



ISO/IEC JTC 1/SC 27 **N8779**

ISO/IEC JTC 1/SC 27/WG 3 **N8779**

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC. TYPE: dispositions of comments

TITLE: Dispositions of comments on ISO/IEC 4th WD 29147 (SC 27 N 8779)
Information technology – Security techniques – Responsible vulnerability disclosure

SOURCE: 40th SC 27/WG 3 meeting

DATE: 2010-04-23

PROJECT: 1.27.65 (29147)

STATUS: Output document of the editing session for 4th WD 29147 (SC 27 N 8779) held during the 40th SC 27/WG 3 meeting Melaka, Malaysia, April 19 – 23, 2010.

This document was available at the above-mentioned meeting. It is being circulated for information.

ACTION: FYI

DUE DATE:

DISTRIBUTION: P-, O-, and L- Members
W. Fumy, SC 27 Chairman, M. De Soete, SC 27 Vice Chair
E. Humphreys, K. Naemura, M. Ohlin, M.C. Kang, K. Rannenbergh, WG-
Conveners

MEDIUM: Server

NO. OF PAGES: 1 + 62

Attachment 1 to SC 27 N8672
[FI] comments on ISO/IEC 4th WD 29147

Date: 2010-03-12	Document: SC 27 N8126
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of com² ment	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.

Attachment 1 to SC 27 N8779
NB comments on ISO/IEC 4th WD 29147

Date: 2010-04-22	Document: SC 27 N8779
------------------	------------------------------

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
[BE] 1	Introduction	para 1	Te	Replace the first sentence with the following text to maintain consistency with the rest of the document	A vulnerability is defined as a set of conditions that can cause security incidents to be the origin of denial of service, unauthorized access, theft or destruction of information	Accept in Principle see US 19 & 20.
[BE] 2	Introduction	Para 2	Te	Vulnerabilities are not limited to mission critical information systems	Remove "mission critical"	Not Accepted as the editor had interpreted this comment to reference the incorrect editing in the previous DoC see US 4
[BE] 3	Terms and definitions	3.1	Te	"Supplier" is nowhere else used in the document	Replace supplier by vendor	Accept remove term also see ZA 6
[BE] 4	Terms and definitions	3.7	Te	Update refers too much to software code changes	Replace update with remediation and use this in the rest of the document	Accept to replace update with remediation.
[BE] 5	Terms and definitions	3.9	Te	This definition must be consistent with the definition in the Introduction	Replace with definition in the introduction	Accept in principle see US 19.
[BE] 6	4		Te	Referring to one specific CERT organisations is not required	Remove JPCERT	Accept in principle refer to UK 8
[BE] 7	6	2 Verification	Te	Reproducing is too vague	Replace with "The vendor, in possible cooperation with the finder, attempts to verify the existence and conditions of the vulnerability"	Accept in principle update 2.a to be "The vendor, in possible co-operation with the finder, attempts to verify the submitted issue is a security vulnerability."
[BE] 8	7	Bullet 1	ed		Replace "This can be range from .." by "This can be (not exclusively) an e-mail address, a toll free telephone number, .."	Not accepted Editors Note: The editor asks that a justification for the change be included
[BE] 9	7	Bullet 1	ed	Level is rather confusing	Replace "All vendors do not have the same level" by "Not all vendors have similar communication policies and	Accept with modification update sentence to be "All vendors do not have the same resources and should write

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.

Attachment 1 to SC 27 N8779
NB comments on ISO/IEC 4th WD 29147

Date: 2010-04-22	Document: SC 27 N8779
------------------	------------------------------

