DRAFT INTERNATIONAL STANDARD
ISO/IEC DIS 22237-1

ISO/IEC JTC 1/SC 39

Secretariat: **ANSI**

Voting begins on:
2020-08-25

Voting terminates on:
2020-11-17

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

ICS: 35.020

IMPORTANT — Please use this updated version dated 2020-07-21, and discard any previous version of this DIS. This version contains line-numbering.

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 22237-1:2020(E)

© ISO/IEC 2020

iTeh STANDARD PREVIEW
(standards.iteh.ai)

COPYRIGHT PROTECTED DOCUMENT

Contents

36   **Foreword**

37   ISO (the International Organization for Standardization) and IEC (the International Electrotechnical
38   Commission) form the specialized system for worldwide standardization. National bodies that are
39   members of ISO or IEC participate in the development of International Standards through technical
40   committees established by the respective organization to deal with particular fields of technical
41   activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international
42   organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the
43   work. In the field of information technology, ISO and IEC have established a joint technical committee,
44   ISO/IEC JTC 1.

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

49   Attention is drawn to the possibility that some of the elements of this document may be the subject
50   of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent
51   rights. Details of any patent rights identified during the development of the document will be in the
52   Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

55   For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and
56   expressions related to conformity assessment, as well as information about ISO's adherence to the
57   World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the
58   following URL: www.iso.org/iso/foreword.html.

59   This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*,
60   Subcommittee SC 39, "*New title*".

61   A list of all parts in the ISO/IEC 22237 (and the ISO/IEC TS 22237) series can be found on the ISO
62   website.

63   This document will supersede ISO/IEC TS 22237-1:2018.

64   The following changes have been made:

65   a)   Clause 7 (Availability) has been revised;

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

68   d)   existing Annex A has been removed;

69   e)   new Annexes A and B have been added;

70   f)   tbd.

71 ## Introduction

72 The unrestricted access to internet-based information demanded by the information society has led to an
73 exponential growth of both internet traffic and the volume of stored/retrieved data. Data centres are housing
74 and supporting the information technology and network telecommunications equipment for data processing,
75 data storage and data transport. They are required both by network operators (delivering those services to
76 customer premises) and by enterprises within those customer premises.

77 Data centres need to provide modular, scalable and flexible facilities and infrastructures to easily accommodate
78 the rapidly changing requirements of the market. In addition, energy consumption of data centres has become
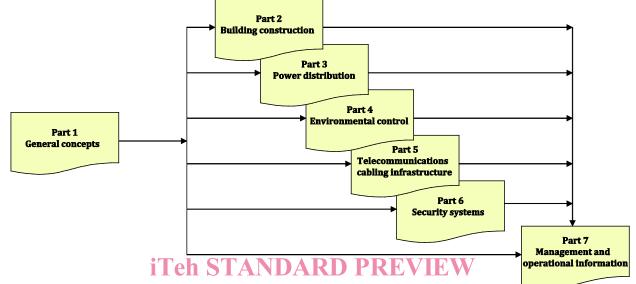79 critical both from an environmental point of view (reduction of carbon footprint) and with respect to
80 economical considerations (cost of energy) for the data centre operator.

81 The implementation of data centres varies in terms of:

82 a) purpose (enterprise, co-location, co-hosting or network operator facilities);

83 b) security level;

84 c) physical size;

85 d) accommodation (mobile, temporary and permanent constructions).

86 Note: Cloud services can be provided by all mentioned data centre types

87 The needs of data centres also vary in terms of availability of service, the provision of security and the
88 objectives for energy efficiency. These needs and objectives influence the design of data centres in terms of
89 building construction, power distribution, environmental control, telecommunications cabling and physical
90 security. Effective management and operational information is required to monitor achievement of the defined
91 needs and objectives.

92 The ISO/IEC 22237 series specifies requirements and recommendations to support the various parties
93 involved in the design, planning, procurement, integration, installation, operation and maintenance of facilities
94 and infrastructures within data centres. These parties include:

95 1) owners, operators, facility managers, ICT managers, project managers, main contractors;

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

98 3) suppliers of equipment;

99 4) installers, maintainers.

