



ISO/IEC JTC 1/SC 27 **N 7797**

ISO/IEC JTC 1/SC 27/WG 3 **N 997**

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 N7393 Summary of voting on document SC 27 N7268 rev1 -- Proposal for a New Work Item on Secure system engineering principles and techniques (NP 29193)

**SOURCE:** 38<sup>th</sup> SC 27/WG 3 meeting

**DATE:** 2009-05-07

**PROJECT:** 29193

**STATUS:** Output document of the editing session for ISO/IEC 29193 pre-WD held during the 38<sup>th</sup> SC 27/WG 3 meeting Beijing, China, May 2-8, 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. Rannenber, WG-Conveners

**MEDIUM:** Server

**NO. OF PAGES:** 1 + 4

1	2	(3)	4	5	(6)	(7)
NB <sup>1</sup>	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
SI1	NWIP N7393	comments	ge	The title does not seem to correctly reflect the content so far: 'Secure System Engineering principles and techniques' is a broader term and for me implies all implementation aspects, but the whole document (esp. 11. Summary) talks about the 'design' only. Therefore 'Secure System Design principles and techniques' could be suggested as new title to clarify the scope.		Accepted. The editor will amend the title accordingly and thanks the Singapore NB for the valuable comment.
SI2	NWIP N7393	comments	ge	It is a worthwhile effort to manage the design first in one report. The actual implementation (aka engineering, testing, and validation of the system) would call for a separate technical report. As such, some proposed chapters like 10.1 Testing for security, 10.2 Penetration testing 9.5.5 Security in software development lifecycles 9.5.6 Secure Coding Principles and techniques might not be within the scope. It would be better to phrase them in such a way that it reflects 'testability' and 'verifiability' of the design...meaning to provide support for test planning etc. as part of the design stage, instead of targeting actual penetration testing on the final implementation.		Accepted The editor will implement this comment during the revision of the 1st WD and thanks the Singapore NB for the valuable comment.
SI3	NWIP N7393	comments	ge	The earlier section such as scope and purpose gives the impression that the focus is more towards software design and development and the target audience is developer / programmers. However, the later sections include areas such as development environment. While it is agreed that the environment is important (in fact it is also one of the areas included in Common Criteria evaluation) and it is good to provide information on it, it is however, probably not within the scope of a typical		Accepted in principle. It is the aim of this TR to provide enough information on the whole lifecycle to place the design principles and techniques in context. Care will be taken to avoid giving too much information to detract from the scope and purpose of this document. The editor thanks the Singapore NB for

1	2	(3)	4	5	(6)	(7)
NB <sup>1</sup>	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
				programmer. The environment set up would probably be determined by the organization's CSO or CTO. As such, providing too much of such information tends to blur the focus of this report.		the valuable comment.
SI4	NWIP N7393	comments	ge	Testing is another area which should be out of scope of this report. Testing itself is a big topic and a separate document could be written for it. More importantly, testing should always be conducted by another person / team instead of the one developing it and therefore not within the target audience of this report.		Accepted in principle. It is the aim of this TR to provide enough information on the whole lifecycle to place the design principles and techniques in context. Care will be taken to avoid giving too much information to detract from the scope and purpose of this document. The editor thanks the Singapore NB for the valuable comment.
SI5	NWIP N7393	comments	ge	Since this report talks on systems which in most cases are the usage of multiple products in parallel / in support of one another, integration of these products becomes important. The interfaces, the communications and the handling of messages from one product to another have to be considered.		Accepted The editor will implement this comment during the revision of the 1st WD and thanks the Singapore NB for the valuable comment.
SI6	NWIP N7393	comments	ge	Even for a single product, it is now commonly developed by integrating various third parties libraries instead of developing entirely from one source / developer. How these libraries are integrated become utmost important.		Accepted The editor will implement this comment during the revision of the 1st WD and thanks the Singapore NB for the valuable comment.
SI7	NWIP N7393	comments	ge	Most designers are aware that security mechanisms are important and build these mechanisms such as I&A,		Accepted The editor will implement this

1	2	(3)	4	5	(6)	(7)
NB <sup>1</sup>	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note (e.g. Table 1)	Type of comment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
				access control etc but often fail to consider whether these controls can be bypassed (e.g. race condition). Therefore, more emphasis should also be placed on prevent bypassing of security controls and separation of security domains.		comment during the revision of the 1st WD and thanks the Singapore NB for the valuable comment.
SI8	NWIP N7393	comments	ge	With the clear restriction in scope to the design phase, this would be a good effort. Otherwise, the 'system engineering' scope might become too broad to manage		Noted The editor thanks the Singapore NB for the valuable comment.
US1	NWIP N7393	comments	ge	The US NB accepts the proposal, but would like the scope to be more explicit in what it will and will not do.	Scope This Technical Report will provide guidance on the principles, best practices and techniques for secure-system design for information and communication systems, complementing already existing design processes with security-specific engineering aspects. It will focus on the principles and techniques used to ensure that the security controls are effective and potential deficiencies of those controls can be handled within the system in a way that minimizes the security impact of such deficiencies. This TR will not address how risk assessments are undertaken nor how specific security controls are selected. The audience will include system	Accepted The editor will implement this comment during the revision of the 1st WD and thanks the US NB for the valuable comment.

1	2	(3)	4	5	(6)	(7)
NB <sup>1</sup>	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of com- ment <sup>2</sup>	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
					architects and designers. Furthermore the Technical Report will provide reference information to system developers and evaluators	