



DPC: 23/30472673 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: 17 April 2023

Origin: International

Latest date for receipt of comments: 28 June 2023

Project No. 2019/03351

Responsible committee: TCT/7 Telecommunications - Installation requirements

Interested committees:

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

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of 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 28 June 2023

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/>.

E-mail: admin.start@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	Comment (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-SC25/3147/CD

COMMITTEE DRAFT (CD)

PROJECT NUMBER:
ISO/IEC 24383 ED1

DATE OF CIRCULATION:
2023-04-07

CLOSING DATE FOR COMMENTS:
2023-07-28

SUPERSEDES DOCUMENTS:
JTC1-SC25/3127/CD, JTC1-SC25/3135A/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	FOREWORD	4
3	INTRODUCTION	5
4	1 Scope	6
5	2 Normative references	6
6	3 Definitions and abbreviations	7
7	3.1 Definitions	7
8	3.2 Abbreviations	9
9	4 Conformance	10
10	5 Principles	10
11	5.1 General	10
12	5.2 Relationship with ISO/IEC 27000 series	10
13	5.3 Risk assessment concepts	10
14	5.4 Defence in depth	11
15	5.5 Network infrastructure	14
16	5.6 Controlling access	14
17	5.7 Perimeters and spaces	14
18	6 Public perimeter	18
19	6.1 General	18
20	6.2 Spaces and structures	18
21	6.3 Pathways	19
22	6.4 Infrastructure components	21
23	7 Equipment/distributor room	21
24	7.1 Spaces and structures	21
25	7.2 Pathways	25
26	7.3 Infrastructure components	25
27	8 Rack/cabinet	26
28	8.1 Spaces and structures	26
29	8.2 Pathways	28
30	8.3 Infrastructure components	29
31	9 Cabling component containment	32
32	9.1 Spaces and structures	33
33	9.2 Pathways	33
34	9.3 Infrastructure components	44
35	10 Cabling component	45
36	10.1 Spaces and structures	45
37	10.2 Pathways	46
38	10.3 Infrastructure components	47
39	11 Administration	50
40	11.1 Reporting of cyber security incidents	50
41	11.2 Labelling	50
42	11.3 Documentation	51
43	11.4 Cable auditing	51
44	11.5 Monitor the system	51
45	11.6 Security documentation	51

46	11.7	Security assessment report.....	52
47	11.8	Training.....	53
48	11.9	Security clearances	53
49	11.10	Access requirements	53
50	12	Evolution of security systems	53
51	Annex A (normative)	Video surveillance	54
52	A.1	Requirements	54
53	A.2	Recommendations	54
54	Annex B (normative)	Intrusion detection.....	56
55	B.1	Requirements	56
56	Annex C (normative)	Access control	58
57	C.1	Requirements	58
58	C.2	Recommendations	59
59	Annex D (normative)	Implementation	60
60	Bibliography.....		61

61

62

63

64 List of figures

65	Figure 1 – Risk assessment concepts	11
66	Figure 2 – Defence in depth model	12
67	Figure 3 – Area and room relationship – solution one	15
68	Figure 4 – Area and room relationship – solution two	17
69	Figure 5 – Area and room relationship – solution three	18
70	Figure 8 – Security requirements for an ‘open’ equipment/distributor room.....	22
71	Figure 13 – Example of various classifications of pathway between equipment racks	31
72	Figure 14 – Optical fibre security conduit application	34
73	Figure 15 – Examples of access pit security configuration	41

74

75 List of tables

76	Table 1 – Equipment room classification and minimum area classification.....	13
77	Table 3 – Minimum acceptable classification combinations for cables for pathway	
78	systems	34
79	Table 4 – Classification security seal minimum requirements.....	43
80	Table 5 – Example of classification cable and outlet box colours.....	47

81

82

83

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

FOREWORD

- 1) ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.
 - 2) 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 National Committees and ISO member bodies.
 - 3) IEC, ISO and ISO/IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees 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.
 - 4) In order to promote international uniformity, IEC National Committees 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 or ISO/IEC publication and the corresponding national or regional publication should be clearly indicated in the latter.
 - 5) ISO and IEC do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. ISO or IEC are not responsible for any services carried out by independent certification bodies.
 - 6) All users should ensure that they have the latest edition of this publication.
 - 7) 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 National Committees 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.
 - 8) 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.
 - 9) Attention is drawn to the possibility that some of the elements of this ISO/IEC Publication 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 can 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.

