

[MB¹] US NB comments on ISO/IEC 1st WD 27033-1³

Date: 2007-MM-DD	Document: SC 27 N5908
------------------	------------------------------

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
[US] 1	ALL		TE	<p>The content for revised ISO/IEC 27033-1 is basically the same as ISO/IEC TR 13335-5, and that is the reason for the scope mismatch (as described in the next US2 comment).</p> <p>ISO/IEC TR 13335-5 is a technical reference and provides guidance with respect to networks and communications to those responsible for the management of IT security. The guidance supports the identification and analysis of the communications related factors that should be taken into account to establish network security requirements.</p> <p>ISO/IEC TR 13335 builds upon Part 4 of the 13335 series by providing an introduction on how to identify appropriate safeguard areas with respect to security associated with connections <u>to communications networks</u>. Detailed design and implementation aspects of the technical safeguard areas are considered to be out of scope.</p> <p>As such the revised ISO/IEC 27033-1 is not meeting the revision objective and serves only as an informative reference for communications aspects. It is not an over-</p>	<p>Part 1 should be an over-arching document for the 27033 series. It should primarily focus on terminology, alignment with other standards, and a roadmap to other parts of 27033.</p> <p>Most of the current draft content is more appropriate in other parts of the series, and is addressed through the other comments.</p> <p>It is recommended that Part 1 establish:</p> <ul style="list-style-type: none"> • terminology for the series (such as network perimeter, internal network (subnets, DMZ, etc.). Even the security terms such as risk, threats, attack, vulnerabilities etc. should be defined • role of security policy in securing networks • role of regulations and 	

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.

3 Subject to SC 27 approval by a 60-day balloting (see SC 27 N5983) and subsequent JTC 1 endorsement of the renumbering from 18028 to 27033.

[MB¹] US NB comments on ISO/IEC 1st WD 27033-1³

Date: 2007-MM-DD	Document: SC 27 N5908
------------------	------------------------------

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
				arching document for the 27033 series – the technical justification and roadmap for the series is not established clearly. It is also critical to establish the alignment with ISO/IEC 13335-1 and ISO/IEC 27000 series (relevant parts) since there is a reference to the controls throughout the document.	governance <ul style="list-style-type: none"> • alignment of the series with other standards • defence in depth considerations and common security solutions such as Firewalls, IDS/IPS, VPNs etc.., • design considerations based on networking scenarios and networking technology (current and future) – this section could actually be part of the roadmap to the other parts • a clear guidance of how the 27033 series should be used, and a roadmap to the other parts of the series 	
[US] 2	Scope		GE	There is a scope mismatch in what was agreed as part of revision of 27033 series and what is noted in the draft. The <u>agreed upon objective</u> of the proposed revision to 27033-1 (previously 18028-1) was as follows:	Retain the agreed upon original scope since it is deals with a more holistic (end-to-end) view of network security and not just a subset related to communications security.	

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.

3 Subject to SC 27 approval by a 60-day balloting (see SC 27 N5983) and subsequent JTC 1 endorsement of the renumbering from 18028 to 27033.

[MB¹] US NB comments on ISO/IEC 1st WD 27033-1³

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>To define and describe the concepts associated with, and provide management guidance on, network security. This should include an overview of network security and related definitions, and guidance on how to identify and analyze the factors to be taken into account to establish broad network security risks and then identify network security requirements. It should also include introductions to achieving good quality technical security architectures, and the specific risk, design and control aspects associated with typical networking scenarios and with the networking ‘technology’ areas prevalent today and projected for the future (dealt with in subsequent parts of ISO/IEC 18028). In effect it should also provide an overview of the ISO/IEC 18028 series and a ‘road map’ to all other parts</p> <p><u>However, the scope noted in the draft contribution has a very narrow focus on “communications security”:</u></p> <p>ISO/IEC 27033-1 provides direction with respect to networks and communications,</p>	<p>Network security applies to security of devices, security of management activities related to the devices, applications/services, end-users, in addition to security of the information being transferred across the communications links.</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.

