



DPC: 20/30417874 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 24 April 2020

Origin: International

Latest date for receipt of comments: 11 June 2020

Project No. 2019/03351

Responsible committee: TCT/7 Telecommunications - Installation requirements

Interested committees:

Title: Draft BS ISO/IEC 24383 Ed1 Information technology - Physical network security for the accommodation of customer premises cabling infrastructure and information technology equipment.

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 11 June 2020

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/Figure/ Table/Note	Type of comment	Commend (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



JTC1-SC25/2949/CD

COMMITTEE DRAFT (CD)

PROJECT NUMBER:
ISO/IEC 24383 ED1

DATE OF CIRCULATION:
2020-04-17

CLOSING DATE FOR COMMENTS:
2020-07-10

SUPERSEDES DOCUMENTS:
JTC1-SC25/2914/CD, JTC1-SC25/2947/CC

IEC ISO/IEC JTC 1/SC 25 : INTERCONNECTION OF INFORMATION TECHNOLOGY EQUIPMENT	
SECRETARIAT: Germany	SECRETARY: Mr Marco Peter
OF INTEREST TO THE FOLLOWING COMMITTEES:	PROPOSED HORIZONTAL STANDARD: ☐ Other TC/SCs are requested to indicate their interest, if any, in this CD to the secretary.
FUNCTIONS CONCERNED: ☐ EMC ☐ ENVIRONMENT ☐ QUALITY ASSURANCE ☐ SAFETY	

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

TITLE:

Information technology - Physical network security for the accommodation of customer premises cabling infrastructure and information technology equipment

NOTE FROM TC/SC OFFICERS:

CONTENTS

1		
2	INTRODUCTION.....	5
3	1 Scope.....	6
4	2 References.....	6
5	3 Definitions and abbreviations.....	6
6	3.1 Definitions.....	6
7	3.2 Abbreviations.....	11
8	4 CONFORMANCE.....	11
9	5 RISK ASSESSMENT AND SECURITY CONCEPTS.....	12
10	5.1 Risk assessment.....	12
11	5.2 Security Grades.....	13
12	6 DESIGN.....	14
13	6.1 General.....	14
14	6.2 SG2.....	14
15	6.3 SG3.....	17
16	7 PLANNING.....	19
17	7.1 General.....	19
18	7.2 SG2.....	19
19	7.3 SG3.....	21
20	8 INSTALLATION.....	22
21	8.1 General.....	22
22	8.2 SG2.....	22
23	8.3 SG3.....	24
24	8.4 Commissioning.....	25
25	9 OPERATION.....	25
26	9.1 SG2.....	25
27	9.2 SG3.....	26
28	9.3 Automated infrastructure management (AIM) systems for security.....	27
29	10 EVOLUTION OF SECURITY SYSTEMS.....	28
30	Annex A (normative) Free standing barriers.....	30
31	Annex B (normative) Video surveillance.....	31
32	B.1 Requirements.....	31
33	B.2 Recommendations.....	31
34	Annex C (normative) Intrusion detection.....	33
35	C.1 Requirements.....	33
36	C.2 Recommendations.....	34
37	Annex D (normative) Access control.....	36
38	D.1 Requirements.....	36
39	D.2 Recommendations.....	37
40	Annex E (normative) Management of personnel.....	39
41	E.1 Requirements.....	39
42	E.2 Recommendations.....	40
43	Bibliography.....	42

44

45	List of figures	
46	Figure 1 – Risk assessment concepts	12
47	Figure A.1 – Examples of free-standing barriers and minimum effective heights	30
48		
49	List of tables	
50	Table 1 – Overview of Security Grades	13
51	Table 2 – Requirements for door hardware and their corresponding conformance	
52	standards for Europe and the USA.....	15
53		
54		

INFORMATION TECHNOLOGY –

Generic cabling – Physical network security for the accommodation of customer premises cabling infrastructure and information technology equipment

FOREWORD

ISO (International Organization for Standardization) and IEC (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. Their preparation is entrusted to technical committees; any ISO and IEC member body interested in the subject dealt with may participate in this preparatory work. International governmental and non-governmental organizations liaising with ISO and IEC also participate in this preparation.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC and ISO member bodies.