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
					capabilities and should write this section appropriately"	this section to match these capabilities."
[BE] 10	7	Bullet 3	te	The finder must provide to the vendor as much information as possible for the vendor to be able to verify the vulnerability and develop a remediation plan		Not accepted. The editor requests that a desired action be included as we could not determine what was the desired outcome.
[BE] 11	Annex B	B.1 par 2	te	It is confusing to speak about "Reporting"	Replace "Reporting" by "Disclosure"	Not Accepted see JP 69
[BE] 12	Annex B	B.1	te	It is confusing to start speaking about Incidents. Unfortunately, a lot of vendors are using terms like CSIRT, PSIRT etc ... to also indicate the internal organisation that deal with vulnerability management, while the I stands for Incidents. Can we come to a redefinition of the I ? I've seen several disclosure policies where Incidents and Vulnerabilities are intermixt.	Replace the meaning of I (Incident) by Issue. Or can we go a step further and replace SIRT by SERT with E = Emergency?	Accept SERT with E = Emergency
[BE] 13	Annex B	B.1	te		Rewrite this section by avoiding the use of Incident and include good elements from section B.3	Accept in principle see JP 69
[BE] 14	Annex B	B.3	ed	The added value of this section is low if B.1 is made more complete and detailed	Remove this section and use good elements in B.1	Accept in principle see JP 69
[BE] 15	Annex B	B.5	ed	This document aims at providing good practices and should not contain bad examples.	Remove this section	Accept in principle see US 58 Editor Note: Editor will remove aspects of trademark names including links but creating references of what not to do are good aspects to avoid
[CA] 1.				The document contains sufficient technical detail to be progressed to CD.	Progress the document to CD.	Accept Editors Note: After much debate

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.

Attachment 1 to SC 27 N8779
NB comments on ISO/IEC 4th WD 29147

Date: 2010-04-22	Document: SC 27 N8779
------------------	------------------------------

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
						from NB's and experts it was decided to progress the document to CD.
[CA] 2.	Title		Ge	The current use of the word "responsible" gives the impression that using a method other than described is irresponsible.	Change the current title to become "Vulnerability Disclosure"	Accept Editors Note: We will require a plenary item to vote for approval of the title change.
[CA] 3.	6	1	Ge	A finder, in a large % of cases, successfully exploits the vulnerability, herein making the Verification phase by the Vendor a reciprocal action. It is understood that a vendor would like to confirm a reported vulnerability, but it should be noted that the previous phase might already provide factual evidence. Vulnerability does not always mean immediate exploitability. Some vulnerability were unexploitable (ergo, unfixed) for a long time, until new exploitation techniques were published/discovered.	Add the following sentence to bullet b in list: "This includes supporting details of the exploit, when possible. To aid in the vulnerability resolution."	Accept in principle. Based on updates to section 7 list item 3 determine this is required or if information in annex is sufficient.
[CA] 4.	6	3c	Ge	It's a well-known fact that fixes sometimes disrupt other critical pieces of software, or modify an expected behaviour, etc. This should be mentioned or taken into account accordingly.	Add the following sentence to bullet c in list: "Testing should include sufficient depth to ensure that other applications will not be affected by the update."	Accept in principle update the new sentence to be "The vendor should attempt to ensure the remediation does not introduce new vulnerabilities".
[CA] 5.	7	2	Ed	Require a statement that addresses follow-up communications.	Add the following sentence: "Vendor should provide regular updates to the finder using the agreed method of communication."	Accept with modification the following will be appended to the provided sentence "and update frequency".
[CA] 6.	7		Ed	Add a new minimum for finder recognition	Add bullet 6 with the following: "Vendor should recognize the contributions of the finder(s) who helped in the discovery or resolution to the vulnerability discovered."	Accept add this a new section 5 titled "Vendor Credit for Finder"
[CA] 7.	8.3	Paragraph 2	Ed	OpenPGP technology should be mentioned	Modify the final sentence of the to be as follows:	Accept sentence as provided. Editors Note: Determine if PGP is a registered

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.