3 Subject to SC 27 approval by a 60-day balloting (see SC 27 N5983) and subsequent JTC 1 endorsement of the renumbering from 18028 to 27033.

[MB¹] US NB comments on ISO/IEC 1st WD 27033-1³

Date: 2007-MM-DD

Document: **SC 27 N5908**

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
				including on the security aspects of connecting information system networks themselves, and of connecting remote users to networks. It is aimed at those responsible for the management of information security in general, and network security in particular. This direction supports the identification and analysis of the communications related factors that should be taken into account to establish network security requirements, provides an introduction on how to identify appropriate control areas with respect to security associated with connections to communications networks, and provides an overview of the technical design and implementation topics and possible control areas, including those dealt with in detail in ISO/IEC 27033-2 to ISO/IEC 27033-7 and on.		
[US] 3	ALL		GE	Currently Part 1 seems to be addressing too many aspects in varying levels of depth. The previous comments have suggested that the content for Part 1 be an over-arching document for the series. However, it appears that the draft is also proposing some other aspects (such as incident management, monitoring etc.) – which obviously is not well integrated into the overall flow.	Depending on the resolution of the first 2 US comments, we also offer another perspective for organizing the content of Part1 using the PDCA model (see Attachment 1). The attachment shows the approach for managing	

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.

3 Subject to SC 27 approval by a 60-day balloting (see SC 27 N5983) and subsequent JTC 1 endorsement of the renumbering from 18028 to 27033.

[MB¹] US NB comments on ISO/IEC 1st WD 27033-1³

Date: 2007-MM-DD	Document: SC 27 N5908
------------------	------------------------------

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>comprehensive ISMS – and thus can be used as the layout for organizing Network Security Guidance – which is Part 1).</p> <p>Thus Part 1 can be the “what” of the 27033 series and the “how” can be presented in the other parts of the series and/or references to other standards (as appropriate)</p>	
[US] 4	ALL		ED	Several times in the document, the term “trust” and “trust relationships” is used. There was an objection to the use of the word “trust” during the meeting in Moscow.	Either the term should be removed or explained in the context in which it is being used.	
[US] 5	ALL		ED	The document uses the phrase “as relevant aided by the use of models/frameworks” several times. It is not clear what is meant by the phrase.	The phrase should be reworded to give specific guidance on what needs to be supplemented, and which frameworks would be relevant	
[US] 6	Section 5		GE	Is it “Structure” of the series or just structure of Part 1? It is not clear because there are too many references to other parts in this section.	The section is too long and wordy. The description should be easy to read and give a sense of the document layout. Roadmap may be better way to handle cross references in a completely separate section.	

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.

3 Subject to SC 27 approval by a 60-day balloting (see SC 27 N5983) and subsequent JTC 1 endorsement of the renumbering from 18028 to 27033.

[MB¹] US NB comments on ISO/IEC 1st WD 27033-1³

Date: 2007-MM-DD	Document: SC 27 N5908
------------------	------------------------------

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
[US] 7	Section 5		TE	The term “Secure Service Management” is confusing – is it referring to security of services supported on the infrastructure or is the context “network and service management” or security of “management activities” . How is it different from “Network Security Management” which also appears in this section?	The terms should be explained at the first instance since they appear throughout the document.	
[US] 8	Section 6		ED	Aim is not a good title and also the content in the section is not very descriptive of the intended objective	Remove the section	
[US] 9	Section 7.2		ED	The title “Identification Process” does not suggest anything.	Change it to “Security Planning Guidance”	
[US] 10	Section 7.2	Figure 3	ED	What is meant by “Management Process in the Context of Network Security”?	Figure caption should be changed to something more meaningful	
[US] 11	Section 7.2	Figure 3	TE	The Figure is not adding any value. Some of the steps such as “Security Requirements Definition”, “Development and Testing” are missing.	The figure should be removed from this document and introduced in a more complete manner in Part 2 of the series.	
[US] 12	Section 8		GE	Section 8 does not flow seamlessly with the rest of the document.	Re-arranging the overall document structure and content should help in a seamless lead into this section.	
[US] 13	Section 8		TE	“Reliability” is mentioned but there is no information provided in terms of how it relates to the contribution and the scope.	Defining a security policy is an important component and this section should provide guidance on “how” to develop a security	

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.