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

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

103 — ISO/IEC 22237-2, *Information technology — Data centre facilities and infrastructures — Part 2:*
104 *Building construction*;

105 — ISO/IEC 22237-3, *Information technology — Data centre facilities and infrastructures — Part 3:*
106 *Power distribution*;

107 — ISO/IEC 22237-4, *Information technology — Data centre facilities and infrastructures — Part 4:*
108 *Environmental control*;

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

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

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

115 The inter-relationship of the specifications within the ISO/IEC 22237 series is shown in Figure 1.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

116

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

ISO/IEC DIS 22237-1

118 This document, ISO/IEC 22237-1, defines the general concepts for the design and operation of data
119 centres. This includes a business risk and operational cost analysis as well as a classification system
120 for data centres with respect to "availability", "physical security" and "energy efficiency enablement".

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

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

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

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

130

131 **1 Scope**

132 This document:

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

135 b) defines the common aspects of data centres including terminology, parameters and reference models
136 (functional elements and their accommodation) addressing both the size and complexity of their
137 intended purpose;

138 c) describes general aspects of the facilities and infrastructures required to support data centres;

139 d) specifies a classification system, based upon the key criteria of "availability", "security" and "energy-
140 efficiency" over the planned lifetime of the data centre, for the provision of effective facilities and
141 infrastructure;

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

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

145 The following topics are outside of the scope of this series of International Standards:

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

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

149 3) safety and electromagnetic compatibility (EMC) requirements (covered by other standards and
150 regulations. However, information given in this International Standard can be of assistance in meeting
151 these standards and regulations).

152 **2 Normative references**

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

156 ISO/IEC TS 22237-2, *Information technology — Data centre facilities and infrastructures – Part 2:*
157 *Building construction*

158 ISO/IEC 22237-3:-, *Information technology — Data centre facilities and infrastructures – Part 3: Power*
159 *distribution*

160 ISO/IEC 22237-4:-, *Information technology — Data centre facilities and infrastructures – Part 4:*
161 *Environmental control*

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

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

166

167 ## 3 Terms, definitions and abbreviations

168 ### 3.1 Terms and definitions

169 For the purposes of this document, the following terms and definitions apply.

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

171 — IEC Electropedia: available at http://www.electropedia.org/

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

173 **3.1.1**
174 **availability**
175 ability of an item to be in a state to perform a required function under given conditions at a given instant of
176 time or over a given time interval, assuming that the required external resources are provided

177 [SOURCE: IEC 60050-191:1990, 191-02-05]

178 **3.1.2**
179 **building entrance facility**
180 facility that provides all necessary services, and which complies with all relevant regulations, for the entry
181 of specific infrastructures or services into a building

182 **3.1.3**
183 **building security**
184 facilities and systems necessary to provide the required levels of security at the entrance to and within the
185 building containing the data centre

186 **3.1.4**
187 **cabinet**
188 enclosed construction for housing closures and other information technology equipment

189 [SOURCE: ISO/IEC 14763-2:2019, 3.1.6 — modified: removed the word "intended" and replaced
190 "telecommunications components and" with "information"]

191 **3.1.5**
192 **co-hosting data centre**
193 data centre in which multiple customers are provided with access to network(s), servers and storage
194 equipment on which they operate their own services/applications

195 Note 1 to entry: Both the information technology equipment and the support infrastructure of the building are provided as a service by
196 the data centre operator.

197 **3.1.6**
198 **co-location data centre**
199 data centre in which multiple customers locate their own network(s), servers and storage equipment

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

202 **3.1.7**
203 **computer room space**
204 area within the data centre that accommodates the data processing, data storage and telecommunication
205 equipment that provides the primary function of the data centre

206 **3.1.8**
207 **control room space**
208 area within the data centre used to control the operation of the data centre and to act as a central point for
209 all control and monitoring functions

210 **3.1.9**
211 **data centre**
212 a structure, or group of structures, dedicated to the centralised accommodation, interconnection and
213 operation of information technology and network telecommunications equipment providing data storage,
214 processing and transport services together with all the facilities and infrastructures for power distribution

215 and environmental control together with the necessary levels of resilience and security required to provide
216 the desired service availability

217 Note 1 to entry: A structure can consist of multiple buildings and/or spaces with specific functions to support the primary function.