IEC, ISO and ISO/IEC publications have the form of recommendations for international use and are accepted by IEC and ISO member bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC, ISO and ISO/IEC publications is accurate, IEC or ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

In order to promote international uniformity, IEC and ISO member bodies undertake to apply IEC, ISO and ISO/IEC publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any ISO/IEC publication and the corresponding national or regional publication should be clearly indicated in the latter.

ISO and IEC provide no marking procedure to indicate their approval and cannot be rendered responsible for any equipment declared to be in conformity with an ISO/IEC publication.

All users should ensure that they have the latest edition of this publication.

No liability shall attach to IEC or ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC or ISO member bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication of, use of, or reliance upon, this ISO/IEC publication or any other IEC, ISO or ISO/IEC publications.

Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 24383 was prepared by subcommittee 25: Interconnection of information technology equipment, of ISO/IEC joint technical committee 1: Information technology.

This International Standard has been approved by vote of the member bodies, and the voting results may be obtained from the address given on the second title page.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

97 INTRODUCTION

- 98 ISO/IEC 14763-2 specifies requirements and recommendations for the installation specification, quality
99 assurance and installation practices for customer premises cabling in accordance with the ISO/IEC
100 11801 series.
- 101 Those requirements provide basic level of physical network security for the cabling and associated
102 infrastructure.
- 103 This Standard builds upon the requirements of ISO/IEC 14763-2 by facilitating the timely and effective
104 protection of the customer premises cabling infrastructure to avoid loss/damage to the physical
105 information transport network.
- 106 This document provides comprehensive planning and installation requirements for physical network
107 security as well as methods that protect the telecommunications infrastructure from theft, vandalism,
108 intrusions, and unauthorized modifications.
- 109 The requirements and recommendations may be applied to existing buildings and also during building
110 construction, or renovation, when actions are significantly less expensive and less disruptive than after
111 the building is occupied.
- 112 The standard incorporates the use of automated infrastructure management (AIM) systems, including
113 those in accordance with ISO/IEC 18598, to further enhance the security of cabling infrastructure and
114 integrate the physical network security with other security systems in the premises.
- 115 This document is intended to be used by
- 116 • architects, building owners, building designers and builders,
 - 117 • consultants,
 - 118 • facility managers and network managers,
 - 119 • designers, suppliers, installers, inspectors (auditors), maintainers and owners of information
120 technology cabling.
- 121
- 122

INFORMATION TECHNOLOGY - Generic cabling – Physical network security for the accommodation of customer premises cabling infrastructure and information technology equipment

1 Scope

This document specifies requirements and recommendations providing security to the physical network comprising customer premises cabling in accordance with ISO/IEC 11801 series, associated infrastructure and accommodation of information technology equipment.

The document covers the security of the telecommunications cables, pathways, spaces, and other infrastructure components of the telecommunications physical infrastructure to protect the telecommunications infrastructure from theft, vandalism, intrusions, and unauthorized modifications.

The document addresses

- risk assessment,
- design (including construction), planning and installation practices based on a required Security Grade (SG),
- intrusion detection,
- administration including Automated Infrastructure Management (AIM).

The document applies to existing buildings and structures together with those being planned for construction.

The following are outside the scope of this International Standard

- data protection methods such as encryption,
- practices that address protection from non-contact cable tapping, audio, visual or RF snooping and other forms of unauthorized monitoring.

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

2 References

The following referenced documents are indispensable for the application 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 14763-2:20xx, *Information technology - Implementation and operation of customer premises cabling - Part 2: Planning and installation*

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

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this document the following definitions and those of ISO/IEC 14763-2 apply.