3 Subject to SC 27 approval by a 60-day balloting (see SC 27 N5983) and subsequent JTC 1 endorsement of the renumbering from 18028 to 27033.

[MB¹] US NB comments on ISO/IEC 1st WD 27033-1³

Date: 2007-MM-DD	Document: SC 27 N5908
------------------	------------------------------

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
				The examples (bullet list) of what the policy should state are not systematically derived. There should be a common thread of these “examples” throughout the contribution (e.g.” no payment instruction is valid without a digital signature” is not discussed again in the doc).	policy to meet the security and business objectives (we can provide contribution in this section)	
[US] 14	Section 9		TE	“Review Network Architectures and Applications” should also include Services.	This section belongs in Part 2, and should focus on infrastructure, applications and services	
[US] 15	Section 14		TE	Section 14 (Reference Networking Scenarios) should be removed (just a reference to Part 3 is sufficient as part of roadmap).	Move content to Part 3 of the series	
[US] 16	Section 11 - specifically section 11.2		TE	What exactly is meant by “Trust Relationships”? It is not clear why this definition of Trust is established in so much detail (it cannot be normative) and should be in Annex if at all. Also insider attacks are a major concern – so not sure why they are viewed as more trustworthy.	Parts of the this section should be merged with the overall risk assessment strategy and the details should be in an Annex.	
[US] 17	Section 12	Table 4	TE	The columns are not vulnerabilities – they are threats.	A standard threat model such as X.800 should be used.	

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.

3 Subject to SC 27 approval by a 60-day balloting (see SC 27 N5983) and subsequent JTC 1 endorsement of the renumbering from 18028 to 27033.

[MB¹] US NB comments on ISO/IEC 1st WD 27033-1³

Date: 2007-MM-DD	Document: SC 27 N5908
------------------	------------------------------

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
[US] 18	Section 12		TE	Security risk is described without reference to threats, vulnerabilities and impact There is no technical justification for this clause and how it can be applied or how it adds value to existing methodologies	Discussion needs to establish the risk assessment to explain the “what” aspects – including threats, vulnerabilities, and impact (some part of current 11.2 can be included here)	
[US] 19	Section 15		TE	The section refers to “Non-technical controls and general technical control areas”, but provides no normative guidance.	The section needs to be established in the context of defining assets that require protection, the threats to the assets, vulnerabilities for realizing the threats and then defining a listing of physical, operational and technical safeguards (instead of simply listing the controls)	
[US] 20	15.2.1		TE	The sub-section provides an informative listing of known elements without any guidance for establishing the “what” in a systematic manner. There needs to be some rationalization and justification.	The section should provide a systematic approach for identifying: <ul style="list-style-type: none"> the different types of network connections the different networking characteristics and related trust relationships the potential types of security risks associated with network connections 	

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.

3 Subject to SC 27 approval by a 60-day balloting (see SC 27 N5983) and subsequent JTC 1 endorsement of the renumbering from 18028 to 27033.