INTRODUCTION

ISO/IEC 14763-2 specifies requirements and recommendations for the installation specification, quality assurance and installation practices for customer premises cabling in accordance with the ISO/IEC 11801 series.

Those requirements provide a basic level of physical network security for the cabling and associated infrastructure.

This document builds upon the basic requirements of ISO/IEC 14763-2 by adding additional requirements to facilitate timely and effective protection of the customer premises cabling infrastructure to avoid loss/damage to the physical information transport network and therefore supports the protection of the transmitted information.

This document provides comprehensive design, planning and installation requirements for improving physical network security.

The requirements and recommendations can be applied to existing buildings and also during building construction, or renovation, when actions are significantly less expensive and less disruptive than after the building is occupied.

This document incorporates the use of automated infrastructure management (AIM) systems, including those in accordance with ISO/IEC 18598, to further enhance the security of cabling infrastructure and integrate the physical network security with other security systems in the premises.

Editor's note: Some requirements for AIM have been lost in the restructure of the document, please resubmit comments for the appropriate parts of the document and to the related sensitivity level.

This document is intended to be used by

- architects, building owners, building designers and builders,
- consultants,
- facility managers and network managers,
- designers, suppliers, installers, inspectors (auditors), maintainers and owners of telecommunications cabling.

When using this standard, it shall be considered relevant specifications from ISO/IEC 27000 series.

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 unauthorized access.

The document addresses

- a) risk assessment guidelines,
- b) design, planning and installation practices based on a required information sensitivity level,
- c) intrusion detection,
- d) administration including Automated Infrastructure Management (AIM).

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

The following are outside the scope of this document:

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

2 Normative 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.

IEC 60839 *Alarm and electronic security systems*

IEC 60839-11-1 *Alarm and electronic security systems - Part 11-1: Electronic access control systems - System and components requirements*

IEC 62676-1-1:2013, *Video surveillance systems for use in security applications – Part 1-1: System requirements – General*

ISO/IEC 14763-2, *Information technology - Implementation and operation of customer premises cabling - Part 2: Planning and installation*

ISO/IEC 27000 *Information security management systems*

3 Definitions and abbreviations

3.1 Definitions

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

3.1.1

access control system

system that provides selective restriction of access to a space or cabling component

3.1.2

administration

methodology defining the documentation requirements of a cabling system and its containment, the labelling of functional elements and the process by which moves, additions and changes are recorded [SOURCE: ISO/IEC 11801-1:2017, 3.1.1]

3.1.3

AIM system

integrated hardware and software system that automatically detects the insertion or removal of cords, documents the cabling infrastructure including connected equipment enabling management of the infrastructure and data exchange with other systems [SOURCE: ISO/IEC 18598:2016, 3.1.3]

3.1.4

alarmed carrier

system for detecting intrusion into a pathway using optical fibre as a vibration sensor

3.1.5

alarm-enabled

capable of triggering an alarm with the intrusion alarm system

3.1.6

authorized personnel

persons able to access a space or pathway of a defined Security Grade

3.1.7

cabling

system of telecommunications cables, cords and connecting hardware that supports the connection of information technology equipment [SOURCE: ISO/IEC 11801-1:2017, 3.1.21]