Attachment 1 to SC 27 N8779
NB comments on ISO/IEC 4th WD 29147

Date: 2010-04-22	Document: SC 27 N8779
------------------	------------------------------

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
					"Pre-disclosure e-mail messages with details shall be protected by mutually agreed encryption mechanisms such as PGP or OpenPGP."	trademark name and identify appropriately.
[CA] 8.	9	Paragraph 1	Ed	Require a statement that references the use of mailing lists.	Add the following sentence where appropriate. "Vendor should create a mailing-list that interested parties can subscribe to. This would include adding the necessary links on vendor web site and posted policy."	Accepted
[CA] 9.	9	2	Ed	Paragraph 9.2 Issues that Affect Multiple Vendors should be numbered 9.3	Update numbering to reflect 9.3	Accept see JP 65
[CA] 10.	Annex A	1	Ed	last item in list "For online service vulnerabilities, input required to reproduce the vulnerability". Requires more details other than the service	Update to add the following: Not only service vulnerabilities but the receive INPUT	Accept
[CA] 11.	Annex A	2	Ed	Clarifying information should be included in the description if the vulnerability could easily be confused with a prior advisory, especially for products with a long advisories history.	Add the following sentence: "When possible, the software revision, patch ID, fix number, date, etc should be included to ensure the specific software has been correctly indentified to the end user."	Accept
FI 1	Whole document		ge	The document needs a thorough read through to correct typos and inconsistencies on e.g. font sizes of section titles.		Accept - will update accordingly
FI 2	3.2	Term "Coordinator"	ed	"coordinator: person or organization that serves as a proxy between the supplier and the finder". Supplier is not defined in the document, and it is the only occurrence of the term. The presumption is that this is a relic from an earlier draft and is meant to be "vendor", not "supplier".	Change "supplier" to "vendor"	Not accepted see ZA 6

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.

Attachment 1 to SC 27 N8779
NB comments on ISO/IEC 4th WD 29147

Date: 2010-04-22	Document: SC 27 N8779
------------------	------------------------------

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
FI 3	4 Abbreviated terms	Clause title	ed	Typo: Abbreviated terms)	Remove the parenthesis	Accept see UK 7
FI 4	4 Abbreviated terms		te	JPCERT is included for some reason, even though CERT is already a defined term. There are other CERTS, like USCERT, KRCERT, CERT-FI, etc. but they are not all defined. Therefore why is JPCERT specifically included in the document?	Remove definition of JPCERT.	Accept in principle refer to UK 8
FI 5	7	First paragraph	te	“Vendors shall define their responsibilities in the vulnerability handling policy.” Comment: Responsible vendors will have a reasonably well defined internal operating procedure for vulnerability and incident response; that’s where the details of roles, responsibilities and operational procedures belong. Therefore, the ISO-RVD should not expect vendors to have *detailed* operating procedures for vulnerability response on the company’s public portal, as that statement in the draft 4, as worded, can be misconstrued. The anticipation would be that a broad yet clear statement of due diligence should suffice, in conjunction with contact details as an input channel from customer to	Change the start of the clause to: “Vendors shall define their responsibilities in the vulnerability handling policy. For an example, see the internet draft on RVD process (http://tools.ietf.org/draft/draft-christeywysopal-vuln-disclosure/draft-christeywysopal-vuln-disclosure-00.txt). A policy shall state the intentions of the vendor as it relates to vulnerability reporting. This might include contact information, timelines, communications channels, etc. It can be as open as the vendor is willing to operate. The vendor may choose not to have a detailed	Accept in principle. See JP 2 for the removal of ietf draft reference. Will add the following sentence after sentence 3. "The vendor may choose not to have a detailed internal operational policy on the company's public portal."

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.

Attachment 1 to SC 27 N8779
NB comments on ISO/IEC 4th WD 29147

Date: 2010-04-22	Document: SC 27 N8779
------------------	------------------------------

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
				vendor.	vulnerability/incident handling policy on the company's public portal. Several examples are listed in Annex B.1 Sample Vulnerability Reporting Policy. A vulnerability policy may include information about the following:"	
FI 6	7	1. How the vendor would like to be contacted	Ed	Typo: "This can be range from e-mail to toll free telephone numbers"	Remove "be" → "This can range from e-mail to toll..."	Accept will remove "be" from sentence
FI 7	8	Whole clause	ed	The title and the text are inconsistent. The title is about receipt, the text discusses about the policy altogether and about communication between the finder and the vendor	Change the title to "Communication between the finder and the vendor" or something similar.	Accept in principle see JP 28
FI 8	8	First paragraph	ed	First and third sentence are equal ("This clause discusses considerations...")	Remove the first sentence	Not accepted see JP 33
FI 9	8	First paragraph	ed	The paragraph says that the clause discusses considerations to be taken into account when creating a policy, not about receipt of vulnerability information. Thus it should be moved to Clause 7	Move the paragraph to Clause 7.	Accept in principle see JP 33
FI 10	8.1	Whole Section	ed	The section should be a subsection in Clause 7 Vulnerability Handling policy	Move the section to Clause 7	Accept to move this to section 7 as a new list item 1.
FI 11	8.3	Second paragraph	te	"If situations where further information is required by the vendor the finder shall be willing to provide this information" This should of course be conditional on the	Change "shall" to "should"	Accept change of "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.

