.3.3 Adjacencies (e.g. human-made environment)

5.3.3.1 Requirements

An environmental risk analysis shall be conducted which, as a minimum, considers the following adjacencies items:

a) facilities storing, processing or in other ways dealing with nuclear, radioactive, explosive, flammable or toxic substances or other hazardous materials. The environmental risk analysis shall differentiate between the different types of nuclear plants;

b) air contamination by adjacency to open-air strip mining, agricultural use, construction sites, traffic, etc.;

c) transportation arteries such as waterways, highways, railway tracks;

d) airport landing and take-off approaches (a minimum distance of 1 000 m to runways and aircraft in flight shall be kept);

e) sources of vibration (e.g. hammer mills, railroad tracks);

f) electromagnetic interference (e.g. created by high-voltage lines or transmitter stations);

g) places of public interest, civil unrest, gatherings or political/potential terrorist targets;

h) tall structures (e.g. telecommunication towers and installations that could damage the data centre if they collapse);

i) other not-related or non-essential operations (e.g. uncontrolled operations in multi-tenant premises);

j) criminal or destructive intentions (e.g. intrusion or sabotage) which could require higher resistance classes for walls, doors, windows, etc.

5.3.3.2 Recommendations

Sufficient space should be provided around the area or the building to enable the creation of buffer zones and a secure perimeter.

Data centres should be located in close proximity to potentially advantageous infrastructure or installations including, but not limited to, the following:

a) emergency response services;

b) vendor support and service personnel;

c) monitoring stations of external security providers.

Future development plans and land designation should be checked to avoid future unexpected adjacent hazards.

5.4 Utility provision

5.4.1 Requirements

Consideration shall be given to access to all utility supplies (e.g. electricity, telecommunications infrastructure, water, sewage and gas) that will be required over the intended lifetime of the data centre in terms of:

a) accessibility (existence of utility services);

b) redundancy (services originating from different sources);

c) availability (reliability based on historical trends, if available);

d) capacity (e.g. electricity, water, sewage).

5.4.2 Recommendations

In order to be able to reuse the heat generated by the data centre, consideration should be given to access to district heating networks. Long term availability of water should consider climate trends and impacts on the local communities.

Access to telecommunication infrastructure from specific network service providers as required by the owner should be considered.

6 Site configuration

6.1 General

The typical data centre spaces are described and shown schematically in ISO/IEC 22237-1:2021, Figure 3.

For information on the designation of spaces within the data centre building regarding their Protection Classes, see ISO/IEC 22237-6.

6.2 Site selection

6.2.1 Requirements

The size and shape of a new site shall be suitable for accommodating the intended functions.

A site survey shall be commissioned to include both surface and geotechnical aspects. The results of the survey shall be relevant (i.e. based on current information).

The geotechnical survey shall include the following items which could potentially influence the construction and operation of the data centre:

a) safe load bearing capacity;

b) buried cavities (natural or man-made);

c) buried utility infrastructures;

d) measurements, and expected variations of, soil resistivity and ground water conditions;

e) presence of contamination;

f) unexploded munitions;

g) risk associated with seismic activity according to ISO/IEC TS 22237-30.

The site survey report shall be used to assist in the design of:

1) foundation configurations (taking account of any load increases due to possible building growth);

2) drainage infrastructure;

3) an aquifer thermal energy storage system when part of the design intent.

The design of the earthing system shall consider the soil resistivity information determined by the geotechnical survey.

The site survey shall consider any need to provide spaces for support equipment such as underground fuel tanks (e.g. diesel or natural gas) to supply the generator(s), HVAC heat rejection systems, etc.

The selection of a site shall take into account any restrictions that could exist concerning land use and environmental impact aspects of any gaseous emissions and sound generation that could restrict fuel storage and generator operation.

6.2.2 Recommendations

The design of adequate drainage and foundation systems that will be required over the intended lifetime of the building should be based on the information provided by the geotechnical survey and should take into account possible future expansion.

6.3 Assessment of existing premises

6.3.1 Requirements

The suitability of the existing premises shall be determined by a risk analysis which reflects the specific needs of the proposed data centre, including assessment of the criteria listed in Clause 5.

The results of an existing survey shall only be used if:

a) a review has been undertaken to identify any changes;

b) it was conducted with a similar objective to that of Clause 5.

6.3.2 Recommendations

The assessment of existing drainage and foundation systems should be based on information provided by a geotechnical survey.

6.4 Utilities

6.4.1 General

The requirements and recommendations for implementation and physical separation of redundant pathways for a given utility serving the power supplies to the data centre are specified in ISO/IEC 22237-3.

The requirements and recommendations for implementation and physical separation of redundant pathways for a given utility serving the environmental control system of the data centre are specified in ISO/IEC 22237-4.

The requirements and recommendations for implementation and physical separation of redundant pathways for a given utility serving the telecommunications infrastructure of the data centre are specified in ISO/IEC TS 22237-5.

6.4.2 Requirements

The provision of external utilities to the premises including, but not restricted to, electricity, gas, water and telecommunications shall be adequate for the intended Availability Class of the data centre as defined in ISO/IEC 22237-1.

The telecommunication carrier or utility provider requirements of the customer shall be identified prior to site selection to ensure that the appropriate telecommunication carriers or utility providers are able to provide network or other services to the site as required by the customer.

The minimum distance of separation between pathways of different utilities are expected to be in accordance with national or local regulations, but not less than a minimum of 1,2 m.

Documentation shall be collated allowing the risk to data centre operation arising from utility infrastructures to be assessed.

A composite utilities plan showing all underground and above-ground utilities shall be provided according to ISO/IEC TS 22237-7.

6.4.3 Recommendations

Recommendations for the selection of pathways for electricity supply are provided in ISO/IEC 22237-3.

In general, where under control of the premises owner, the pathways within the premises should be located underground, unless the risk of accidental excavation is considered higher than the risk of atmospheric disturbance or deliberate or accidental physical damage.

Redundant pathways for the same utility serving the data centre, other than those of 6.4.1, should be physically separated between the boundary of the premises and the point of entry into buildings to ensure that a single incident will not cause damage to both paths and entrance facilities. Any additional distance of separation between pathways of different utilities should be based upon risk analysis.