3.1.8

common distribution space

primary or secondary building distribution space

3.1.9

countermeasure

step taken to prevent a threat triggering a security event

3.1.10

dialler unit

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

3.1.11

door hardware

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

3.1.12

electronic locking mechanism

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

- 241 **3.1.13**
 242 **effective height of a free-standing barrier**
 243 shortest distance between any point on the top of the permanent part of the free-standing barrier
 244 (excluding any toppings) and the surface of the supporting ground when measured in the plane of the
 245 barrier
- 246 **3.1.14**
 247 **external boundary**
 248 physical barrier(s) demarcating a space or structure of a given Security Grade (SG)
 249 Note 1 to entry: Access floors and suspended ceilings through which unauthorised access to a space can be gained are not
 250 considered to be external boundaries. In such cases, the fixed building fabric upon which these structures are built is the external
 251 boundary.
- 252 **3.1.15**
 253 **external telecommunications cabinet**
 254 outdoor enclosure accommodating telecommunications equipment and associated cabling
- 255 **3.1.16**
 256 **free-standing barrier**
 257 wall, fence, gate, turnstile or other similar self-supporting barrier, and its associated foundations,
 258 designed to prevent entry to a space of a given Security Grade
- 259 **3.1.17**
 260 **inspectable**
 261 able to be easily observed for tampering or damage without tools other than a light
- 262 **3.1.18**
 263 **inspectable area**
 264 vertical and horizontal area from the outside of a sensitive facility in which a threat can be
 265 identified and removed
- 266 **3.1.19**
 267 **intelligent building system**
 268 equipment and telecommunication infrastructure that supports monitoring, control, operation and
 269 management of building services
- 270 **3.1.20**
 271 **keypad**
 272 manual input devices, typically requiring telecommunications connectivity, that allow individuals to enter
 273 specific codes to arm, disarm or diagnose intrusion systems
- 274 **3.1.21**
 275 **joint closures**
 276 sealed housing protecting the joining or splicing of the conductors and optical fibres of
 277 telecommunications cables
- 278 **3.1.22**
 279 **junction box**
 280 protective housing and associated space that enables cables to be routed between pathway systems
- 281 **3.1.23**
 282 **mechanical locking mechanism**
 283 device that allows access by means of physically coded key or tool
- 284 **3.1.24**
 285 **protected pathway system**
 286 conduit, hardened raceway, hardened optical fibre cable, and other means of physically
 287 restricting the access to telecommunications cables
- 288 **3.1.25**
 289 **security event**
 290 vulnerability that has been exploited by a threat

3.1.26**surveillance system**

devices and mechanisms used to monitor and detect behaviour or activity to protect the physical network

3.1.27**tamper evident**

designed or enabled to show access or attempts to access

3.1.28**terminal equipment**

equipment at an outlet used to access information provided by transmission equipment

[SOURCE: ISO/IEC 11801-1:2017, 3.1.81]

3.1.29**terminal equipment outlet**

fixed connecting device which provides an interface to the terminal equipment

[SOURCE: ISO/IEC 11801-1:2017, 3.1.80, modified - Note 1 to entry deleted]

3.1.30**threat**

method by which a vulnerability can be exploited to create a security event

3.1.31**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

3.1.32**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]

3.1.33**uninspectable area**

vertical and horizontal area from the outside of a sensitive facility in which a threat cannot be identified and removed

3.1.34**volumetric detector**

intrusion sensor used to detect an unauthorized person in a confined space when the space is normally unoccupied

Note 1 to entry: Examples are ultrasonic, microwave and infrared sensors.

3.1.35**vulnerability**

weakness that can be potentially exploited by a threat

3.2 Abbreviations

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

CMS cable management system

PPS protected pathway system

SG Security Grade

SL Security level

4 Conformance

For the physical network security of a telecommunications cabling infrastructure to conform to this document it shall conform to the selected level determined by the risk assessment.

- a) Open: As a minimum, to the specification, planning and installation requirements of ISO/IEC 14763-2 shall be met. This provides a basic level of physical network security and addresses the minimum information sensitivity level denominated.
- b) Restricted: All requirements for level Open and the requirements for Restricted in Clause 6, 7, 8, 9, 10 and 11 shall be met.
- c) Secure: All requirements for level Restricted and the requirements for Secure in Clause 6, 7, 8, 9, 10 and 11 shall be met.
- d) Highly secure: All requirements for level Secure and the requirements for Highly Secure in Clause 6, 7, 8, 9, 10 and 11 shall be met.

5 Principles

5.1 General

A cyber security strategy sets out an organization's guiding principles, objectives and priorities for cyber security and shall also cover an organization's threat environment, cyber security initiatives (an action plan), or investments the organization plans to make as part of its cyber security program.

Without a cyber security strategy, organizations risk failing to adequately plan for and manage security and business risks within their organization.