Editors NOTE: The “greyed-out” definitions are from ISO/IEC 14763-2 and are for clarity in early drafts of this document. They will be removed in the later stages of development.

- 165 **3.1.1**
166 **access control system**
167 system that provides selective restriction of access to a space or cabling component
- 168 **3.1.2**
169 **administration**
170 methodology defining the documentation requirements of a cabling system and its containment, the
171 labelling of functional elements and the process by which moves, additions and changes are recorded
172 [SOURCE 11801-1:2017, 3.1.1]
- 173 **3.1.3**
174 **AIM system**
175 integrated hardware and software system that automatically detects the insertion or removal of cords,
176 documents the cabling infrastructure including connected equipment enabling management of the
177 infrastructure and data exchange with other systems
178 [SOURCE 18598:2016, 3.1.3]
- 179 **3.1.4**
180 **alarmed carrier**
181 system for detecting intrusion into a pathway using optical fibre as a vibration sensor
- 182 **3.1.5**
183 **alarm-enabled**
184 capable of triggering an alarm with the intrusion alarm system
- 185 **3.1.6**
186 **authorized personnel**
187 persons able to access a space or pathway of a defined Security Grade
- 188 **3.1.7**
189 **cabinet**
190 enclosed construction intended for housing closures and other telecommunications components and
191 equipment
192 [SOURCE 14763-2:20xx, 3.x.x1]
- 193 **3.1.8**
194 **cable management system**
195 system used for the support and/or containment, retention, protection of all types of cables, information
196 and communication lines, electrical power distribution conductors and their associated accessories
197 Note 1 to entry Includes ducts and tubes housing, or intended to house, blown telecommunications cables and/or cable elements.
198 [SOURCE 14763-2:20xx, 3.x.x]
- 199 **3.1.9**
200 **cabling**
201 system of telecommunications cables, cords and connecting hardware that supports the connection of
202 information technology equipment
203 [SOURCE 11801-1:2017, 3.1.21]
- 204 **3.1.10**
205 **cabling component**
206 any product associated with the cabling installation including cables, connecting hardware, closures,
207 cabinets, frames, racks and pathway systems together with components used to provide bonds to
208 earthing systems
209 [SOURCE 14763-2:20xx, 3.x.x]
- 210 **3.1.11**
211 **closed pathway system**
212 cable management system which does not allow installation of cables by laying without tensile load

213 [SOURCE 14763-2:20xx, 3.x.x]

214 **3.1.12**

215 **common distribution space**

216 primary or secondary building distribution space

217 **3.1.13**

218 **countermeasure**

219 step taken to prevent a threat triggering an event

220 **3.1.14**

221 **dialler unit**

222 device that communicates with external monitoring or response entities to report exceptions to pre-programmed
223 conditions via a specific telephone number, set of telephone numbers or a network connection.

224 **3.1.15**

225 **door hardware**

226 metallic fixtures that enable opening, closing, and locking a door

227 **3.1.16**

228 **entrance room**

229 space within, or at the boundary of, a building housing the demarcation point where facilities owned by
230 external access and/or service providers interface with the premises cabling

231 [SOURCE 14763-2:20xx, 3.x.x, modified by deletion of NOTE 1 to entry]

232 **3.1.17**

233 **electronic locking mechanism**

234 device that allows access following receipt of digital or analog information indicating an appropriate
235 authorisation status of the person entering the information

236 **3.1.18**

237 **effective height of a free-standing barrier**

238 shortest distance between any point on the top of the permanent part of the free-standing barrier
239 (excluding any toppings) and the surface of the supporting ground when measured in the plane of the
240 barrier

241 **3.1.19**

242 **event**

243 vulnerability that has been exploited by a threat

244 **3.1.20**

245 **external boundary**

246 physical barrier(s) demarcating a space or structure of a given Security Grade (SG)

247 Note 1 to entry: access floors and suspended ceilings through which unauthorised access to a space may be gained are not
248 considered to be external boundaries. In such cases, the fixed building fabric upon which these structures are built is the external
249 boundary.