[MB¹] US NB comments on ISO/IEC 1st WD 27033-1³

Date: 2007-MM-DD	Document: SC 27 N5908
------------------	------------------------------

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
					(and the use of services supported via those connections) This type of content is also more relevant to Part 2 of the series.	
[US] 21	Section 16		TE	Section 16 is very high level with a lot of redundancy across sub-sections for common risks. It is more important to focus on the design issues and considerations related to networking technologies, rather than on the known risks and best practices (which can be listed in the annex).	The section should be restructured into 3 major subsections – Background, Security Risks, and Controls. The technology should be rolled into these sections (or moved into Annex)	
[US] 22	7.1	Figure 2	E	Phone network is unclear.	Change “Phone Network” to “VoIP Network” in diagram for clarity	
[US] 23	7.1	Paragraph 4	T	WLAN infrastructures typically require authentication (WPA, EAP/LEAP, 802.1x, etc), not just isolation.	Add “and authentication” after “isolation.”	
[US] 24	7.1	Paragraph 9	E	“Security problems” is not a commonly known term.	Replace “security problems” with “security events.”	
[US] 25	9.3	Paragraph 1	E	Bullet points could benefit from specific examples.	Add an example protocol after each bullet (shared media – Ethernet, routing protocol – OSPF, etc)	
[US] 26	9.3	Paragraph	T	IP networks (v4 or v6) could implement IPsec,	Replace “do not provide any	

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.

3 Subject to SC 27 approval by a 60-day balloting (see SC 27 N5983) and subsequent JTC 1 endorsement of the renumbering from 18028 to 27033.

[MB¹] US NB comments on ISO/IEC 1st WD 27033-1³

Date: 2007-MM-DD	Document: SC 27 N5908
------------------	------------------------------

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
		2		but choose not to for a variety of reasons (performance, scalability). Text needs to reflect the fact that it is a choice.	security” to “do not implement any security”	
[US] 27	12	Figure 4	T	Confidentiality for data at rest not addressed.	Add confidentiality for data at rest for end systems.	
[US] 28	12	Table 4	E	Agree with editor’s note to delete this table	Delete table	
[US] 29	15.2.5	Paragraph 1	E	The last sentence references new network technology. The sentence is rather specific and may not include all possible scenarios.	Add “and networked environments” at the end of the sentence.	
[US] 30	15.5	Whole section	T	Clause does not address log storage and retrieval.	Text should provide guidance on using security management tools for log storage, retrieval, and reporting. US member body is unable to provide the text at this point.	
[US] 31	15.7	Paragraph 3	T	Spyware is a type of malicious code but is not addressed. Malware is a commonly used term for malicious code.	Add terms “spyware” and “malware” where appropriate.	
[US] 32	16.1.1	Paragraph 2	T	Generally the use of hubs are discouraged (evsdropping on traffic, performance issues, etc).	Add the following at the end of the paragraph: Use of hubs is generally discouraged due to a variety of security (e.g., eavesdropping on traffic) and performance issues.	
[US] 33	16.1.1	Paragraph 3	T	Reference to 802.11 is incomplete.	Change “802.11” to “802.11 a/b/g/n”	

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.

3 Subject to SC 27 approval by a 60-day balloting (see SC 27 N5983) and subsequent JTC 1 endorsement of the renumbering from 18028 to 27033.

[MB¹] US NB comments on ISO/IEC 1st WD 27033-1³

Date: 2007-MM-DD	Document: SC 27 N5908
------------------	------------------------------

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
[US] 34	16.1.3	Paragraph 1	T	NAT is not viewed as a security feature.	Delete "configure devices with private IP addresses."	
[US] 35	16.2.2	Paragraph 1	T	Availability can also be effected if there is an intrusion.	Add "and availability" after "integrity" in the first bullet.	
[US] 36	16.2.3	Paragraph 1	T	Recommend adding a control discussing the use of an out of band network for management, or encryption to protect the traffic.	Add the following bullets: Out of band network management Encryption of network traffic.	

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.

3 Subject to SC 27 approval by a 60-day balloting (see SC 27 N5983) and subsequent JTC 1 endorsement of the renumbering from 18028 to 27033.

[MB¹] US NB comments on ISO/IEC 1st WD 27033-1³

Date: 2007-MM-DD	Document: SC 27 N5908
------------------	------------------------------

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.