Organizations can protect their systems and information from cyber threats. These security principles are grouped into five key activities:

- a) **Identify:** Identify security risks.
- b) **Protect:** Implement methods to reduce security risks.
- c) **Detect:** Detect security breaches and incidents.
- d) **Respond:** Take action regarding a detected incident.
- e) **Recover:** Restore any capabilities or services that were impaired due to an incident.

This document provides requirements and recommendations to protect and enhance the security, resiliency, and reliability of the organization's communications infrastructure.

Organizations may to follow regulations that determine information classification and protection.

5.2 Relationship with ISO/IEC 27000 series

The ISO/IEC 27000 series is a series of 46 individual standards that assist organizations improving their cyber information security; ISMS (information security management system). The ISMS is a systematic approach to risk management, containing measures that address the three pillars of information security: people, processes and technology.

ISO/IEC 24383 provides direction on security controls and treatments around information technology cabling, pathways and spaces for customer premises. These measures are not discussed in ISO/IEC 27000 series. ISO/IEC 24383 has been prepared so that it dovetails into ISMS, addressing cyber infrastructure security, to provide organizations with a complete, effective end-to-end cyber security implementation.

5.3 Risk assessment concepts

5.3.1 General

ISO/IEC 24383 does not address risk assessment techniques or any form of analysis. The organization is responsible to determine the cyber security risks that it faces.

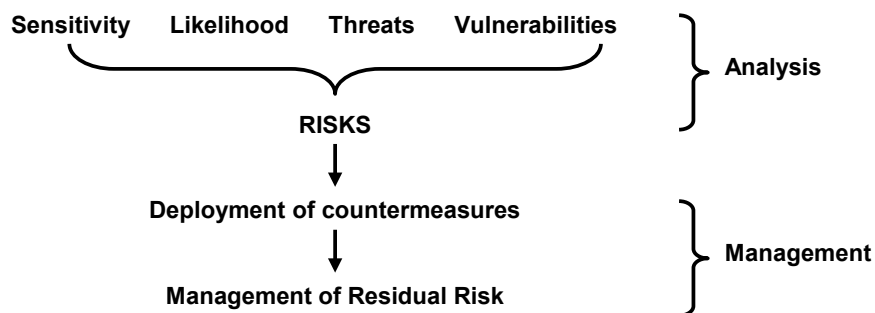


Figure 1 – Risk assessment concepts

This document defines four levels of information sensitivity, and the controls and treatments for those defined sensitivity levels.

The organization can determine that they require additional classifications of information sensitivity levels. These additional levels will not impact on the controls or treatments defined in this document. The organization can expand on the treatments and controls discussed in this standard.

5.3.2 Information sensitivity levels

The sensitivity of the data determines the needed security level to protect the data.

5.4 Defence in depth

5.4.1 General

Defence in depth is a strategy used in Information (cyber) security in which multiple layers of security controls are layered in order to protect valuable data and information. ISO/IEC 24383 would form part of a larger ISMS (ISO/IEC 27000 series) cyber security defence in depth strategy.

ISO/IEC 24383 takes a systematic approach when applying security treatments and control to information technology cabling, pathways and spaces for customer premises. The defence in depth is a strategy undertaken is as follows:

- e) Public perimeter,
- f) Organizational perimeter,

Editor's note: Please consider to submit comments for the requirements/recommendations for Organizational perimeter.

- g) Equipment/distributor room,
- h) Rack/cabinet,
- i) Cabling component containment,
- j) Cabling component.

The application of defence-in-depth for the protection of IT cabling systems and the cyber information moving across the IT cabling, is enhanced using successive layers of physical security. All layers are designed to limit access to people without the appropriate authorisation to access systems at a facility.