Attachment 1 to SC 27 N8779
NB comments on ISO/IEC 4th WD 29147

Date: 2010-04-22	Document: SC 27 N8779
------------------	------------------------------

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
				nature and circumstances of the specific issue; it may not always be possible to provide additional information to the finder/requester.		
FI 12	8.3	Second paragraph	te	“Pre-disclosure e-mail messages with details shall be protected by mutually agreed encryption...” It should be up to the vendor to decide if they want to use protected communication.	Change to “Pre-disclosure e-mail messages with details should be protected by mutually agreed encryption mechanisms such as PGP if decided by vendor. The system should be set up to support encryption.”	Accept as the last sentence "It is recommended that a vendor setup encryption capabilities prior to communication with finders."
FI 13	8.4	Last sentence	ed	An extra quotation mark at the end	Remove “	Accept
FI 14	8.4	Whole Section	ed	Assigning a unique identifier should be handled in Clause 7 (handling policy)	Move Section 8.4 to Clause 7	Accept will move current section 8.4 to paragraph in 7.3
FI 15	Annex B	Responding to Customer Incidents	te	<p>“However, final decision-making regarding how incidents are handled remains with the customer and/or end user of the product and/or service.”</p> <p>This requires some clarification, because a vendor’s internal vulnerability/incident handling procedure would in practice dictate how incidents are handled (as per the lifecycle model). The current formulation seems to read that (whether intentionally or unintentionally) that the customer/end user can override the internal RVD procedure/policy of the company.</p> <p>It also seems to conflict with the next statement after that - “<Company name> reserves the right to determine the type and degree of assistance it may offer in connection with any incident, and to withdraw from any incident at</p>	<p>Change the paragraph to:</p> <p><Company name> plays a supporting role in responding to customer security incidents, offering technical support and expertise.</p> <p><Company name> shall reserve all rights in how vulnerabilities and incidents that are reported are handled, and in determining the type and degree of assistance it offers in connection with any vulnerability or incident.</p> <p><Company name> reserves the right to</p>	Accept Editors Note: Will update to reflect content provided

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 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><i>any time.</i>"</p> <p>The expectation would be that, in accordance with the company's RVD standard operating procedure, the company exercises due diligence in recording and handling the reported issue, and retains the rights thereafter on how the issue is dealt with, of course with the expected acknowledgement to the customer/end user and consequent follow-ups.</p> <p>However, final decision-making regarding how incidents are handled, once reported by the customer/end user, shall remain with the vendor of the product and/or service, who shall strive with due diligence and in accordance with the company's internal response procedures to resolve the reported incident on behalf of the customer/end user.</p>	determine the type and degree of assistance it may offer in connection with any incident, and to withdraw from any incident at any time. <Company Name> may give special consideration to security incidents that involve actual or potential threats to persons, property, or the Internet, as well as requests from law enforcement agencies or formal incident response teams.	
JP 1.	Table of Contents		ed	<p>The following items are missing:</p> <ul style="list-style-type: none"> ● Clause 6 Life Cycle of a Vulnerability ● A.1 Receiving Vulnerability Information ● B.3 Vulnerability Reporting Form Examples ● B.4 Advisory Examples 	The table of contents should be updated in accordance with the current document.	Accept - Will update the ToC accordingly
JP 2.	Introduction	5 th paragraph	ed	<p>Reference 15 is missing in the bibliography</p> <p>Reference 15 means the internet draft on RVD process (see JP10 on SC27N8127). However, Internet-Drafts have no formal status, and are subject to change or removal at any time; therefore they should not be cited or quoted in any formal document. (See http://www.ietf.org/id-info/)</p>	Delete the subordinate clause "As defined by reference 15 in the bibliography."	Accept - will remove the reference to Bibliography entry 3.
JP 3.	1	2 nd paragraph 3 rd paragraph	ed	<p>The two paragraphs try to define "vendors" in deferent ways, which makes them felt a little contradictory. The former one should mention the variety of products but not of vendors.</p>	The 2 nd paragraph should be moved after the 3 rd paragraph and changed as follows:	Accept will change accordingly.