7 Outside spaces

7.1 Access routes

7.1.1 Requirements

The number of access routes to the site shall take into account the risk of blockage which can affect the delivery of labour and materials and the accessibility for emergency services to the data centre. The design and construction of access routes shall consider expected loads and dimensions of vehicles. Above-ground exterior installations relevant to the data centre infrastructure (e.g. cooling towers) shall be protected, for example by guard rails.

The boundaries between access routes and the data centre spaces and surrounding areas shall meet the requirements for Protection Classes of ISO/IEC 22237-6. The protective measures shall provide protection against vehicle-related hazards [e.g. vehicles overheating and catching fire or losing control (e.g. break failure), vibration created by heavy vehicles, etc.].

7.1.2 Recommendations

Blockages resulting from extreme weather conditions (heavy snowfall, hail, flood, ice, etc.) and infrastructure repairs (bridges, roads, etc.) should be considered.

7.2 Parking

7.2.1 Requirements

The security requirements for the location and access restrictions to parking areas are specified in ISO/IEC 22237-6.

The layout and construction of parking areas shall consider expected loads, number and dimensions of vehicles, and environmental exposure. The parking area shall be designed to allow for positive drainage.

7.2.2 Recommendations

Recommendations for the location and access restrictions to parking areas are specified in ISO/IEC 22237-6.

Consideration should be given to any additional parking facilities which would be necessary during emergency situations, including those involving disaster recovery scenarios.

7.3 Temporary facilities

7.3.1 Requirements

The operation and growth of data centres can rely on the use of equipment which are only present on an intermittent or temporary basis (e.g. portable generators, UPS, chillers) and also the temporary storage of materials.

Spaces allocated to items of equipment which are only present on an intermittent or temporary basis shall be:

a) designated as reserved space which shall not be used for other purposes;

b) designed with, or to enable the temporary construction of, an adequate load bearing surface;

c) enable unobstructed connection of the equipment to the relevant data centre infrastructure;

d) located so that when the equipment is in operation it does not impact the operation of other facilities of the data centre and maintains the Protection Class.

Spaces allocated to temporary storage of materials shall be:

1) designated as reserved space which shall not be used for other purposes;

2) designed with, or to enable the temporary construction of, an adequate load bearing surface;

3) located so that delivery or removal of the stored materials does not impact the operation of other facilities of the data centre;

4) without hazard to adjacent facilities, infrastructures and premises.

7.3.2 Recommendations

Temporary facilities should not be located in spaces which are designated expansion areas of the data centre.

7.4 Fuel storage facilities and infrastructure

7.4.1 Requirements

The construction of fuel storage facilities, pumps and refill stations shall meet the requirements of the applicable Protection Class for the power supply and power distributions systems (see ISO/IEC 22237-3 and ISO/IEC 22237-6).

The design of bulk fuel storage facilities (both above and underground) shall consider:

a) the use of double-walled tanks to minimize leakage to the surrounding environment;

b) the hazard to adjacent facilities, infrastructures and premises;

c) the leakage detection system for the storage tank and fuel pipes to the generators;

d) the hazard of frost to fuel pipes (i.e. depth of running underground pipes, insulation, heating of pipes);

e) the limitations on the volume of the fuel allowed to be stored on-site;

f) the structure or device to contain leakage during the refuelling process (permanent or temporary).

7.4.2 Recommendations

If above-ground fuel tanks are exposed to the sun or other heat sources, shielding from heat sources or shading should be considered. If generators are located inside a building, a sloped floor to a dry sump pit with moisture detection should be considered for the generator room.

7.5 Underground facilities

7.5.1 Requirements

Vehicular traffic shall not be routed over underground facilities unless the facilities are protected by appropriate constructional measures.

7.5.2 Recommendations

Underground fuel storage tanks should be installed in proximity to the generator(s) but outside of potential future building expansion areas.

Underground fuel storage systems (tanks, piping, etc.) should be installed in locations where the components can be easily replaced or removed after their lifetime.

7.6 Perimeter design and Protection Class boundaries

7.6.1 General

ISO/IEC 22237-3, ISO/IEC 22237-4 and ISO/IEC 22237-6 specify required Protection Classes for the data centre spaces and areas. Requirements and recommendations for each Protection Class (and the boundaries between them) are specified in ISO/IEC 22237-6. The following subclauses specify the relevant constructional requirements and recommendations of boundaries of these areas in outside spaces with reference to the Protection Class of ISO/IEC 22237-6. Requirements and recommendations regarding co-location of boundaries are given in ISO/IEC 22237-6.

Subclause 8.4 contains requirements for all materials used to construct the boundaries of spaces of a given Protection Class. These are based on a minimum time of intrusion resistance using a specified set of tools as defined in Table 1.

Table 1 — Intrusion resistance

Resistance Class	Type of intruder	Tools of intruder (examples)	Resistance time [a]	Description
RC1	opportunistic intruder, not determined	n/a	n/a	RC offers only limited protection against physical force
RC2	opportunistic intruder with simple, basic tools	screwdrivers, knife, pipe wrench, pliers and wedges	3 min	attack with some preparation and a number of tools, allowing to make some but not prolonged noise
RC3	experienced intruder with heavy duty tools	additional second screw-driver, crowbar, hammer	5 min	deliberate intrusion attempt of a well-protected data centre facility, using a variety of tools with little regard for noise
RC4	experienced intruder using power tools	strike axe, crowbar, hammer, chisel, battery drills	10 min	experienced attempts at forced entry of a data centre facility, with no regard for noise
RC5	experienced intruder using power drill and cutting tools	drill hammer, jigsaw or reciprocating saw, angle grinder	15 min.	
RC6	experienced intruder using power drill and cutting tools	drill hammer, jigsaw or reciprocating saw, angle grinder	20 min	

NOTE This table is based on European Standard EN 1627. [5]

[a] Time period of uninterrupted intrusion attempt.

Six Resistance Classes (RC) for physical intrusion resistance properties of constructional elements, including but not limited to walls, roofs, gates, doors, windows and free-standing barriers, are defined in Table 1 by a combination of the three factors: type of intruder, tools of intruder and resistance time.