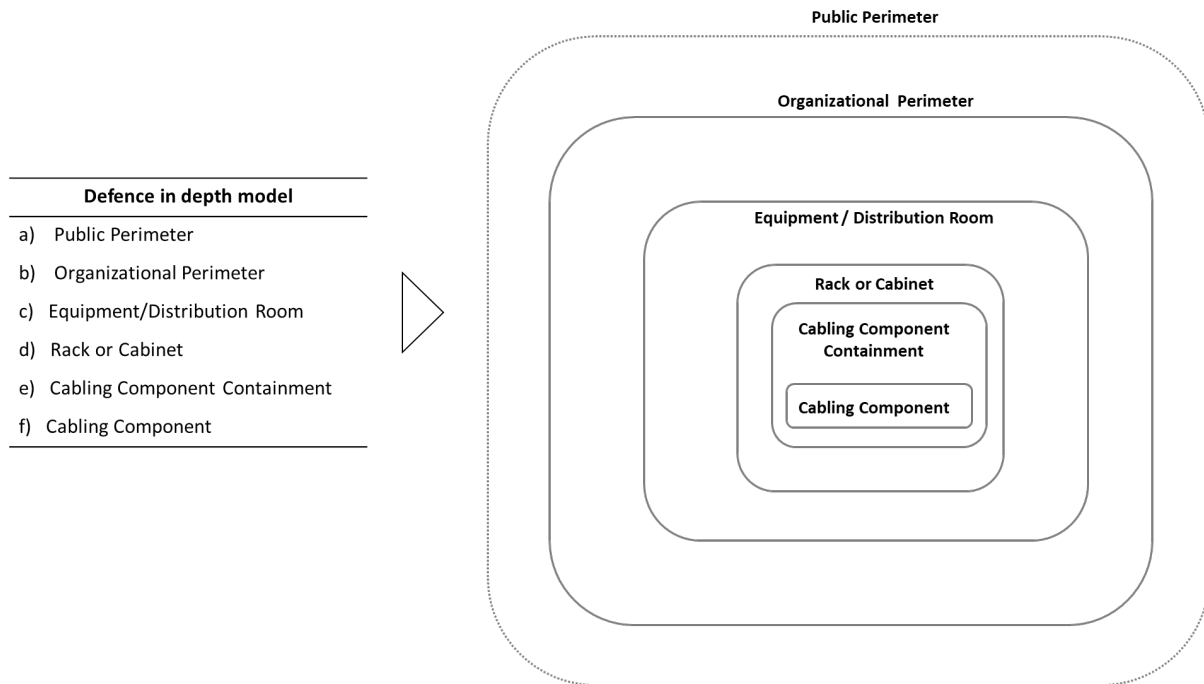


Figure 2 – Defence in depth model

5.4.2 Public perimeter

The first layer in the protection of information technology cabling, pathways and spaces is the line demarcating the boundary between the public accessible areas and the organizational side. These various classified areas can be:

- Open,
- Restricted,
- Secure,
- Highly secure.

The line demarcating the extent between the public accessible areas and the organizational side is often a physical barrier (visible or non-visible). This physical barrier is dependent on the organization and the facility. This demarcation could be:

- Buried sensing cables and motion detectors around the site.
- A security rated fence and commensurately rated portals around the site.
- Access control doors (mechanical or electronic) from a public foyer or waiting area.
- Access control doors (mechanical or electronic) from a public open area (e.g. parks, gardens, and the like).

Access points within the demarcation line provides a means of organization personnel (people or vehicles) on entering/exiting between public area and the organization area.

5.4.3 Organizational perimeter

The second layer in the protection of information technology cabling, pathways and spaces is the line demarcation between the internal boundary between the various classified areas within the organization facility. These various classified areas can be:

- Open,
- Restricted,

c) Secure,

d) Highly secure.

Only the (cyber) information of that classification or lower, can be created, disclosed, altered or destroyed in that classification of area.

As an example, Restricted Network (RN) telecommunications outlets and workstations can appear in the Restricted Area (RA) and in the Secure Area (SA). Secure Area (SA) telecommunications outlets and workstations are prohibited to appear in either the Restricted Area (RA) or the Open Area (OA).

It is feasible for an organization to have two separate Restricted networks, each one existing solely and independently within a restricted area. As an example, Restricted Network 1 (RN1) can only have telecommunications outlets and workstations in Restricted Area 1 (RA1); likewise, Restricted Network 2 (RN2) telecommunications outlets and workstations can only appear Restricted Area 2 (RA2) and are prohibited in Restricted Area 1 (RA1), and vice versa.

Editor's note: Please consider to submit comments for the requirements/recommendations for Organizational perimeter.

