

[MB<sup>1</sup>] comments on Preliminary Draft for ISO/IEC 27034-1\*

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
US 1	1 Scope		Ge	<p>While the current working draft is meant to provide the guidelines for "application security" to organizations that already have an IT infrastructure including certain security elements such as firewalls, anti-virus and intrusion detection systems, and are possessing a team of in-house software developers, readers of the working draft could be misled to believe that the guidelines are equally applicable to commercial (off the shelf) software vendors/developers.</p> <p>The major problem here is that the development lifecycle for software products/services produced by commercial vendors/developers is very different from the development lifecycle for one-off software projects developed by in-house developers of a parent organization. Therefore, guidelines that may be deemed applicable to in-house developers of an organization are not necessarily applicable to commercial (off the shelf) software vendors/developers. An outline of the security development lifecycle which has been effectively deployed by Microsoft can be found in the US CS1 contribution "CS1/07-0212 Microsoft White Paper – the Trustworthy Computing Security Development Lifecycle" with its accompanied slide deck presentation to SC27. The outline shows that the security development lifecycle used by a commercial (Off the shelf) software vendor such as Microsoft is different from the "application security lifecycle" described in the current working draft.</p> <p>The supporting data accumulated by Microsoft since the start of the Microsoft security development lifecycle in 2002 shows that the Microsoft security development lifecycle is effective for reducing security issues for customers who use the Microsoft products/services that have been subject to the Microsoft security development</p>	<p>Please clarify that the guidelines provided in this working draft do not necessarily apply to commercial (off the shelf) software vendors/developers.</p> <p>Please add elements in the working draft to allow for the introduction of a set of acceptable guidelines that effectively address the security development lifecycle of commercial software products and services.</p>	

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.

[MB<sup>1</sup>] comments on Preliminary Draft for ISO/IEC 27034-1\*

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
				lifecycle. The Microsoft security development lifecycle is also successfully being used in managed code line of business (LOB) application development environments at Microsoft. The project editor and the responsible SC27 WG4 for the working draft may find it useful to review the Microsoft security development lifecycle for an in-depth understanding on why specific elements of the Microsoft security development lifecycle are effective for reducing security issues.		
US 2	3.6 Application Security 3.7 Application Security Certification		Te	<p>One-off software projects developed by in-house developers ultimately use commercial (off the shelf) software products such as software compilers, operating systems, productivity application packages, web clients, and backend servers and databases, and commercial web services such as public key infrastructure for identity services and web base commercial software distribution/installation and patching services for registered customers.</p> <p>All software (both COTS and one-off solutions) should follow secure development practices throughout the development process in order to address security concerns. However, one-off software projects have additional considerations in that no trustworthiness can be effectively assigned to these software projects developed by in-house developers unless the trustworthiness of the underlying commercial software products and services have been effectively determined.</p>	<p>Given that the current working draft is meant to address the one-off software projects developed by in-house developers of an organization, it is recommended the focus of the further development of the current working draft is directed to the "Acquisition Process" and "Supply Process" areas which are only briefly mentioned in the working draft, but still under-developed as the working draft text materials. We don't see that the current working draft could be complete and be useful as an ISO standard without a set of acceptable guidelines that effectively address the security development lifecycle of commercial software products and services. These guidelines are necessary to determine the trustworthiness of commercial software products and services for the "Acquisition Process" and "Supply Process" areas mentioned in the current working draft.</p> <p>We recommend the development of an</p>	

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.

**[MB<sup>1</sup>] comments on Preliminary Draft for ISO/IEC 27034-1\***

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
					ISO working draft for security development lifecycle of commercial software products and services. As a member of the US delegation to SC27, Microsoft is willing to contribute to the development of an ISO working draft for security development lifecycle of commercial software products and services based on its extensive experience gained through its on-going deployment of its security development lifecycle applied to hundreds of millions of lines of production software code.	

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.

**[MB<sup>1</sup>] comments on Preliminary Draft for ISO/IEC 27034-1\***

Date: 2007-MM-DD	Document: <b>SC27 N5737</b>
------------------	-----------------------------

1	2	(3)	4	5	(6)	(7)
<b>NB<sup>1</sup></b>	<b>Clause No./ Subclause No./ Annex</b> (e.g. 3.1)	<b>Paragraph/ Figure/Table/ Note</b> (e.g. Table 1)	<b>Type of com- ment<sup>2</sup></b>	<b>Comment (justification for change) by the NB</b>	<b>Proposed change by the NB</b>	<b>Resolution on each comment</b>

\* subject to JTC 1 endorsement on the New Work Item Proposal (SC 27 N5726) by 2007-09-19

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.