There are a number of internationally recognized assessment and audit schemes for intrusion resistance. Applicable regional and national standards, respectively, shall be taken into consideration.

NOTE 1 For Europe, EN 1627[5] is applicable, with its principles extended to other constructional elements including but not limited to those listed above.

NOTE 2 For the US, UL 752[21] applies.

The resistance times shall be taken into account in the design of the response system following identification of a potential intruder (see 8.4 for interior Protection Class boundaries).

The need for visual or acoustic screening of the data centre perimeters, exterior installations or individual exterior data centre areas shall be assessed.

The number of penetrations of the external physical barriers of Protection Classes should be minimized.

Where external areas exist, they shall be maintained. Buffer zones should be created to minimize disturbance to or by neighbours.

7.6.2 Free-standing barriers

The minimum effective height of free-standing barriers, h_e, is specified in Table 2. Table 2 also contains requirements for the height to which optimum penetration resistance is provided.

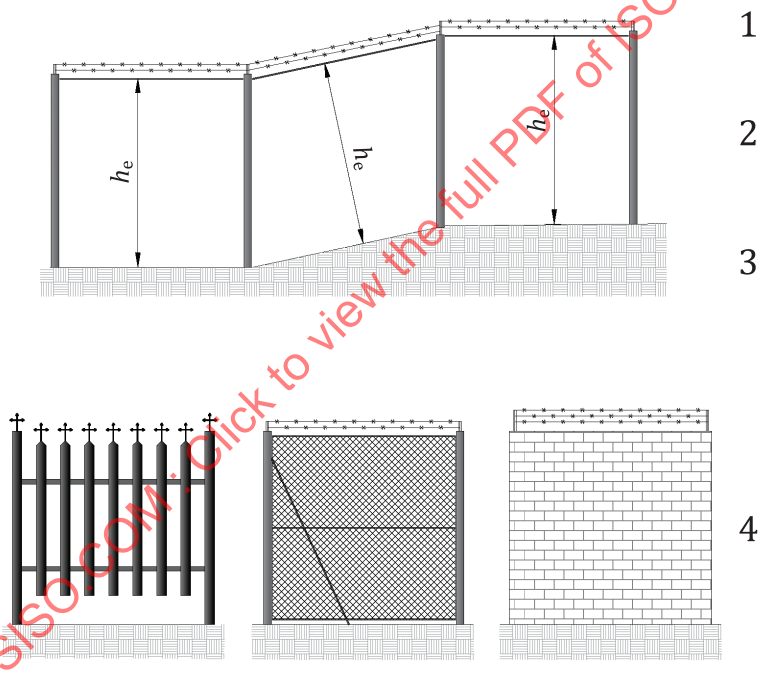
Table 2 — Heights and topping requirements for free-standing barriers

Resistance Class	Minimum effective height, h_e, above finished ground or floor surface as defined in Figure 2 m	Minimum height above finished ground or floor surface up to which the barrier shall provide optimum penetration resistance m	Topping
RC2	2,0	2,00	No
RC3	2,4	2,25	No
RC4	2,8	2,25	Yes

The installation of the components of the barrier shall ensure that the intended intrusion resistance of the complete free-standing barrier is maintained.

The installation of the free-standing barrier shall prevent intrusion under, over and around the free-standing barrier for a time equal to or greater than the time associated with the Resistance Class.

A horizontal distance of at least 2 m shall be maintained between the free-standing barrier and any structures of height of up to h_e that could allow intruders to gain access over the barrier. The horizontal distance between the free-standing barrier and any structures of height of more than h_e shall ensure that intruders cannot gain access over the barrier.



Key

1 topping (resistance class 4)
2 free-standing barrier
3 ground/floor
4 examples of free-standing barrier

Figure 2 — Examples of free-standing barriers and minimum effective height

7.6.3 Protection Class 1

The external boundary of areas designated Protection Class 1 shall be provided with an identifiable physical barrier. So far as is practicable, the construction of the boundary of an area of Protection Class 1 together

with the surveillance systems surrounding that space shall be designed to prevent intrusion. Resistance Class 2 of 7.6.1 should be applied.

NOTE The ability to provide extensive and distant surveillance outside the boundaries of Protection Class 1 can restrict the opportunity to prevent all intrusion attempts.

Pedestrian access to an area of Protection Class 1 shall be physically separated from the pedestrian access to any contained areas of Protection Class 2.

If vehicular access is required for an area or space of Protection Class 2, vehicular access to an area of Protection Class 1should be physically separated.

7.6.4 Protection Class 2

The external boundary of areas designated Protection Class 2 shall be provided with an identifiable physical barrier. The construction of the boundary of an area of Protection Class 2together with the surveillance, intrusion detection and response systems of ISO/IEC 22237-6 surrounding that space shall be designed to prevent intrusion. Resistance Class 2 of 7.6.1 should be applied.

Any penetrations of the physical barrier defining the outer boundary of an area of Protection Class 2 shall prevent unauthorized access.

If vehicular access is required for an area or space of Protection Class 3, vehicular access to an area of Protection Class 2 shall be physically separated.

7.6.5 Protection Class 3

The external boundary of areas designated Protection Class 3 shall be provided with an identifiable physical barrier. Any penetrations of the physical barrier defining the outer boundary of an area of Protection Class 3 shall prevent unauthorized access to spaces of the data centre.

A minimum of Resistance Class 2 of 7.6.1 shall be applied unless the risk assessment indicates a more stringent requirement. Resistance Class 3 of 7.6.1 should be applied.

The construction of the boundary of Protection Class 3 together with the surveillance, intrusion detection and response systems of ISO/IEC 22237-6 surrounding that space shall be designed to prevent intrusion.

7.6.6 Protection Class 4

The external boundary of areas designated Protection Class 4 shall be provided with an identifiable physical barrier. Any penetrations of the physical barrier defining the outer boundary of an area of Protection Class 4 shall prevent unauthorized access to spaces of the data centre.

A minimum of Resistance Class 2 of 7.6.1 shall be applied unless the risk assessment indicates a more stringent requirement. Resistance Class 3 of 7.6.1 should be applied.