5.4.4 Equipment/distributor room

The third layer in the protection of information technology cabling, pathways and spaces systems is the equipment rooms and distributor rooms. Within ISO/IEC 24383 all these rooms and spaces will be referred as the Equipment/distributor room (ER).

The security treatments and access for the equipment room housing the various classified (open, restricted, secure, highly secure) network cabling and/or equipment will differ.

The equipment room shall be classified to the highest level of the network rack/cabinet present in the room. There is a solution for the facility that houses a HSER, without a secure area. This is not recommended and is the only solution of existing facilities, with limited capability to be upgraded only.

After the equipment room has been classified, the equipment room shall be located in an area that is at a maximum of one classification level less than the equipment room. Where equipment rooms are placed in an area that is at a lower classification than the equipment room, additional security treatments shall be applied.

Table 1 – Equipment room classification and minimum area classification

Network rack/cabinet present	Equipment room classification	Minimum area classification
Open network (ON)	Open ER (OER)	Open area (public space)
Restricted network (RN)	Restricted ER (RER)	Open area (organization space)
Secure network (SN)	Secure ER (SER)	Restricted area
Highly secure network (HSN)	Highly secure ER (HSER)	Restricted Area (Secure area recommended)

5.4.5 Rack/cabinet

The fourth layer in the protection of information technology cabling, pathways and spaces systems is the equipment rack/cabinet.

The equipment rack shall be classified to the highest level of the (classified) network present in the rack/cabinet.

The security treatments and access for the equipment racks/cabinets that are classified either open, restricted, secure, highly secure will differ.

5.4.6 Cabling component containment

The fifth layer in the protection of information technology cabling, pathways and spaces systems is cabling component containment.

The cabling containment and the associated security treatments and controls shall match the classification of the network (information technology) cabling within.

5.4.7 Cabling component

The sixth layer in the protection of information technology cabling, pathways and spaces systems is the cabling component (cable, cord or connecting hardware).

The security treatments and controls for the cable, cords and outlets and the like shall match the classification of the network (information technology) information that is being transported over the cabling component.

5.5 Network infrastructure

While physical security can provide a degree of protection to information communicated over network infrastructure. It is recommended that all the network and cabling infrastructure be located in the areas authorised for the processing of such information.

5.6 Controlling access

Physical security controls are implemented to protect network devices and cabling, especially those in public areas, from physical damage or unauthorised access.

Risk assessed physical protection shall be provided for all network devices and cabling, especially those in public areas, to prevent an adversary physically damaging a network device with the intention of interrupting services. The physical protection shall be fit for the intended purpose.

Physical access to network devices can allow an adversary to reset devices to factory default settings by pressing a physical reset button, connecting a serial interface to a device or connecting directly to a device to bypass any access controls.

Resetting a network device to factory default settings can:

- a) Disable security settings including authentication and encryption functions.
- b) Reset administrator accounts and passwords to known defaults.
- c) If access to a network device is not gained, a likely denial of service attack could occur.

Physical access can be restricted through methods such as:

- 1) Physical enclosures that prevent access to console ports and factory reset buttons.
- 2) Mounting devices on ceilings or behind walls.
- 3) Placing devices in locked rooms or cabinets.
- 4) Physical access to cabling should be minimized to avoid threats.

5.7 Perimeters and spaces

5.7.1 General

This clause discusses the relationship between areas of various classifications, and equipment rooms of various classifications. This clause outlines the requirements and recommendations

for perimeter security and access control at the demarcation line between the internal boundary between the various classified areas within the organization facility.

5.7.2 Area and room relationships

5.7.2.1 General

The location of the various classified areas and equipment rooms will differ from organization to organization. Even within an organization, the purpose and layout of facilities will differ.

Figure 3, Figure 4 and Figure 5 do not encompass all cyber infrastructure classification installation solutions. Their purpose is to demonstrate the relationship and logic on the placement of:

- a) Areas of various classification that house telecommunications outlets and workstations.
- b) Placement of equipment rooms of various classifications.

5.7.2.2 Example: solution one

In this example there are four separate classified areas: open, restricted, secure and highly secure. The information technology security philosophy behind the example in Figure 3 is as follows:

An open area contains only open elements. A restricted area may contain both open and restricted elements. Each security level may not contain higher secure elements, but it may contain less secure elements.

