

US National Body Contribution on ISO/IEC 4th WD 27004

[US¹] NB comments on ISO/IEC 4th WD 27004

Date: 2006-09-12	Document: SC27 N5094
------------------	-----------------------------

1	2	(3)	4	5	(6)
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
US1	All		TE	It is not clear how this document fits into the ISO/IEC 27000 series of standards; i.e., which ISO/IEC 27000 standards are prerequisite to ISO/IEC 27004 and which ISO/IEC standards come after ISO/IEC 27004.	Identify where ISO/IEC 27004 is within the documentation roadmap for the ISO/IEC 27000 series of standards.
US2	All		TE	The document implicitly assumes that the selection and validation of controls is covered in other parts of ISO 27000 series. However, it is not very clear to the reader whether the selection/validation of controls is within the scope of ISO 27004.	Add an explicit "Assumption" sub-section in Section 5 to include the following: <ul style="list-style-type: none"> This document will not contain any guidelines for ensuring the sufficiency of selected controls. It is assumed that the control selection and implementation is done as part of ISO 27003. It is assumed that the Risk Assessment process validates the sufficiency of the selected controls.
US3	All		ED	The document terminology is inconsistent in the usage of the terms "ISM measurement", "ISM Measurement" "ISM measures". "Measurement" and "Measures" are used interchangeably.	The case and usage should be consistent throughout the document. Perhaps the comment that appears late in Section 9 about the term measurement and measure should be introduced early on and then the terms should be used appropriately as relevant.
US4	5.1	1	Te	The objective seems to be very broad and doesn't cover everything that is really discussed in the standard. Security requirements are not just based on risk assessment and applicable legal and regulatory requirements.	Recommend inclusion of standards, and business policy and objectives in this paragraph.
US5	6.1	1 and 2	Te	The objectives listed here are not discussed within the measurement process section. This section seems to be covering Roles and Responsibilities as well as the place in the ISMS cycle that measurements should be located. These objectives do not appear to be related to the rest of the portions of section 6. The second bulleted list appears to be each of the sections (7 through 11) of the document.	Possibly make the objectives be an overview or if the intent is to have these be the objective of the process itself then describe that this is the process itself and breakout the rest of section 6 that discusses roles and responsibilities.
US6	6.5		ED	Typo in item (vi) – there is an extra comma	Remove the comma.

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.

US National Body Contribution on ISO/IEC 4th WD 27004

[US¹] NB comments on ISO/IEC 4th WD 27004

Date: 2006-09-12	Document: SC27 N5094
------------------	-----------------------------

1	2	(3)	4	5	(6)
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
US7	6.5.1.1		TE	Item (g) – “improve effectiveness of the ISM Measurement” is very vague and how is it aligned with item (b).	Item (g) should be removed or tied to some specific success metrics or baseline criteria. The process as part of the PDCA model should be aligned with the ISO 27001 process and since item (b) seems to state that, then Item (g) appears to be unnecessary.
US8	6.5.1.2		TE	There is no reference to auditors throughout the document.	Would the beneficiaries include the auditors? If so, they can be listed in this section.
US9	7.3		TE	Section 7.3 refers to “applicable assets and technology”, but no reference is provided in the document as to how to identify such assets.	Document should specify that a standardized, systematic procedure be followed to ensure that all information assets are identified. ISO/IEC 18028-2 decomposes an organization’s information technology systems into a layered hierarchy of equipment and facilities groupings and examines the activities that occur at each layer to identify information assets that need protection. If such a specification is included in ISO/IEC 27003, then a reference will be sufficient.
US 10	7.4		TE	Section 7.4 does not provide any guidance for systematically establishing the measures	Document should specify that a standardized, systematic procedure be followed for identifying appropriate performance measures. For example, ITU-T X.805 offers a perspective of organizational activities which can be relevant to measure definition - for instance securing access of a business object such as customer database by an IT organization (for maintenance) versus a customer care group (for trouble shooting) would need to be measured and monitored using different performance measures.
US 11	7.4	G		To provide consistency with the entire document the stakeholders should include all that are covered in section 7.4.3 Missing Measure Reviewer.	Add Measure review as one of the stakeholders to match listed stakeholders in 7.4.3
US 12	7.4.3 and 7.4.4		Ed	To provide consistency with the list in 7.4, sections 7.4.3 and 7.4.4 should be swapped.	Re-order 7.4.3 and 7.4.4
US 13	7.4.4		ED	Misspelled word “derives”	It should be “derived”
US 14	7.5		TE	The criteria “meaningful” can be subjective and may not guarantee comprehensiveness of selected measures.	ISO/IEC 18028-2 framework can be used to provide a comprehensive justification of the defined measures, and should be specified as a recommended approach. It would also be consistent with the threat and vulnerability assessment that should

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.

US National Body Contribution on ISO/IEC 4th WD 27004

[US¹] NB comments on ISO/IEC 4th WD 27004

Date: 2006-09-12	Document: SC27 N5094
------------------	-----------------------------

1	2	(3)	4	5	(6)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of com- ment ²	Comment (justification for change) by the NB	Proposed change by the NB
					utilize ISO/IEC 27003 as well.
US 15	Annex B		TE	Some more situation specific examples will be helpful	Examples of regulatory compliance and additional measure definitions and measurement approaches for a simple case study can be added
US 16			Ge	The use of both “implementation plan” and “Implementation plan” seems to be confusing.	Be consistent with usage of either “implemenation plan” or “Implementation plan”

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.