The construction of the boundary of Protection Class 4 together with the surveillance, intrusion detection and response systems of ISO/IEC 22237-6 surrounding that space shall be designed to prevent intrusion.

8 Building construction

8.1 Load-bearing structure

8.1.1 Requirements

Load bearing structures shall be designed to support the anticipated point and distributed loading for the intended life of the data centre. Consideration shall be given to requirements for expansion.

Based on the risk assessment regarding seismic activity, relevant measures of ISO/IEC TS 22237-30 shall apply.

8.1.2 Recommendations

If an expansion of the data centre can be anticipated, the layout of the load-bearing structure should incorporate additional future loads. Alternatively, the structure should allow for modifications without risks to data centre operation (vibration, etc.). Consideration should be given to prevent a progressive collapse of the data centre building.

8.2 Building materials and finishes

8.2.1 Requirements

All open or rough surfaces shall be sealed to prevent dust or chemically-active particles from being distributed by the constant airflow in air-conditioned spaces.

The design of, and the materials used to construct, spaces intended to contain gaseous fire extinguishing systems shall provide the required level of air-tightness.

The design of, and the materials used to construct, spaces that have an identified risk of flooding shall provide the required level of water tightness (see also 10.1).

Building materials shall be selected which minimize the particulate matter produced during construction, operation or alterations.

Building materials shall be selected to minimize mould growth and rodent damage.

Building materials that can produce conductive particles shall be avoided.

Building materials shall be selected to minimize repetitive maintenance tasks.

Materials shall be selected with consideration of their reaction to fire (e.g. limit smoke and flame spread).

The amount of thermal insulation shall consider both the ambient environmental conditions and technical equipment heat output.

Based on the risk assessment regarding seismic activity, relevant measures of ISO/IEC TS 22237-30 shall be taken into account.

8.2.2 Recommendations

The building should be insulated thermally to minimize operating cost. Building materials in areas which will have low levels of fresh air circulation should be selected to minimize the emission of hazardous substances.

8.3 Electromagnetic interference

Consideration shall be given to sources of electromagnetic interference which could disrupt the effective operation of data processing, data storage and data transport. Assessment of the electromagnetic environment shall be undertaken in order to determine the need for any specific construction mitigation measures (e.g. upgrading the shielding).

Any aspects of building construction necessary to implement the telecommunication system bonding requirements of ISO/IEC 30129 shall be implemented.

8.4 Protection Class boundaries

8.4.1 General

ISO/IEC 22237-6 specifies Protection Classes for the data centre spaces. Requirements and recommendations for each Protection Class (and the boundaries between them) are specified in ISO/IEC 22237-6. The following subclauses specify the relevant constructional requirements and recommendations of the boundaries of

these areas with reference to the Protection Class against intrusion to data centre spaces of ISO/IEC 22237-6. Requirements and recommendations regarding co-location of boundaries are specified in ISO/IEC 22237-6. The requirements for cabinets, racks and frames are specified in ISO/IEC 22237-6.

8.4.2 Protection Class 1

The external boundary of areas designated Protection Class 1 shall be provided with an identifiable physical barrier.

Pedestrian access to an area of Protection Class 1 shall be physically separated from the pedestrian access to any contained areas of Protection Class 2.

So far as is practicable, the construction of the boundary of an area of Protection Class 1 together with the surveillance systems surrounding that space shall be designed to prevent intrusion.

NOTE The inability to provide extensive and distant surveillance outside the boundaries of Protection Class 1 can restrict the opportunity to prevent all intrusion attempts.

Based on the necessary security level, all doorsets, windows, grilles and shutters which form the external boundary of Protection Class 1 and all other boundary materials should meet the objectives of Table 1, Resistance Class 2.

8.4.3 Protection Class 2

The external boundary of areas designated Protection Class 2 shall be provided with an identifiable physical barrier.

If the boundary of an area of Protection Class 2 is co-located with one or more boundaries of areas of Protection Class 1 then the boundary of the lower Protection Class shall meet the requirements of Protection Class 2.

The construction of the boundary of an area of Protection Class 2 together with the surveillance, intrusion detection and response systems of ISO/IEC 22237-6 surrounding that space shall be designed to prevent intrusion.

Based on the necessary security level, all doorsets, windows, grilles and shutters which form the external boundary of an area of Protection Class 2 and all other boundary materials should meet the objectives of Table 1, Resistance Class 2, unless the risk assessment indicates a more stringent requirement.

Any penetrations of the physical barrier defining the outer boundary of an area of Protection Class 2 shall prevent unauthorized access. Such penetrations include those which are open or could be opened to enable normal or emergency function of the data centre infrastructures (such as pressure relief for gaseous extinguishing systems) where the prevention mechanisms shall be taken into account in the functional design of the penetration.

8.4.4 Protection Class 3

The external boundary of areas designated Protection Class 3 shall be provided with an identifiable physical barrier.

The construction of the boundary of an area of Protection Class 3 together with the surveillance, intrusion detection and response systems of ISO/IEC 22237-6 surrounding that space shall be designed to prevent intrusion.

Based on the necessary security level, all doorsets, windows, grilles and shutters which form the external boundary of an area of Protection Class 3 and all other boundary materials shall meet the objectives of Table 1, Resistance Class 2, unless the risk assessment indicates a more stringent requirement. Table 1, Resistance Class 3 should be applied.

Any penetrations of the physical barrier defining the outer boundary of an area of Protection Class 3 shall prevent unauthorized access to spaces of the data centre. Such penetrations include those which are open or

could be opened to enable normal or emergency function of the data centre infrastructures (such as pressure relief for gaseous extinguishing systems) where the prevention mechanisms shall be taken into account in the functional design of the penetration.

Access to areas of Protection Class 3 from docking bays, for receipt and dispatch of materials and equipment, should be separate from personnel entrances to areas of Protection Class 3.

8.4.5 Protection Class 4

The external boundary of areas designated Protection Class 4 shall be provided with an identifiable physical barrier.

The construction of the boundary of an area of Protection Class 4 together with the surveillance, intrusion detection and response systems of ISO/IEC 22237-6 surrounding that space shall be designed to prevent intrusion.