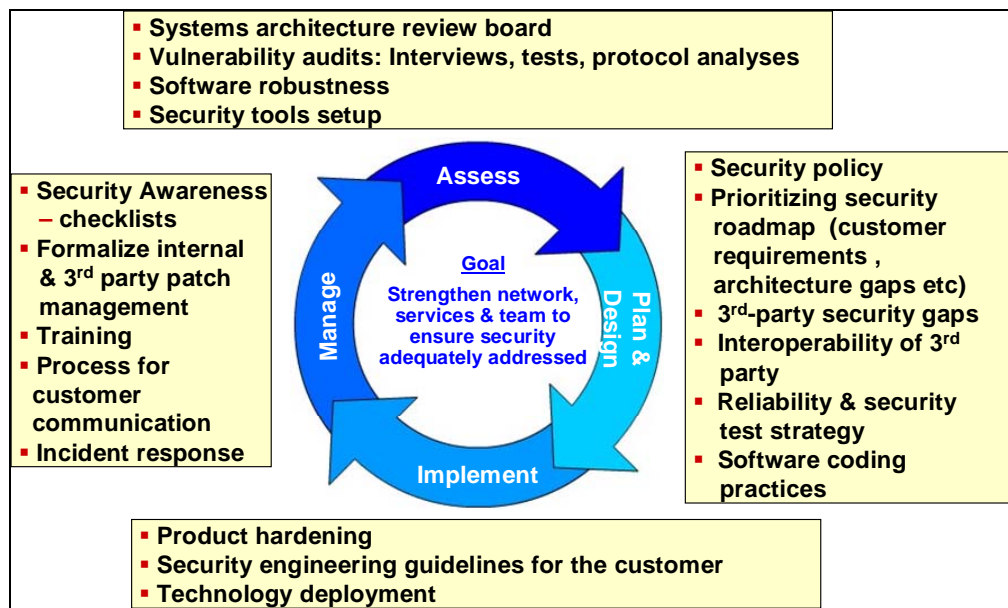
3 Subject to SC 27 approval by a 60-day balloting (see SC 27 N5983) and subsequent JTC 1 endorsement of the renumbering from 18028 to 27033.

Comments on ISO/IEC 1st WD 27033-1³

(3)	4	5	(6)	Res
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	Res on each

Attachment 1 for SC27N5908 Document

The PDCA model can be utilized to organize Part 1 to provide a context to the various sections which currently do not flow well in the draft. The content here is taken from existing ISMS documents and is primarily to illustrate a possible layout for Part 1 (Guidance on Network Security) which changes as appropriate.



Plan activities address the establishment of the information security management system and include:

- Definition of the information security management system coverage (e.g., location, assets, technology)
- Definition of an information security policy that reflects organizational needs
- Definition of a risk assessment methodology
- Identification and assessment of risks
- Identification and evaluation of options for the treatment of risks
- Selection of control objectives and controls
- Preparation of a statement of applicability (which gives the reasons for selection and exclusion of controls)

Do activities are concerned with the implementation and operation of the information security management system and include:

- Creation of plans to allocate responsibilities and priorities for risk treatment
- Implementation of controls
- Training and awareness programs
- Operations and resource management
- Procedures for detecting and reacting to incidents

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.

3 Subject to SC 27 approval by a 60-day balloting (see SC 27 N5983) and subsequent JTC 1 endorsement of the renumbering from 18028 to 27033.

Comments on ISO/IEC 1st WD 27033-1³

(3)	4	5	(6)	
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	Res on each

Check activities are concerned with monitoring and reviewing the information security management system and include:

- Execution of monitoring and other control procedures
- Reviews of information security management system effectiveness
- Reviews of residual risks and acceptable risks

Act activities are concerned with maintaining and improving the information security management system and include:

- Implementing improvements (including taking corrective and preventive actions to eliminate the cause of nonconformities and guard against future nonconformities)
- Learning from experiences (one's own and those of other organizations)
- Ensuring that improvements meet the objectives

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.

³ Subject to SC 27 approval by a 60-day balloting (see SC 27 N5983) and subsequent JTC 1 endorsement of the renumbering from 18028 to 27033.