250 **3.1.21**

251 **external telecommunications cabinet**

252 outdoor enclosure accommodating telecommunications equipment and associated cabling

253 **3.1.22**

254 **free-standing barrier**

255 wall, fence, gate, turnstile or other similar self-supporting barrier, and its associated foundations,
256 designed to prevent entry to a space of a given Security Grade

- 257 **3.1.23**
258 **frame (rack)**
259 open construction intended for housing closures and other telecommunications equipment
260 [SOURCE 14763-2:20xx, 3.x.x]
- 261 **3.1.24**
262 **hand hole**
263 point of access to a pathway that is too small for a person to enter to perform work but that allows the
264 routing of cables during the cable installation process such that bending and pulling requirements are
265 met (an example of a hand-hole within a building is called a draw-box)
266 [SOURCE 14763-2:20xx, 3.x.x]
- 267 **3.1.25**
268 **intelligent building system**
269 equipment and telecommunication infrastructure that supports monitoring, control, operation and
270 management of building services
- 271 **3.1.26**
272 **keypad**
273 manual input devices, typically requiring telecommunications connectivity, that allow individuals to enter
274 specific codes to arm, disarm or diagnose intrusion systems
- 275 **3.1.27**
276 **joint closures**
277 sealed housing protecting the joining or splicing of the conductors and optical fibres of
278 telecommunications cables
- 279 **3.1.28**
280 **junction box**
281 protective housing and associated space that enables cables to be routed between pathway systems
- 282 **3.1.29**
283 **maintenance hole (telecommunications)**
284 vault/chamber located in the ground or earth as part of an underground conduit system and used to
285 facilitate placing, connectorization, and maintenance of cables as well as the placing of associated
286 equipment, in which it is expected that a person will enter to perform work
287 [SOURCE 14763-2:20xx, 3.x.x]
- 288 **3.1.30**
289 **mechanical locking mechanism**
290 device that allows access by means of physically coded key or tool
- 291 **3.1.31**
292 **open pathway system**
293 pathway system which allows installation of cables by laying without tensile load
294 [SOURCE 14763-2:20xx, 3.x.x]
- 295 **3.1.32**
296 **openable pathway system**
297 cable management system which restricts access to installed cables but which can be opened to allow
298 installation of cables by laying without tensile load
299 [SOURCE 14763-2:20xx, 3.x.x]
- 300 **3.1.33**
301 **pathway (cable route, cable way)**
302 defined route for cables between termination points
303 [SOURCE 14763-2:20xx, 3.x.x]

- 304 **3.1.34**
 305 **pathway system**
 306 cable management system or other area or volume defined by markings or fittings used to protect and/or
 307 support the cabling in order that its desired performance is maintained
 308 [SOURCE 14763-2:20xx, 3.x.x]
- 309 **3.1.35**
 310 **primary building distribution space**
 311 space accommodating primary point of distribution of any common cabling infrastructure within multi-
 312 tenant buildings
 313 [SOURCE 14763-2:20xx, 3.x.x]
- 314 **3.1.36**
 315 **rack**
 316 see frame
 317 [SOURCE 14763-2:20xx, 3.x.x]
- 318 **3.1.37**
 319 **secondary building distribution space**
 320 space accommodating optional points of distribution, additional to the main point of distribution, of any
 321 common cabling infrastructure within multi-tenant buildings
 322 [SOURCE 14763-2:20xx, 3.x.x]
- 323 **3.1.38**
 324 **space**
 325 specified volume (e.g. room, maintenance hole or part thereof) housing closures and/or other
 326 telecommunications equipment
 327 [SOURCE 14763-2:20xx, 3.x.x]
- 328 **3.1.39**
 329 **surveillance system**
 330 devices and mechanisms used to monitor and detect behaviour or activity to protect the physical network
- 331 **3.1.40**
 332 **tamper evident**
 333 designed or enabled to show access or attempts to access
- 334 **3.1.41**
 335 **terminal equipment**
 336 equipment at an outlet used to access information provided by transmission equipment
 337 [SOURCE: ISO/IEC 11801-1:2017, 3.1.81]
- 338 **3.1.42**
 339 **terminal equipment outlet**
 340 fixed connecting device which provides an interface to the terminal equipment
 341 [SOURCE: ISO/IEC 11801-1:2017, 3.1.80, modified by deletion of Note 1 to entry]
- 342 **3.1.43**
 343 **threat**
 344 method by which a vulnerability can be exploited to create an event
- 345 **3.1.44**
 346 **topping**
 347 construction, added to the top of a free-standing barrier, and designed to be an effective intruder
 348 deterrent or for a decorative display of security