Based on the necessary security level, all doorsets, windows, grilles and shutters which form the external boundary of an area of Protection Class 4 and all other boundary materials shall meet the objectives of Table 1, Resistance Class 2, unless the risk assessment indicates a more stringent requirement. Table 1, Resistance Class 3 should be applied.

Any penetrations of the physical barrier defining the outer boundary of an area of Protection Class 4 shall prevent unauthorized access to spaces of the data centre. Such penetrations include those which are open or could be opened to enable normal or emergency function of the data centre infrastructures (such as pressure relief for gaseous extinguishing systems) where the prevention mechanisms shall be taken into account in the functional design of the penetration.

Based on the risk assessment regarding seismic activity, relevant measures of ISO/IEC TS 22237-30 shall apply.

8.5 Foundations

8.5.1 Requirements

Any foundations used to support the structure(s) accommodating the data centre spaces shall take into consideration the result of the site survey (see 6.2). When looking into a floor below grade level, water infiltration issues shall be considered, including height below surrounding drainage systems, secure and continuous vapour barriers, and water and vapour extraction systems.

Based on the risk assessment regarding seismic activity, relevant measures of ISO/IEC TS 22237-30 shall be taken into account.

The layout of the building's foundation and structure shall incorporate the earthing and bonding system, where required, as protection against lightning and electromagnetic interference. The design of the building's earthing system can vary according to the required Lightning Protection Level and to the site parameters including the soil resistivity. For protection against lightning, IEC 62305-3 shall be applied.

8.5.2 Recommendations

The design strength and extent of any foundations should consider any forecast expansion of the data centre spaces (vertical or lateral).

8.6 Exterior walls

8.6.1 Requirements

Based on the result of required risk assessments in ISO/IEC 22237-6, exterior walls shall provide the desired degree of physical protection against intrusion and external environmental events.

Exterior walls shall be designed and constructed to be resistant to the predicted external climatic conditions and external environmental events including fire, electromagnetic interference, vibration (including seismic activity and earthquake measures of ISO/IEC TS 22237-30), flooding, gas and dust hazards during the lifetime of the enclosed data centre spaces. During any repair of the exterior walls, the combination of any external protection provided to the repair together with the construction of the exposed material shall maintain the design performance.

Any fittings attached to penetrations of the Protection Class 2 boundaries with the intention of restricting access from areas of Protection Class 1 (intrusion bars fitted to windows) shall be designed to prevent attachment of towing cables, etc.

Where exterior walls provide the boundary of Protection Classes, the number of openings shall be minimized in accordance with the access requirements during both operation and emergency situations. Openings in walls and the doors in transportation routes shall be of sufficient width and height to allow for the largest pieces of equipment expected to be transported.

Any penetrations of the boundaries to areas of a given Protection Class which are open or can be opened to enable normal or emergency function of the data centre infrastructures (such as pressure relief for gaseous extinguishing systems) shall be provided with physical protection to prevent ingress of objects that might damage or restrict that function. When closed, they shall provide protection against the ingress of contaminants (particulate, liquid or gaseous). Such physical protection shall be taken into account in the functional design of the penetration.

Where there is an identified risk of ingress of contaminants (including water resulting from firefighting activity) from other spaces, mitigation shall be provided in the form of:

a) sealing;

b) detection;

c) drainage.

The position and size of openings that will provide pressure relief for gaseous fire extinguishing systems shall be addressed in the design phase. When calculating the size of openings in walls (e.g. pressure relief wall penetrations), the reduction of the clear opening by security features (i.e. lattices, grates, etc.) shall be considered.

8.6.2 Recommendations

None.

8.7 Interior walls and barriers

8.7.1 Requirements

The number of openings at Protection Class boundaries shall be minimized according to the access requirements during both operation and emergency situations.

Based on the result of the required risk assessments in ISO/IEC 22237-6, interior walls at the boundary of Protection Classes shall provide the desired degree of physical protection and maintain their function when subject to internal fire and internal environmental events including vibration (relevant seismic activity and earthquake measures of ISO/IEC TS 22237-30 shall apply), flooding, gas, dust and electromagnetic interference. They shall provide a barrier against the ingress of contaminants (particulate, liquid or gaseous) including water resulting from firefighting activity.

Interior walls shall be constructed in such a way as to allow for modifications, while at the same time providing the required intrusion resistance. Consideration shall be given to protection against surreptitious attacks to gain access to or damage the data stored, processed or transported which could require additional wall linings to detect or prevent this form of penetration.

Boundaries constructed from free-standing barriers shall meet the requirements of 7.6.2.

Openings in walls and the doors in transportation routes shall be of sufficient width and height to allow for the largest pieces of equipment expected to be transported.

All doors and door furniture shall have the same level of security as the boundary they are part of.

8.7.2 Recommendations

Mitigation measures against environmental events should be implemented by the use of construction methods and materials.

8.8 Roofs

8.8.1 Requirements

Where a roof covers, directly or indirectly, any data centre spaces, the roof and its sub-structure shall be designed and constructed to protect the data centre spaces from predicted external climatic conditions and from air-borne debris. Furthermore, relevant seismic activity and earthquake measures of ISO/IEC TS 22237-30 shall apply.

The design of sub-structures of the roof shall take into account the need for the repair of the roof and shall provide the required protection during the repair process.

The construction of the roof and its sub-structure shall be capable of supporting any additional loads created by any elements of the data centre facilities and infrastructures that are to be accommodated at roof level. The construction of the roof and its sub-structure shall also provide permanent access to any elements of the data centre facilities and infrastructures that are to be accommodated at roof level.

The requirements for visual screening of roof-top facilities and infrastructure shall be included in any calculations of loads to be supported.

Roofs and their sub-structures shall be designed and constructed to be resistant to the predicted external climatic conditions and external environmental events including fire, electromagnetic interference, vibration (including earthquakes), flooding, gas, strong winds and dust hazards during the lifetime of the directly or indirectly covered data centre spaces.

During any repair of the roofs, the combination of any external protection provided to the repair together with the construction of the sub-structure shall maintain the design performance.

Based on the result of required risk assessments in ISO/IEC 22237-6 the roof structure of each Protection Class shall provide the desired degree of physical protection against intrusion and external environmental events.

