

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
US1			GE	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 27005 and which ISO/IEC standards come after ISO/IEC 27005	Identify where ISO/IEC 27005 is within the documentation roadmap for the ISO/IEC 27000 series of standards.	
US2			GE	The document does not show a real life example on how to perform a risk assessment.	Provide an example illustrating how a risk assessment would be performed as an informative Annex.	
US3	A.1 20, page 36		TE	The process used to develop the target system's functional description should leverage security architecture models/ frameworks such as ITU-T X.805, ISO/IEC 18028-2.  Include ITU-T X.805, ISO/IEC 18028-2 as a reference as  Annex I	A detailed description of target system security is possible only by evaluating its ecosystem. Ecosystem includes the system hardware/ and its various external and internal interfaces.  Cyber security is of particular importance in the functional description of a target systems or solution. ITU-T X.805, ISO/IEC 18028-2 provides an architectural framework that will help in developing a methodical functional description for cyber security. The resulting description would describe the feature functionality of different types of information and how it is employed for use, management and control of a system. The factors influencing the information (such as potential threats, vulnerabilities) will also be a part of the resulting functional description cyber-security risk.	

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.

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
US4	5	4 <sup>th</sup> /5 <sup>th</sup> para.	te	The 4 <sup>th</sup> para. states that “risk management process can be iterative.” The 5 <sup>th</sup> para. follows that statement that “an iterative approach to risk assessment.” These two paragraphs appearing one after the other leads the reader to believe that the terms “risk management” and “risk assessment” are interchangeable. Is that the intent? The two terms should not be considered interchangeable in that risk assessment is just one piece of risk management.	Replace “An iterative approach to risk assessment increases depth and detail of the assessment at each iteration.”  with  An iterative approach to conducting risk assessment increases depth and detail of the assessment at each iteration.	
US5	6.1.2	1 <sup>st</sup> bullet	te	An additional parameter common among risk assessment approaches is that of likelihood or probability of exploitation. This parameter can be thought of in terms of a threat or threat agent’s motivation, opportunity, and means (MOM). Additionally, historical instances (or lack of) exploitation should be considered when evaluating risks, as well as other mitigating factors.	Add likelihood or probability of exploitation to the listing of parameters.	

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.

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
US6	7.1	1 <sup>st</sup> para.	te	The statement, “Risks should be identified, quantified, and prioritized” leaves no room for qualitative assignment of risk. In many instances, assets cannot be quantified (e.g., reputation) and therefore, a method for qualifying the risk for an asset that cannot be quantified should be allowed.	Replace “Risks should be identified, quantified, and prioritized against criteria for risk acceptance and objectives relevant to the organization.”  With  “Risks should be identified, quantified or qualitatively described, and prioritized against criteria for risk acceptance and objectives relevant to the organization.”	
US7	Section 7.2.1.1/Annex B		TE	Section 7.2.1.1 and Annex provide only high-level implementation guidance on identification of assets	Document should specify that a standardized, systematic procedure is followed to ensure that all information assets are identified	

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.

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
US8	7.2.1.3	2 <sup>nd</sup> para.	te	While “likely level of weakness, i.e. ease of exploitation” is a necessary factor, especially when determining risk levels, assessing that factor during vulnerability identification would be difficult at best since threat factors (e.g., opportunity, methods, etc.) and implemented controls should be considered when assessing the ease of exploiting a given vulnerability.	Replace :This stage includes identifying weaknesses that may be exploited by a threat source to cause harm to the assets, the business they support and assesses their likely level of weakness, i.e. ease of exploitation”  With  “This stage includes identifying and assessing the likely level of the weaknesses that may be exploited by a threat source to cause harm to the assets and the business they support. The likely level of weakness, i.e. ease of exploitation, can be assessed through examining existing controls and applicable threat factors.”	
US9	7.2.2.4	3 <sup>rd</sup> para.	te	This text discusses impact of security incidents and asset valuation, which are not mentioned in the “Action” statement. Paragraph seems out of place here.	Delete paragraph.	
US10	7.3	4 <sup>th</sup> para.	te	The 1 <sup>st</sup> bullet states, “Whether a risk needs treatment.” A risk should require treatment at all times, even if that treatment is risk retention, as specified as a risk treatment option presented in Clause 8.1,	Remove bullet,	
US11	8.4 & 8.5		ed	These two clauses should be reversed to remain consistent with the previous text in Clause 8.1 and Figure 2.	Reverse the two clauses.	

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.

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
US1 2	A.2	Pg 24, lines 6 & 7	te	Why is it inappropriate to “base security investments on cost-effectiveness?” This basis is a necessary factor to consider when incorporating security controls within an organization or system.	Replace: “Even though it is inappropriate to base security investments on cost-effectiveness, some kind of economic justification is generally required by the organisation's financial departments.”  With  “While it is not always appropriate to base security investments on cost-effectiveness, some kind of economic justification is generally required by the organisation's financial departments.”	
US1 3	Annex A, D.2		TE	Section D.2 in Annex A refers to scanning tools, STE, and penetration testing methods, but contains no guidance for performing an overarching vulnerability analysis.	Document/Annex A should include a section providing guidance on how to perform an overall vulnerability analysis.	
US1 4	Appendix C	1 <sup>st</sup> Table, Natural Events Category	te	What meteorological even would be considered as “deliberate?” Should this not be limited to “environmental?”	Remove “D” from the Origin column.	
US1 5	Appendix C	1 <sup>st</sup> Table, Compromise of Information Category	te	Text states that “Theft of media or documents” and “Theft of equipment” can be accidental or deliberate. Under what circumstances can “theft” be considered “accidental?”	Remove “A” from the Origin column.	

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.

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
US1 6	Appendix E.2.1	Table 1	te	The horizontal matrix factor of “Likelihood of occurrence – Vulnerability” does not seem to match the previous text discussing the matrix. Should this factor be “Ease of exploitation” or perhaps “Impact” or “Consequence of Occurrence?”	Replace “Likelihood of occurrence – Vulnerability” with “Ease of Exploitation.”	
US1 7	Appendix E.2.1	Pg 55, Line 25	te	The text discusses finding the risk using the columns for “identified by the consequence of the threat and the vulnerability.” This identification does not appear in Table 1.	Revise language describing the table to be consistent with the column and row headings.	
US1 8	Annex F, A.1 12		TE	No background or reference was provided regarding the six (CIA+) security concerns listed in Annex F A.1 12.	Document should provide guidance on why these six concerns were identified. Either reduce to CIA or use a standardize set of security concerns. ISO/IEC 18028-2 has a set of eight security concerns.	
US1 9	Annex G		TE	Annex G provides a general overview on ISMS awareness and training, but does not provide specifics on risk assessment and risk treatment training.	Although the ISO/IEC 27005 could be used as training vehicle, the document/Annex G should include specifics directly related to risk assessment and treatment training and awareness.	
US2 0	ALL		GE	What is the justification for the 3 “shall’s” in the document.	If appropriate change the “shall” to “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.