218 Note 2 to entry: The boundaries of the structure or space considered the data centre, which includes the information and
219 communication technology equipment and supporting environmental controls, can be defined within a larger structure or building.

220 [SOURCE: ISO/IEC 30134-1:2016, 3.1.4]

221 **3.1.10**
222 **data centre security**
223 necessary facilities and systems that provide the required levels of security at the entrance to and within
224 the data centre

225 **3.1.11**
226 **demarcation point**
227 point where the operational control or ownership changes

228 **3.1.12**
229 **electrical distribution space**
230 area used for housing facilities to distribute electrical power between the transformer space and electrical
231 spaces within the data centre or elsewhere within the premises or individual buildings within the premises

232 **3.1.13**
233 **electrical space**
234 area within the data centre used for housing facilities to deliver and control electrical power to the data
235 centre spaces (including switchboards, batteries, uninterruptible power systems (UPS) etc.)

236 **3.1.14**
237 **enterprise data centre**
238 data centre that is operated by an enterprise which has the sole purpose of the delivery and management
239 of services to its employees and customers

240 **3.1.15**
241 **external premises security**
242 facilities and systems that provide the required levels of security for the area between the building and the
243 boundary of the premises

244 **3.1.16**
245 **energy efficiency enablement**
246 ability to measure the energy consumption and to allow calculation and reporting of energy efficiency of the
247 various facilities and infrastructures

248 **3.1.17**
249 **facility**
250 spaces and pathways that accommodate a specific infrastructure

251 **3.1.18**
252 **functional capability**
253 ability of the data centre (or system or sub-system) to deliver its intended function

254 **3.1.19**
255 **functional element**
256 source of supply, device or path

257 **3.1.20**
258 **generator space**
259 area used for housing the installation of electrical power supply generation equipment together with control
260 systems, storage of associated fuels or energy conversion equipment
261

262 **3.1.21**
263 **holding space**
264 area within the data centre used for the holding of equipment prior to being brought into service or having
265 been taken out of service

266 **3.1.22**
267 **infrastructure**
268 technical systems providing functional capability of the data centre (e.g. power distribution, environmental
269 control and physical security)

270 **3.1.23**
271 **main distributor**
272 distributor used to make connections between the main distribution cabling subsystem, network access
273 cabling subsystem and cabling subsystems and active equipment

274 [SOURCE: ISO/IEC 11801-5:2017, 3.1.6, - modified: removed "as specified in ISO/IEC 11801-1"]

275 **3.1.24**
276 **mechanical space**
277 area that is used for housing mechanical equipment and infrastructure that provides environmental control
278 for the data centre spaces (including chillers and water treatment, air handling and fire suppression
279 systems)

280 **3.1.25**
281 **network operator data centre**
282 data centre that has the primary purpose of the delivery and management of broadband services to the
283 operators customers

284 **3.1.26**
285 **physical security**
286 measures (combining physical and technological controls), procedures and responsibilities to maintain the
287 desired level of availability for the facilities and infrastructures of the data centres in relation to access
288 control and environmental events

289 **3.1.27**
290 **planned downtime**
291 period of time during which a system or sub-system does not provide functional capability whilst it
292 undergoes maintenance or is switched off to test the response of a related system or sub-system

293 **3.1.28**
294 **premises entrance facility**
295 facility that provides all necessary services, and which complies with all relevant regulations, for the entry
296 of specific infrastructures or services into premises

297 **3.1.29**
298 **reliability**
299 probability of an item to be in a state to perform a required function under given conditions over a given
300 time interval

301 **3.1.30**
302 **storage space**
303 secured area where general goods and/or data centre goods to be used in the premises and data centre
304 are stored