8.8.2 Recommendations

The roof areas should be considered for installation of renewables (e.g. solar panels). Penetrations through the roof and sub-structures should be avoided over spaces for data processing, data storage or data transport, or over spaces for electrical distribution equipment

8.9 Water drainage

8.9.1 Requirements

The roof and any sub-structure for the drainage of rain water from the roof or elsewhere shall be designed and constructed:

a) to avoid accumulation of rain water which could affect data centre spaces;

b) to ensure that all rain water is carried through a drainage system of appropriate capacity, taking into account expected seasonal and climatic changes.

The drainage system shall be designed and constructed to facilitate inspection, cleaning and repair.

Drainage systems and other piping systems (including those of the environmental control systems of ISO/IEC 22237-4) shall not be present in areas of Protection Class 2 and above unless suitable mitigation is applied in case of leakage.

8.9.2 Recommendations

Areas where leakage can occur should be fitted with a drainage detection system (see ISO/IEC 22237-6) and/or drainage facility.

The re-use of rainwater (e.g. roof top collected rainwater) should be considered (e.g. for data centre cooling or in sanitary systems).

8.10 Floors

8.10.1 Requirements

Based upon the risk analysis, relevant seismic activity and earthquake measures of ISO/IEC TS 22237-30 shall apply.

The floors and floor covering materials shall be capable of supporting the required static and dynamic loads. Floor covering materials shall be resistant to the expected levels of abrasion.

If a floor is part of a drain system, it shall be sloped accordingly (1 % to 3 %). In case of a levelled floor, the flatness of any finished floor shall have less than 3 mm height difference per any given m^2.

The load bearing capacity for respective areas of flooring, including the weight of any raised access floor plus any materials installed thereon, shall be designed and installed in accordance with Table 3, taking into account applicable regional and national standards, respectively. If requirements differ, the more stringent figure governs.

NOTE 1 For Europe, EN 1991-1-1[7] is applicable.

NOTE 2 For the US, ASCE 7[14] is applicable.

NOTE 3 For Japan, The Building Standard Law of Japan[22] is applicable.

The required load bearing capacity shall be communicated to, and coordinated with, the structural engineer.

Table 3 — Load capacity guidance for building structures

		Data centre spaces and access routes to those spaces					
		Computer room space [a]		Docking bay [b]		Other spaces	
		Required [c]	Recommended	Required [c]	Recommended	Required [c]	Recommended
Floor	Uniform load [d] (kN/m^2)	7,2	12,0	10,0	ffs	5,0	ffs
	Point load (kN)	5,0	7,5	7,5	12,0	3,0	ffs
Ceiling	Uniform hanging load [d] (kN/m^2)	1,2	2,4	—	—	1,2	2,4

NOTE Access routes include any paths and spaces used to transport or store equipment for installation in the specified spaces.

[a] The floor loading capacity for the electrical and mechanical spaces, and equipment access routes to support equipment replacement through the building to the electrical and mechanical spaces, shall be designed to meet the electrical and mechanical equipment located within the spaces (e.g. indoor generators, switchgear, battery strings, chillers, pumps, etc.).

[b] If the building is designed to support the loading or unloading of heavy components and the use of heavy loading or unloading devices such as an industrial fork lift, the docking bay load capacity shall be increased accordingly.

[c] If the minimum requirements are not met, it can be necessary to provide structural measures to distribute the loads.

[d] For interfloor structures the uniform load for floor and ceiling shall be added.

8.10.2 Recommendations

The load bearing capacity for respective areas of flooring, including the weight of any raised access floor plus any materials installed thereon, should meet the recommendations of Table 3.

In order to minimize the risk of electrostatic discharge to electronic equipment, floor surfaces should have an electrical resistance in accordance with regional and national standards, respectively.

For Europe, the electrical resistance should be less than (1×10^9) Ω in accordance with EN 1081:2018 + A1: 2020, method B (resistance to earth, R2).[3]

For the US, the flooring should meet ANSI/ESD S20.20-2021,[11] with electrical resistance less than (1×10^9) Ω in accordance with ANSI/ESD STM 97.1-2015,[12] and charge generation less than 100 V in accordance with ANSI/ESD STM 97.2-2016.[13]

PVC is not recommended as flooring material.

8.11 Raised access floors

8.11.1 Requirements

The need for a raised access floor within any data centre space shall be considered during the design phase since it affects delivery of the infrastructures and any decision can be irreversible.

Where used, raised access floors shall take into consideration applicable regional and national standards, respectively.

NOTE For Europe, EN 12825[8] is applicable.

The load bearing capacity for respective areas shall be determined according to the anticipated loading. The load class of a raised access floor shall be indicated at the entrance to the space.

The assembly shall be levelled and locked at a selected height, preventing vibrating displacement.

Consideration shall be given to prevent a progressive collapse of the raised access floor. This concerns the implementation of the assembly as well as operational procedures.

The raised access floor shall have a sufficient height above the slab to accommodate all projected services.

Ventilation panels shall be selected to provide the required airflow and support the required load.

ISO/IEC 30129 contains additional requirements in relation to the management of electrostatic discharge within the construction of raised access floors.

8.11.2 Recommendations

If stringers are used, they should be fixed.

NOTE 1 For Europe Where used, for raised access floors EN 12825:2001, class 6 is applicable. [8]

NOTE 2 For Japan, raised access floor systems are tested in accordance with JIS A 1450.[17]

8.12 Ceilings

8.12.1 Requirements

The load bearing capacity for respective areas of ceiling, including the weight of any suspended ceilings, M&E equipment and containment, shall be determined and shall meet the requirements of Table 3. The required load bearing capacity shall be communicated to, and coordinated with, the structural engineer.

Where suspended ceilings are installed in data centre spaces, a ceiling system constructed from non-particulating materials shall be installed.

Relevant seismic activity and earthquake measures of ISO/IEC TS 22237-30 shall apply.

8.12.2 Recommendations

The minimum clear height of computer rooms between finished floor to ceiling or ceiling beams depends on the environmental control concept and other infrastructure details (e.g. raised floor, overhead cabling) and should be a minimum of 3,0 m.