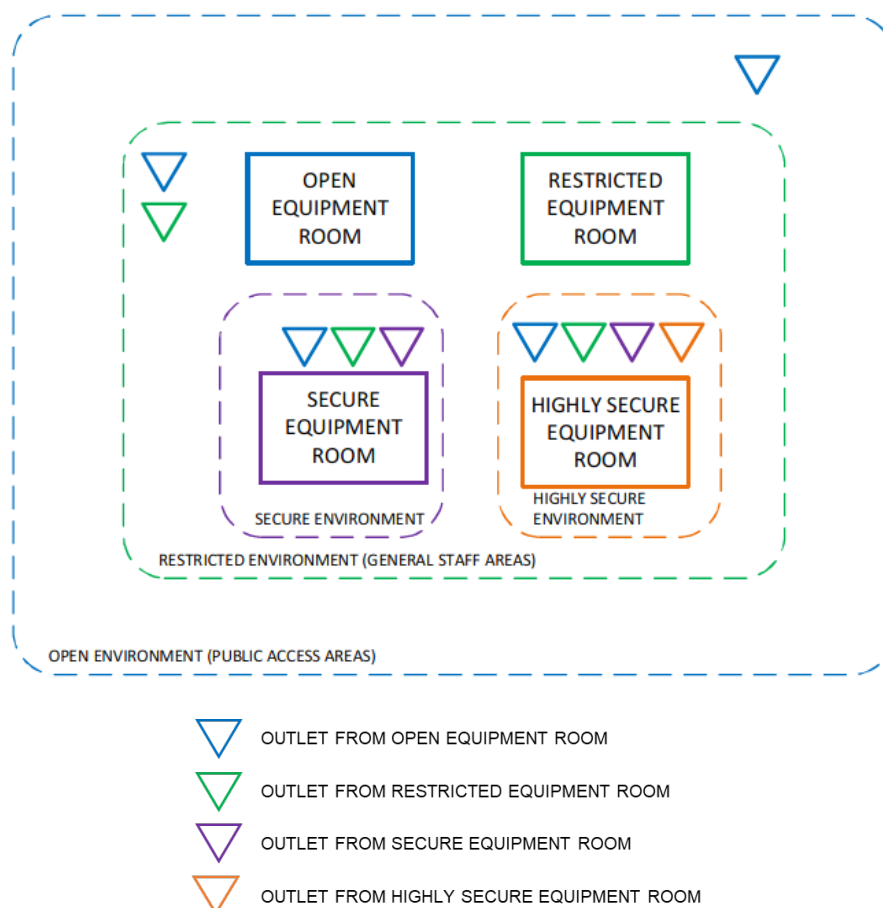


Figure 3 – Area and room relationship – solution one

In the example (Figure 3) where open is operating in a higher classification domain (Restricted), appropriate measures must be in place to ensure information flow is in one direction only, from open to restricted, not vice versa. Or, although open is in the restricted area, there is no

information exchange between the different domains. Open will be subject to the physical and other security controls that the restricted environment is operating under in this example.

5.7.2.3 Example: solution two

In this example there are four separate classified areas; open, restricted, secure and highly secure. The information technology security philosophy behind the example in Figure 4 is as follows:

- a) In the open area “Open network (ON)” telecommunications outlets and workstations are located. In this situation, the organizational “Open ER (OER)” is directly accessible from a public space. This OER will require additional security treatments and controls equivalent to a Restricted ER (RER). Due to the location “Restricted network (RN)”, “Secure network (SN)” and “Highly secure network (HSN)” racks/cubicles are prohibited.