305 **3.1.31**
306 **system**
307 set of interrelated functional elements considered in a defined context as a whole and separated from their
308 environment
309

310 **3.1.32**
311 **telecommunications**
312 branch of technology concerned with the transmission, emission, and reception of signs, signals, writings,
313 images, and sounds, that is, information of any nature by cable, radio, optical, or other electromagnetic
314 systems

315 [SOURCE: ISO/IEC 11801-1:2017, 3.1.78 – modified: Note 1 to entry deleted]

316 **3.1.33**
317 **telecommunications cabling**
318 telecommunications cabling infrastructure from the telecommunications space(s) to the premises entrance
319 facility

320 **3.1.34**
321 **telecommunication equipment**
322 equipment within the data centre that provides telecommunication services within the data centre

323 **3.1.35**
324 **telecommunications space**
325 area which may house demarcation points and telecommunication equipment associated with the building
326 entrance facility and which may allow service providers restricted access to the data centre

327 **3.1.36**
328 **testing space**
329 area within the data centre used for the testing and configuring of equipment prior to being brought into
330 service

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

332 **3.1.37**
333 **transformer space**
334 area used for housing equipment necessary to convert voltage levels and/or provide necessary isolation
335 for the connection to the equipment within the premises or individual buildings within the premises

336 **3.1.38**
337 **uninterruptible power system**
338 combination of convertors, switches and energy storage devices (such as batteries), constituting a power
339 system for maintaining continuity of load power in case of input power failure

340 Note 1 to entry: Continuity of load power occurs when voltage and frequency are within rated steady-state and transient tolerance
341 bands and with distortion and interruptions within the limits specified for the output port. Input power failure occurs when voltage and
342 frequency are outside rated steady-state and transient tolerance bands or with distortion or interruptions outside the limits specified
343 for the UPS.

344 [SOURCE: IEC 62040-1:2017, 3.101]

345 **3.1.39**
346 **unplanned downtime**
347 unexpected time taken, following a failure of functional capability, to repair the relevant infrastructure
348 together with the "re-boot" time necessary to recover functional capability following that repair

349 **3.2 Abbreviations**

350 For the purposes of this document the following abbreviations apply:

351 CRAC   Computer Room Air Conditioner/Conditioning

352 CRAH   Computer Room Air Handling Unit

353 ffs   for further study

354 MTBF   Mean Time Between Failures

355 MTTR   Mean Time To Repair

356 NOC   Network Operating Centre

357   UPS   Uninterruptible Power System

4 Conformance

359   For a data centre design to conform to this document:

360   a)   a business risk analysis according to Clause 5 shall be completed;

361   b)   an appropriate Availability Class in 7.2 shall be selected using a business risk analysis in Clause 5;

362   c)   appropriate Protection Classes for the data centre spaces and pathways shall be in accordance with
363   7.3.1;

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

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

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

367   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

370   The overall availability of a data centre is a measure of the continuity of its data processing, storage, and
371   transport functions. The acceptable level of the overall availability of a data centre is determined by a
372   number of factors including:

373   a)   a business impact analysis (see 5.2) - the cost associated with a failure of service provision, which
374   depends upon a number of factors including the function and importance of the data centre;

375   b)   externally applied commercial pressures (e.g. insurance costs).

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

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

382   The availability of each of the facilities and infrastructures of the data centre required to support the desired
383   overall availability is described by an availability classification (see 7.2). The design of each of the data
384   centre infrastructures shall take account of their impact on overall availability and the costs associated with
385   the predicted downtime associated with failure or planned maintenance.

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

392   A business risk analysis identifies the aspects of the facilities and infrastructures that require investment in
393   terms of design improvements to reduce their impact and/or probability of those risk events.

5.2 Business impact analysis

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

397   The parameters to be considered within such an analysis will depend upon the purpose of the data centre.
398   Some organisations can assign a monetary value (or range) to loss of service which may include the
399   following:

400   a)   immediate financial penalties;

401   b)   consequential losses;