In rooms conditioned by freely circulated air, the underside of the ceiling should be even without any beams, etc. If beams are present, they should run parallel to the airflow in order not to present any obstruction to air circulation. If beams run at a right angle to the airflow, a suspended ceiling should be considered.

Suspended ceiling systems should also be considered in areas permanently occupied by personnel (control centre, offices, lobby, etc.) for acoustical reasons. Electrical and mechanical rooms should not have a suspended ceiling. For the computer room and telecommunication spaces a suspended ceiling is not recommended unless there are functional reasons, e.g. suspended ceiling space to be used for returning air.

8.13 Corridors and doors

8.13.1 Requirements

Access routes along which equipment and other goods are to be delivered to and from the data centre spaces shall be of sufficient width and height to allow for the largest pieces of equipment expected to be transported. Doors shall have no door sill and double doors shall have no centre post. If door sills are required (e.g. electromagnetic protection, contaminant ingress protection, smoke tightening, etc.), measures shall be taken into account to address the occasional need for moving equipment, e.g. a door threshold ramp.

Relevant seismic activity and earthquakes measures of ISO/IEC TS 22237-30 shall be taken into account.

The fire resistance rating of doors or windows in a wall shall conform to the fire resistance rating of the walls and barriers as specified in 11.1.

The construction of escape routes shall take into account the expected Protection Classes to be applied to the data centre spaces (see ISO/IEC 22237-6).

8.13.2 Recommendations

Doors within access routes along which equipment and other goods are to be delivered to and from the data centre spaces should provide a minimum vertical clearance of 2,4 m. Consideration should be given to the need for double-width doors. Surfaces of access routes and corridors should be of smooth material to avoid damage to transported equipment on castors or wheels. Thresholds should be avoided.

8.14 Transportation lifts

8.14.1 Requirements

Lift shafts and cabins shall be integrated into the Protection Class concept (see ISO/IEC 22237-6).

The requirements of interior wall openings shall apply to the height and width of the lift door.

For transportation lifts, the safety requirements of applicable regional and national standards shall be applied, respectively.

NOTE 1 For Europe, the EN 81 series[1] is applicable.

NOTE 2 For the US, ASME A17.1[15] is applicable.

NOTE 3 For Japan, the Building Standard Law of Japan, [22] JIS A 4302[18] and related regulation are applicable.

8.14.2 Recommendations

The cabin and its dimensions should allow for IT and technical components that are normally transported during daily operations. The load bearing capacity of the lift should be at least 1 500 kg. For other components, there should be a concept for alternative vertical transport routes.

9 Design of data centre spaces

9.1 Accommodation

9.1.1 General

The number and types of data centre spaces depends upon the size and complexity of the data centre.

Based on the risk assessment, data centre spaces need to be protected from (including, but not limited to) the following:

a) the impact of fire (flames spread, heat release, smoke and acid gas release);

b) water ingress (leakage, floods, fire-fighting water);

c) intrusion.

Regarding seismic activity and earthquakes, relevant measures of ISO/IEC TS 22237-30 shall apply.

The constructional challenge is to combine the required protection level with the flexibility and modularity needed to be able to keep up with rapidly changing and growing IT demands.

9.1.2 Requirements

The requirement for dimensions and unobstructed clearances in areas within the data centre structure reserved for data centre spaces shall be determined based on:

a) the environmental control concept from ISO/IEC 22237-4;

b) other infrastructure details such as cabinet heights, the requirements of raised access flooring and of pathways;

c) the sizing of transport routes for moving and/or replacing equipment and of areas for maintenance activities;

d) the requirements for emergency exit and evacuation.

The provision of on-site monitoring and/or management functionality shall be considered for all data centres.

Consideration shall be given to locating toilet facilities in such a way as to minimize the necessity for personnel to cross the boundaries of Protection Classes.

9.1.3 Recommendations

The accommodation of data centre spaces should consider the impact of:

a) new technologies (flexibility);

b) adaptation to changing parameters (adaptability);

c) increasing demands for space (scalability);

d) air containment systems.

The spatial relationship between the different data centre spaces should facilitate the overall operation based on adjacency factors.

The floor plan should minimize the amount of demolition during any expansion phase.

The organization of the building, the room program and the arrangement and adjacencies of rooms should mirror the functional and security requirements of data centre operations. For the supply of the building with utility and data services, this includes redundant and separate entrance rooms for telecommunication links, fuel lines, water and sewage. For the technical operation of the building this includes spaces for electrical and mechanical systems.

9.2 Control room space

The control room space typically houses computer system and network traffic monitors, and building automation systems and security systems monitoring equipment.

As needed, office(s) and meeting rooms should be provided adjacent to the control room space for supervisory functions and to form an emergency trouble-shooting area.

9.3 Computer room space

9.3.1 Requirements

The computer room space shall be designed to provide adequate space for initial and predicted quantities of information technology and network telecommunications equipment and support equipment. The design of the computer rooms shall consider the specific requirements of the system's components (size, clear height, floor loading, vibration, cooling/ventilation, etc.).

Factors to determine the location of a computer room space include:

a) proximity to power to reduce lengths of bus bars or cabling;

b) proximity to mechanical distribution rooms to reduce length of pipes and air ducts;

c) proximity to the communications distribution point (carrier entrance rooms) of the building.

9.3.2 Recommendations

Cabinets, racks and frames should be aligned in rows to create aisles. Computer room cabinet row length should not exceed 20 cabinets, racks or frames.

The installation of non-IT systems in computer rooms such as electrical (PDUs, etc.) or mechanical (AHUs, etc.) components and systems should be limited and associated risks should be mitigated.

9.4 Electrical space

9.4.1 Requirements

For layout of the rooms for the data centre's main electrical systems, the compartmentalization as described in ISO/IEC 22237-1 and ISO/IEC 22237-3 shall be applied. The design of the electrical rooms shall consider the specific requirements of the system's components (size, clear height, floor loading, vibration, cooling/ventilation, etc.).

9.4.2 Recommendations

The ease of accessibility of electrical systems during maintenance and emergencies should be considered.

9.5 Mechanical space

9.5.1 Requirements

For layout of the rooms for the data centre's main mechanical systems, the compartmentalization as described in ISO/IEC 22237-1 and ISO/IEC 22237-4 shall be applied. The design of the rooms shall consider the specific requirements of the system's components (size, clear height, floor loading, vibration, electrical supply, etc.).

