

[US¹] comments on ISO/IEC 2nd CD 27000

Date: 2007-MM-DD	Document: SC27 N5851
------------------	-----------------------------

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
US1	Whole doc		t	The US' comments are supported by a revised Word version of the subject document.	See US Attachment 'A'.	
US2	Whole doc & §2		E	The multitude of footnotes stating 'under preparation' (or similar) is unnecessary and could be addressed more directly and singularly	Remove all such footnotes and add to the appropriate heading in §2 (§2.3.2, '3, '4, '5(27007 - when added), §2.4.1) the text "(Under preparation)". See US Attachment 'A'.	
US3	Whole doc		E	Numerous grammatical and typographic errors	Correct as per marked-up document. See US Attachment 'A'.	
US4	Whole doc		T	ISO/IEC 27007 is not included comprehensively.	Add appropriate coverage of 27007 in: Introduction; §2.3.5; Figure 1.	
US5	§2.1.1	Title	E	Clarification	Add to title "(This document)"	
US6			T	'foundation' is misleading - 27001 provides the foundation - everything else is relative to and of little value without it.	Rephrase as "ISO/IEC 27000 provides a focal point which explains the ISMS family of standards and provides a common glossary used within it."	
US7	§2	Second figure	E	Key has hidden text the figure title	Reveal titling	
US8	§3	2 nd para	E	Use of "If ..." weakens the expression	Replace with "It is the intention that these terms and definitions apply also for other documents, particularly those in the ISO/IEC 27000 family of standards. When this is so, this shall be indicated in these other documents by using the following introductory paragraph: "For the purposes of this document, the	

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.

[US¹] comments on ISO/IEC 2nd CD 27000

Date: 2007-MM-DD	Document: SC27 N5851
------------------	-----------------------------

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
					<p>terms and definitions given in ISO/IEC 27000 apply".</p> <p>The definitions below are given in an order which develops the readers understanding and which ensures that no term uses another term from this set of definitions which has not already been defined. A separate alphabetic listing is given in an index.</p> <p>"</p>	
US9	§3	Sub-sectioning	T	<p>A number of problems, for which a single solution is proposed (and provided):</p> <p>The definitions are broken into different categories (§3.1 – '.5 inclusive) – this is not necessary nor advantageous: moreover it has the effect of actually diminishing the significance of certain terms, e.g. 'SoA', 'ISMS policy' and 'information security policy' (plus many others) are relegated to being 'related to documentation'. This is almost misleading – these terms are fundamental to what ISMS is about and their significance is not apparent if they are placed under such a categorization;</p>	<p>Present the definitions as a single set without artificial and contentious divisions.</p> <p>See the table in US Attachment 'A', in which all definitions have been coalesced..</p>	
US10	§3	Sub-sectioning	T	<p>Some terms use others within the list but which have not been previously defined – this is not helpful for the reader. The fact that the list is NOT alphabetic is applauded, but to be most effective the list should set out the terms in an order which allows the reader to follow a flow, as a kind of story-telling. Therefore, re-order to ensure that no term uses another unless the referenced term has been previously defined</p>	<p>re-arrange the definitions, such that none of them make reference to another which has not already been defined. Explain this in the introduction to §3.</p> <p>See the table in US Attachment 'A', in which all definitions have been re-ordered as necessary to ensure that any definitions which use another term do not precede it. Suitable introductory</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.

[US¹] comments on ISO/IEC 2nd CD 27000

Date: 2007-MM-DD	Document: SC27 N5851
------------------	-----------------------------

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
					text has been added.	
US11	§3	Sub-sectioning	T	The definitions are generally well-constructed but one instance of circularity exists.	Re-worded to avoid circularity. See the table in US Attachment 'A', in which the definition has been suitably re-worded.	
US12	§3	Sub-sectioning	T	Two relevant terms should be added: 'non-conformity' and 'information system'	Add these terms and appropriate definitions. See the table in US Attachment 'A', in which all such additions are made.	
US13	§3	Sub-sectioning	T	In 27001 all definitions identify a source, omitted in 27000. Is this an oversight or a deliberate action?	Add sources references?	
US14	§3	Sub-sectioning	E	Various typographic and grammatic oversights require remedying.	See the table in US Attachment 'A', in which all such instances are marked and corrected.	
US15	§3	Sub-sectioning	E	Where a definition uses a term which is itself defined within 27000 it should be shown in bold to emphasise that it has a special significance.	Make all such terms bold. See the table in US Attachment 'A', in which all such instances are marked in bold.	
US16	§3	'information security policy'	E	Notes to information security policy are inappapropriate, since note 1 address a process which has no bearing on what such a policy is and note 2 similarly does not affect the definition.	Remove notes in this definition and all other instances where these or similar notes apply.	
US17	§3	'interested party' & 'stakeholder'	E	Notes are not pertinent: in note 1 there is no reference to a decision maker, so it is out of context and confusing; note 2 makes an assertion but does not quantify it. Moreover, stakeholders have a more specific interest rather than a broader one, since they either directly influence events or are materially affected by them, whereas interested parties may just like watching but	Review the definitions and make them more specific, so as to make explicit the differentiation between them. Remove the note 2 (or at the least make it more explicit).	

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.

[US¹] comments on ISO/IEC 2nd CD 27000

Date: 2007-MM-DD	Document: SC27 N5851
------------------	-----------------------------

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
				have no control nor are they materially affected. Consider whether the definitions are inadequate (or perhaps they're fine as are) if such a not is required.		
US18	§3	'interested party' & 'stakeholder'	E	One refers to individual, one to person. What's the difference?	If the usage is not significant, use one or the other to be consistent, or otherwise explain the difference. Consider where there may be similar usage within the terms (e.g. 'third party' uses 'person').	
US19	§3	'third party'	E	Refers to a 'body' - how does that differ from a group or an organization? Is it a different type of entity?	If the usage is not significant, use one or the other to be consistent, or otherwise explain the difference. Consider where there may be similar usage within the terms.	
US20	§3	'audit criteria'	E	Definition is not sufficiently comprehensive since it overlooks that the criteria are the basis for an assessment's determinations, not just an audit	Revise the definition. See the table in US Attachment 'A', in which revised text is presented.	
US21	§3	'auditor'	E	The note is unnecessary – it does not affect the definition and other parts of this document describe what individual other documents do.	Remove note(s).	
US22	§3	'risk treatment plan'	E	The note is unnecessary – it does not affect the definition and other parts of this document describe what individual other documents do.	Remove note(s).	
US23	§3	'review'	E	Definition is not sufficiently comprehensive since it overlooks the fact that there must be some basis of comparison against which a review is undertaken	Revise the definition. See the table in US Attachment 'A', in which revised text is presented.	
US24	§3	'guidelines'	E	Definition is not sufficiently comprehensive since it implies that guidelines relate only to policy (not so).	Revise the definition. See the table in US Attachment 'A', in which revised text is presented.	

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.

[US¹] comments on ISO/IEC 2nd CD 27000

Date: 2007-MM-DD	Document: SC27 N5851
------------------	-----------------------------

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 com- ment²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

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.