3.1.45**transmission equipment**

active equipment used to distribute information from distributors to other distributors and to outlets
[SOURCE: ISO/IEC 11801-1:2017, 3.1.84]

3.1.46**vulnerability**

weakness that can be potentially exploited by a threat

3.2 Abbreviations

For the purposes of this document the following abbreviations and those of ISO/IEC 14763-2 apply.

AHJ authorities having jurisdiction

SG Security Grade

4 CONFORMANCE

For the physical network security of a telecommunications cabling infrastructure to conform to this International Standard it shall conform, as a minimum, to the specification, planning, installation and installation requirements of ISO/IEC 14763-2. This provides a basic level of physical network security designated Security Grade (SG) 1.

In order to provide increased levels of physical network security determined by a risk assessment, the requirements for either SG2 or SG3 shall be met.

5 RISK ASSESSMENT AND SECURITY CONCEPTS

5.1 Risk assessment

The requirements for physical network security should be determined by the organization responsible for the data transported over the telecommunications infrastructure. There may be multiple authorities having jurisdiction (AHJ) involved in the assessment of security impacts to a system, facility or user. It is important to identify the various AHJs involved in the risk assessment, as well as their areas of expertise, responsibility and authority.

The requirements should be determined following a risk assessment based on the threats posed to the data, and the “classification” of that data.

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

Figure 1 illustrates the concept of the risk assessment which is described as follows.

- a) Sensitivity: the classification of the information (data) sensitivity should be determined at an early stage, so that it is possible to deploy appropriate countermeasures. The nature of the “classification” maybe “native”, or “raised” due to the effects of data aggregation.
- b) Likelihood: the probability of some form of attack against the physical network and the data transported by it.
- c) Threat (forcible or surreptitious) analysis: for example, posed by unauthorized access to the information (data) resulting in loss or unavailability of the assets.
- d) Vulnerability analysis: for example, inadequate physical security or technical controls of the hosted data.

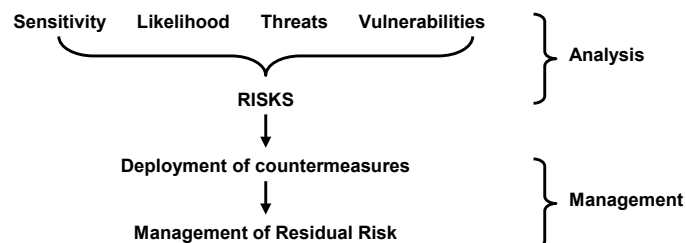


Figure 1 – Risk assessment concepts

These four items are analysed during the risk assessment process, to identify the baseline risk posed to the physical network. Management of the identified baseline risk employs appropriate technical, physical and procedural countermeasures or a combination thereof.

Following the deployment of baseline countermeasures, further decisions shall be taken relating to the residual risk(s) as follows, driven by the acceptance of risk of the asset owner.

- 1) Toleration: the remaining risk(s) are accepted and no additional countermeasures deployed.
- 2) Treatment: additional measures are deployed to counter the remaining risk(s).
- 3) Transferral: the risk(s) are transferred to another party, for example obtaining additional insurance to mitigate the risk(s).
- 4) Termination: the activity posing the risk is terminated.