



ISO/IEC JTC 1/SC 27 **N 8123**

ISO/IEC JTC 1/SC 27/WG 3 **N 38123**

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 DTR 19791 (SC 27 N 7860)  
Information technology – Security techniques – Security assessment  
of operational systems

**SOURCE:** Project Editor

**DATE:** 2009-11-03

**PROJECT:** 1.27.41

**STATUS:** This document was made available at the 39<sup>th</sup> SC 27/WG 3 meeting  
Redmond, US, 2nd – 6th November 2009.  
  
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. Bañón, M.C. Kang, K. Rannenber, K. Rannenber,  
WG-Conveners

**MEDIUM:** Server

**NO. OF PAGES:** 1 + 3

Template for comments and secretariat observations

Date: 2009-09-09	<b>ISO/IEC JTC 1 N9592</b> DTR 19791, Security techniques – Security assessment of operational systems
------------------	---

1	2	(3)	4	5	(6)	(7)
MB <sup>1</sup>	Clause No./ Subclause No./ Annex (e.g. 3.1)	Line No.	Type of comment <sup>2</sup>	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted

LU-1	6.2	3 <sup>rd</sup> last	Te	Accreditation has a different meaning in ISO27006	Use another term, e.g. certification	Not accepted. Accreditation is used in this document in a manner consistent with ISO/IEC 15408 (see terms and definitions) and 6.2's final paragraph already makes it clear that the model being described here is an extension to the ISO/IEC 15408 model.
LU-2	Page 6	8 <sup>th</sup> last line	Ed	The standard should be well linked to other ISO standards.	Also refer to the future ISO 31010 for risk assessment	Not accepted. Given that we are saying that risk assessment is out of scope of this TR, one reference (to ISO/IEC 27005) is considered adequate.
LU-3	6.3.1, .p.7	all	Ed	There is a lot of information, which make the standards valuable, but it makes it hard to get an overview.	Add a figure to illustrate the 4 phase and to summarize the main activities in each phase	Accepted. A new figure has been added.
LU-4	7.3, p.13	Point d)	Te	Clarify how this verification is done typically. We think that it is not enough to assess that the system is running correctly at a given point of time.	Unclear whether this may include or mandate hacking the system, or simulating an activity of the identified threats.	Not accepted. Examination of the referenced ASO class will show that this is done by examination of audit records only. "Hacking" and other operational testing falls under AOT and thus is part of activity (b).

**Template for comments and secretariat observations**

Date: 2009-09-09	<b>ISO/IEC JTC 1 N9592</b> DTR 19791, Security techniques – Security assessment of operational systems
------------------	---

1	2	(3)	4	5	(6)	(7)
MB <sup>1</sup>	Clause No./ Subclause No./ Annex (e.g. 3.1)	Line No.	Type of comment <sup>2</sup>	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted

SG-1	7.4 Composite operational systems	page 14,5 <sup>th</sup> paragraph	ed	Original: “However, a component as defined in this Technical Report has a wider scope than a ISO/IEC 15408 module”	...than a ISO/IEC 15408 module”	Accepted and implemented.
SG-2	7.4 Composite operational systems	page 16, last para	ed	Original “The interface specifications need to cover any security requirements for the interface or for the communications links”	..communication links”	Accepted and implemented.
SG-3	All		ge	J1N9593 uses sometimes the term “unevaluated” and sometimes “non-evaluated”. (e.g. Section 7.5, “may equally well be unevaluated. For non-evaluated products”). It is not clear if and what difference exists.	It is suggested to use one term only or clarify the meaning and difference of both in the glossary	Accepted and implemented. The term “unevaluated” is now used throughout.
SG-4	7.6 Types of security controls		ed	Original: “(since they are purely relate to management).”	“... related to management).”	Accepted. Changed to “since they purely relate to management.”
SG-5	All		ge	J1N9593 uses sometimes the term “operational system evaluation” and sometimes “operational systems evaluation”. It is suggested to use one term only.	Use "operational system evaluation" without using the plural in the word 'system'	Accepted and implemented.
SG-6	All		te	Since version 3.1 (and also in the new release for ISO 15408) there is thye concept of 'composition' within CC. This seems relevant especially to the integration aspect of components being addressed by J1N9593, but is not addressed anywhere. It would be good to contrast this scope with CAP, and also to elaborate how CAP would/could be used to define the critical aspect of product interaction.		The concept of domain assurance used within this TR provides an alternative method for composition of assurance where the environment is fixed and limited evaluation results are available. So this is already

**Template for comments and secretariat observations**

Date: 2009-09-09	<b>ISO/IEC JTC 1 N9592</b> DTR 19791, Security techniques – Security assessment of operational systems
------------------	---

1	2	(3)	4	5	(6)	(7)
MB <sup>1</sup>	Clause No./ Subclause No./ Annex (e.g. 3.1)	Line No.	Type of comment <sup>2</sup>	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
						covered. See subclause 7.5. Product interaction is out of scope of this document (and already dealt with in 15408/CC).
SG-7	All		te	J1N9593 uses SST for 'System Security Target'. CC has a supporting document on site certification, where SST is used for 'Site Security Target'. This may cause misunderstandings, especially due to the close link to CC. If SST cannot be changed anymore, it would be good to at least make a note on the different scopes.		Accepted and implemented. A note has been added to subclause 9.7.