9.5.2 Recommendations

The ease of accessibility of mechanical systems during maintenance and emergencies should be considered.

9.6 Telecommunications space

For requirements on telecommunications space, the requirements of ISO/IEC TS 22237-5 shall be applied and its recommendations should be considered.

9.7 Spaces for firefighting systems

9.7.1 General

For requirements and recommendations for firefighting systems, see ISO/IEC 22237-6.

9.7.2 Requirements

If the fire protection concept includes a system that requires pumps, compressors, valves, containers, etc. (clean agent, oxygen reduction, water mist), space shall be provided for the placement of these components of a fire extinguishing or prevention system.

If the fire protection concept includes a pre-action/double-interlocked sprinkler system, the sprinkler valves for the computer room shall be valved separately from other sprinkler systems. Valves controlling water to the computer room sprinkler system shall be labelled and easily identified as being separate from valves controlling sprinkler water to the rest of the building.

9.7.3 Recommendations

With most systems, the storage containers of the fire extinguishing medium should be installed in their own room or secured space and, depending on the fire extinguishing medium, in close proximity to the space they protect. The same applies to the central components of oxygen reduction systems.

Even if no fire prevention or extinguishing system is considered initially, an appropriate space should be allocated.

9.8 Storage space

9.8.1 Requirements

If removable digital media (e.g. tape drives) are stored on site or kept until disposal, a secure storage room shall be considered during design. The room shall conform to appropriate requirements regarding climate control, intrusion resistance, access control and fire protection.

9.8.2 Recommendations

If general storage rooms are provided, they should be located near receiving rooms and/or equipment rooms. Sufficient storage should be provided for all anticipated items such as hardware, spare parts, paper, cabling, etc.

If the data centre has an IT storage room for high value IT media or IT media with highly classified content and the media is picked up for disposal, separate pathways should be considered to ensure that these personnel have no contact with the other data centre staff.

9.9 Testing and holding spaces

As an intermediate space between the docking bay and the computer room, arriving information technology and network telecommunications equipment shall be uncrated and prepared in this space before installation in the computer rooms, in order to prevent or minimize the induction of contaminants into the computer room.

The space should be a separate room and typically has similar security requirements to a computer room.

9.10 Docking bay

9.10.1 Requirements

A data centre shall have an area where deliveries can be brought into the data centre and equipment or waste can be taken out of the data centre. A docking bay shall be designed to accommodate the largest items, and the largest quantity of items, expected to be delivered or removed from the data centre during operation.

9.10.2 Recommendations

The docking bay should provide shading and other protection against all types of precipitation and other environmental events. A docking bay should be designed to accommodate all sizes of locally standard commercial delivery vehicles. Receiving areas internal to the facility should be considered, as they provide greater physical security and protection from environmental elements.

9.11 General office space

Office areas should be at or near the main building entrance on the building perimeter to allow outside visibility.

10 Construction of data centre spaces

10.1 Protection against flooding

10.1.1 Requirements

Where the accommodation of the data centre spaces and pathways connecting them lies wholly or in part below the predicted range of ground water level or is at identified risk of flooding, water infiltration mitigation and extraction systems shall be considered. See also 8.5.1.

10.1.2 Recommendations

Data centre spaces and connecting pathways should avoid areas that lie wholly or in part below the predicted range of ground water level or that are at identified risk of flooding. See also 8.5.1.

10.2 Access to data centre spaces

10.2.1 Requirements

In data centre spaces and in access routes to those spaces along which equipment and goods will be transported, stairs shall be avoided in favour of ramps or lifts.

The width of ramps and lift doors shall be in accordance with those of doors in interior walls as specified in 8.13.

Ramps intended specifically for the transport of equipment and goods shall have a maximum inclination of 1:12.

10.2.2 Recommendations

Surfaces of access routes and corridors should be of smooth material to avoid damage to transported equipment on castors or wheels. Thresholds should be avoided.

10.3 Vapour density

10.3.1 Requirements

A risk assessment concerning vapour seal necessities shall be conducted with regard to both adjacent spaces, environmental conditions and equipment requirements, and measures shall be implemented accordingly. The vapour seal shall maintain a humidity level or prevent vapour infiltration to the controlled spaces.

10.3.2 Recommendations

Since vapour barriers are difficult to install and to seal off in existing buildings, areas that could become humidified in the future should have barriers installed during new construction. Flexibility is required to facilitate any on-going expansion. Therefore, it is necessary to analyse and clearly identify the areas which need vapour barriers or which could require them in the future.

If appropriate due to high fire loads, identified in the immediate adjacencies to data centre areas, construction methods for room partitions that prevent extreme heat radiation and extended vapour relief into adjacent data centre spaces should be considered, e.g. dedicated room cell systems in accordance with applicable regional and national standards

NOTE For Europe, EN 1047-2[2] is applicable for room cell systems.

11 Fire compartments and fire barriers

11.1 Fire compartments

11.1.1 Requirements

This subclause addresses the management of fire barriers together with the constructional aspects of fire compartments and associated spaces related to specific extinguishing systems. For information on technical aspects with regard to firefighting systems, see ISO/IEC 22237-6.

The data centre spaces together with the access routes and infrastructure pathways that penetrate the boundaries between those spaces shall comprise defined fire compartments bounded in three dimensions with appropriate levels of fire performance in order to prevent the spread of fire and combustion products (smoke and toxic gases) and to minimize the extent of loss.

The selection of compartment boundaries shall take into account the impact of fire within each compartment. Fire compartments shall, as a minimum, be defined by the boundaries of the Protection Classes of ISO/IEC 22237-6. The walls and barriers separating the fire compartments shall have a minimum fire rating in accordance with the requirements of the highest Protection Class present at the boundary of the fire compartment.

When pressurized fire suppression systems are implemented, the boundaries of the protected space shall have sufficient structural strength and integrity to contain the extinguishant discharge, and pressure relief shall be used to prevent excessive over- or under-pressurization of the protected space.

The ability to resist the impact of firefighting water shall be taken into account.