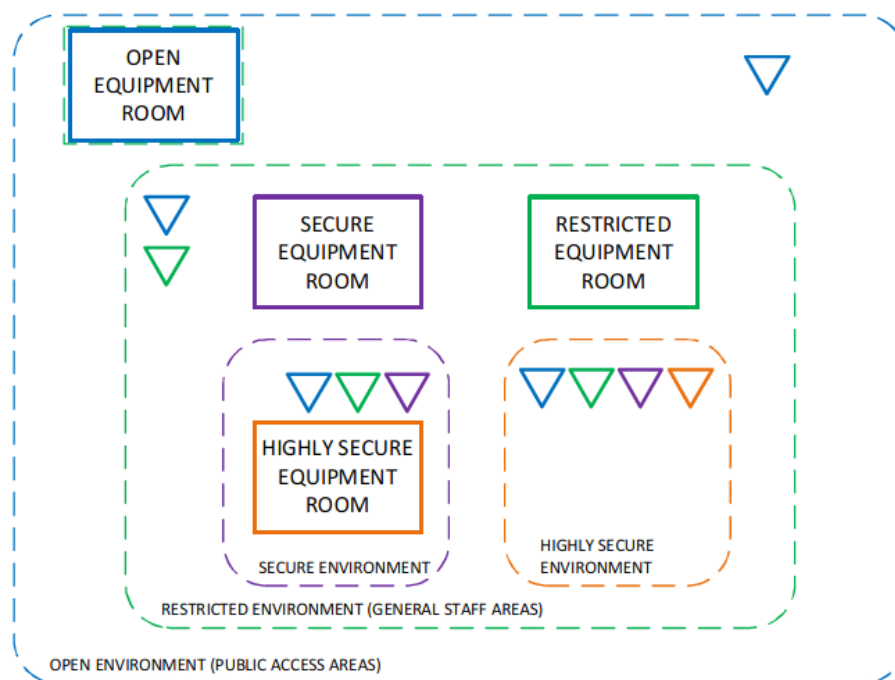
NOTE: In this situation, a Restricted area was built around the OER.

- b) In the restricted area, “Open network (ON)” and “Restricted network (RN)” telecommunications outlets and workstations are located. There are two separate equipment room; a Restricted ER (RER) and a Secure ER (SER). The Secure ER needs additional treatments.

Editor’s note: Please consider to submit comments on additional treatments to the Secure ER and other ERs specified in this document.

- c) In the secure area, “Open network (ON)”, “Restricted network (RN)” and “Secure network (SN)” telecommunications outlets and workstations are located. There is one separate equipment room; Highly secure ER (HSER). The Highly Secure ER needs additional treatments.

- d) In the highly secure area, “Open network (ON)”, “Restricted network (RN)”, “Secure network (SN)” and “Highly secure network (HSN)” telecommunications outlets and workstations are located.



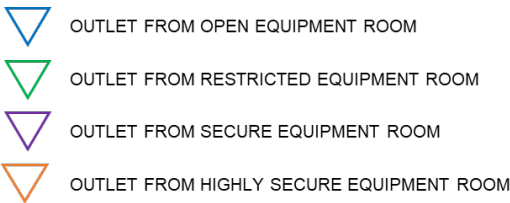


Figure 4 – Area and room relationship – solution two

5.7.2.4 Example: solution three

In this example there are four separate classified areas; open, restricted, secure and highly secure. The information technology security philosophy behind the example in Figure 5 is as follows:

- a) In the open area “Open network (ON)” telecommunications outlets and workstations are located. In this situation, the organizational “Open ER (OER)” is directly accessible from a public space. This OER will require additional security treatments and controls equivalent to a Restricted ER (RER). Due to the location “Restricted network (RN)”, “Secure network (SN)” and “Highly secure network (HSN)” racks/cubicles are prohibited.

NOTE: In this situation, a Restricted area was built around the OER.

- b) In the restricted area, “Open network (ON)” and “Restricted network (RN)” telecommunications outlets and workstations are located. Due to constraints, there are three separate equipment rooms; a Restricted ER (RER), a Secure ER (SER) and a Highly secure ER (HSER). The SER and HSER will require additional security treatments and controls equivalent to a Secure ER (SER) – in essence, a secure area is being built around the HSER to bring it into line with the recommendations of Table 1. This is absolutely the lowest classified area that a HSER shall be found.
- c) In the secure area, “Open network (ON)”, “Restricted network (RN)” and “Secure network (SN)” telecommunications outlets and workstations are located.
- d) In the highly secure area, “Open network (ON)”, “Restricted network (RN)”, “Secure network (SN)” and “Highly secure network (HSN)” telecommunications outlets and workstations are located.

