



ISO/IEC JTC 1/SC 27 **N 7791**

ISO/IEC JTC 1/SC 27/WG 3 **N 991**

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC. TYPE: dispositions of comments

TITLE: Dispositions of comments on ISO/IEC 1st PDTR 19791 (SC 27 N 7386) Information technology – Security techniques – Security assessment of operational systems

SOURCE: 38th SC 27/WG 3 meeting

DATE: 2009-05-06

PROJECT: 19791

STATUS: Output document of the editing session for 1st PDTR 19791 (SC 27 N 7386) held during the 38th SC 27/WG 3 meeting Beijing, China, 4th – 8th May 2009.

This document was available at the above-mentioned meeting. It is being circulated for information.

ACTION: FYI

DUE DATE:

DISTRIBUTION: P-, O-, and L- Members
W. Fumy, SC 27 Chairman, M. De Soete, SC 27 Vice Chair
E. Humphreys, K. Naemura, M. Ohlin, M.C. Kang, K. Rannenbergl, WG-Conveners

MEDIUM: Server

NO. OF PAGES: 1 + 3

NB Comments on ISO/IEC PDTR 19791 (revision)

Source Date: 2008-12-31	Source Document: SC 27 N7264
-------------------------	-------------------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
AU 1	ALL		Ed	AU has not been able to undertake a comprehensive review of this PDTR and offers the comments below to accompany an ABSTAIN vote.		Noted.
AU 2	3		Ed	A number of terms are duplicated and defined both within this document and ISO/IEC 27000 (see comments below).	Greater consistency, alignment and tighter integration among the Information technology – Security techniques documents should be studied.	Noted, but this is a supporting document to ISO/IEC 15408/18045. Where there are differences between ISO/IEC 15408/18045 and ISO/IEC 27000, the definitions from the former must be used.
AU 3	3		Ed	A large number of the terms defined within ISO/IEC 27000 were found to be used within this document. Annex A provides a summary of the extent of term usage. Making a definition of the respective terms available to the reader of this document would enhance the reader's understanding of the document content.	Insert the following reference to allow the reader to be able to access a definition for each of these undefined terms: “For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.”	Not accepted. There is already an external terms and definitions reference in the TR to ISO/IEC 15408 and 18045, and most of your allegedly undefined technical terms are defined there! We will make a check that none of your Annex A terms used in a technical sense are not defined either here or in 15408/18045.
AU 4	3.7 – Risk		Te	The existing definition differs significantly to the definition currently provided in ISO/IEC 27000 and is expected to differ from the revised publication of ISO Guide 73.	Revise this definition to be aligned with the definition proposed in ISO Guide 73 to be published in 2009.	Not accepted. We use the definition from ISO/IEC 27005 (with source acknowledgment), which is a recent and relevant published document. It cannot yet be guaranteed that your proposed definition will be accepted.
AU 5	3.8 – Risk Analysis		Ed	This term is identically duplicated as being defined both within this document and ISO/IEC 27000. It is suggested that greater consistency, alignment and tight integration among the Information technology – Security techniques documents would be beneficial to the reader.	Either remove identically duplicated terms and insert the following reference: “For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.” Or insert a normative cross-reference to ISO/IEC 27000 against each of the	Not accepted. We reference ISO/IEC Guide 73:2002 as the source, which is that referenced by the current 27000 FDIS! This TR is not part of the 270xx set of standards and should reference the primary source.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

NB Comments on ISO/IEC PDTR 19791 (revision)

Source Date: 2008-12-31	Source Document: SC 27 N7264
-------------------------	-------------------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
					duplicated terms.	
AU 6	3.9 – Risk Avoidance		Ed	This term is identically duplicated as being defined both within this document and ISO/IEC 27000. It is suggested that greater consistency, alignment and tight integration among the Information technology – Security techniques documents would be beneficial to the reader.	Either remove identically duplicated terms and insert the following reference: “For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.” Or insert a normative cross-reference to ISO/IEC 27000 against each of the duplicated terms.	Not accepted. We do not define “risk avoidance”, definition 3.9 is for “risk assessment” where we use the published definition from ISO/IEC Guide 73:2002. The term “risk avoidance” is only used once, in a general sense (and isn’t defined in 27000).
AU 7	3.10 – Risk Management		Ed	This term is identically duplicated as being defined both within this document and ISO/IEC 27000. It is suggested that greater consistency, alignment and tight integration among the Information technology – Security techniques documents would be beneficial to the reader.	Either remove identically duplicated terms and insert the following reference: “For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.” Or insert a normative cross-reference to ISO/IEC 27000 against each of the duplicated terms.	Not accepted. We reference ISO/IEC Guide 73:2002 as the source, which is that referenced by the current 27000 FDIS! This TR is not part of the 270xx set of standards and should reference the primary source.
AU 8	3.11 – Risk Treatment		Te	The existing definition uses the concept of "options" v. "measures" that is used within the same definition within ISO/IEC 27000.	Revise this definition to be aligned with the definition used in ISO/IEC 27000.	Not accepted. We use the same concepts because we use the same definition from ISO/IEC Guide 73:2002, as used by the current 27000 FDIS! This TR is not part of the 270xx set of standards and should reference the primary source.
AU 9	3.18 – Vulnerability		Te	This is an overly complex definition that is not easily substituted into the text were the term is used. The existing definition also differs significantly to the definition currently provided in ISO/IEC 27000.	Revise this definition to be aligned with the definition used in ISO/IEC 27000.	Accepted in part. We will use the definition from FDIS ISO/IEC 15408-1, 3.5.7 – please note that “vulnerability” is not defined in the published 2005 edition of 15408-1.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

NB Comments on ISO/IEC PDTR 19791 (revision)

Source Date: 2008-12-31	Source Document: SC 27 N7264
-------------------------	-------------------------------------

1	2	(3)	4	5	(6)	(7)
NB¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
AU 10	4 – ISMS Information Security Management System		Ed	ISMS Information Security Management System is defined as an abbreviated term but this term is not used within the text of the document.	Delete the inclusion of this abbreviated term.	Accepted.
CA 1	ALL	-	Ge	Canada requests that SC27 clarify if the intent of the PDTR is convert this work into a International Standard?	Canada will vote in support regardless.	It is intended to publish this revision as a Technical Report, since major new Annex D (methodology) is untested in practice.
NL 1	ALL	-	Ge	No need for this standard.	-	Noted. However, of 28 National Bodies voting, the Dutch NB was the only one to disapprove this draft, and there were 17 approval votes. It therefore seems that there is substantial support for republishing this Technical Report. We will therefore proceed to DTR ballot as planned.

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.