

1	2	(3)	4	5	(6)
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
US1	3.1	1	Te	One of the critical success factors for any ISMS is to have strong management commitment to the System. This section is labeled as "Management Commitment" under Critical success factors.	Recommend that there is a statement made for the critical success factor of Management Commitment.  Add text: The organization should have communication from management that demonstrates the level of commitment to establishing , implementing and operating an effective ISMS.
US2	6.2.3	1	Te	This section discussion important starting points but currently only lists one item. There are additional documents that could be included as starting points as well.	Include beyond just annual reports as a document starting point to include mission statements of the organization as well as defined business operational objectives.
US3	6.2.3	1	Te	The paragraph states "Consider the organizations core activity and its 'role' in a macro-environmental perspective". This should also include the culture of the organization which may have an impact on the operational objectives.	Include the impact of organizations culture in the macro-environmental perspective.
US4	6.2.5	2	te	In the second paragraph it is stated that "sufficient" records should be kept. Since what is considered sufficient varies for each organization or person's interpretation there should be examples of what might be considered sufficient records.	Include examples of sufficient records
US5	6.3.2	1		Precondition for success of an operational analyse is that access and awareness of existing policies and processes	Include access and awareness of existing policies and processes as part of the preconditions.
US6	6.4.2	1		To do a risk assessment of an organization there needs to be some understanding of the types of threats to that organization's objectives.	Precondition needs to include an understanding of the types of threats to the organization's objectives
US7	6.4.4	1		Currently there is no text for who to involve in a Risk Assessment.	Suggested text: "Suitable staff for a risk analysis is management personnel and a good insight into the organization's objectives, individuals with a good insight into what is currently relevant in terms of threats to the organizations objectives such as information security and IT security personnel."
US8	6.5.3	1		When creating policies many times they appear to be created without understanding of the capabilities of the	Recommend that those that are going to be involved implementing the policies should be part of organising the work of creating the policies.

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.

**CS1/06-0215 Cisco Systems Contribution**  
**[MB<sup>1</sup>] NB comments on ISO/IEC 2<sup>nd</sup> WD 27003**

Date: 2006-MM-DD	Document: <b>SC27 N5092</b>
------------------	-----------------------------

1	2	(3)	4	5	(6)
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
				organization. To make sure that the policies can be complied with there should be involvement from those that would be implementing the policies.	
US9	6.5.4	1		Currently there is no text on who to involve in Policy creation.	Suggested text: "People to involve in policy creation is management, information security, implementors of policy (this could be IT organizations, Human Resources, etc)"
US1 0	6.5.5	3 c		This bullet discusses what should be in a short presentation regarding policies. The information about what these are currently in the organization should have been gleaned during the Operational and Situational analyses. There is however no reference back to that in this bullet and this should be stated.	Include text that states the list of general security policies that are significant to an organization should be gleaned from situational and operational analyses.
US1 1	6.5.6	1		The text states that the results will be Information security policy. However the results may include multiple policies.	Change text from: "Information security policy " To "Information security policy or policies"
US1 2	6.6.1	1		In describing the controls it should be noted what kind of control it is and regulatory controls should be included as well.	To describe controls should include regulatory (such as legal or governmental) that were gleaned during the operational and situational analyses
US1 3	6.6.5	1		The section 6.6 is Applicability of controls to an organization. Part of Applicability is not only policies that are created but also processes that may be created based on findings in the various analyses that were done.	Recommend that additional test is created to discuss processes, not just policies.

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.