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.

Attachment 1 to SC 27 N8779
NB comments on ISO/IEC 4th WD 29147

Date: 2010-04-22	Document: SC 27 N8779
------------------	------------------------------

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
					Products can include software, hardware, application services, and online /web application	
JP 4.	3.1		ge, te	The definition is not appropriate, since it can't replace the defined term "advisory" in context. See D.1.5.3 in Annex of ISO/IEC Directives, Part.	Rewrite the definition. A candidate definition is: announcement or bulletin that serves to inform, advise and usually warn users about a vulnerability of a product	Accept will update the current definition to the one proposed by JP and add the NOTES per US 10.
JP 5.	3.2		ge	"Supplier" is an undefined term, and it seems to mean "vendor."	Add definition of "supplier" or replace "supplier" with "vendor."	Accept in Principle use vendor not supplier
JP 6.	3.4		te	The definition is not appropriate.	Rewrite the definition. A candidate definition is: goods and/or services that a vendor makes available in its entirety	Not Accepted see UK 5
JP 7.	3.5		te	The definition is of "online service providers" but not of "online services."	Rewrite the definition. A candidate definition is: computer communication service in which users could access various services and information resources such a bulletin boards, downloadable files and programs, news articles, chat rooms, and electronic mail services	Accept with modifications "service which is implemented by hardware, software or a combination of them, and provided over a communication line or network".
JP 8.	3.4 3.5		ed	They are out of an alphabetical order.	Sort them in an alphabetical order.	Accept see US 13
JP 9.	3.6		ge	It is our consensus at the Redmond meeting that the term will be deleted. See the resolution of JP 20 in SC27	Delete the term.	Accept

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.

Attachment 1 to SC 27 N8779
NB comments on ISO/IEC 4th WD 29147

Date: 2010-04-22	Document: SC 27 N8779
------------------	------------------------------

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
				N8127.		
JP 10.	3.8		ed	Definition shall not be followed by a full-stop. See D.3.2 in Annex of ISO/IEC Directives, Part.	Remove the full-stop.	Accept will remove "."
JP 11.	4		ed	The parenthesis ")" at the end of the clause title is a typo.	Delete the left parentheses ")" from the title.	Accept
JP 12.	4	CC	ed, te	The term "CC" meaning "common criteria" is not used elsewhere in this document.	Delete the term or change the definition as follows: coordination center	Accepted will remove reference to CC
JP 13.	4	CERT JPCERT IPA	ge	Proprietary trade names (i.e. trade marks) for a particular product should as far as possible be avoided, even if they are in common use. If exceptionally, trade names cannot be avoided, their nature shall be indicated, e.g. by the symbol ® for a registered trade mark. (See 6.6.3 in ISO/IEC Directives, Part 2.)	Indicate their nature by the trade mark symbol (®) and move them to somewhere in the annex (informative), or delete them.	Accept in Principle will remove references to both IPA, CERT, JPCERT.
JP 14.	4	SIRT	ge	In the community, CSIRT is a more widely used term than SIRT.	Replace SIRT with CSIRT, which stands for Computer Security Incident Response Team.	Accept with modifications. SIRT to be removed and CSIRT to be reference based on UK 8.
JP 15.	5	3 rd paragraph	ed	The ditto mark (") at the end of the 3rd bullet subclause is a typo.	Remove the ditto mark (").	Accept
JP 16.	5	4 th paragraph	ed	The ditto mark (") at the end of the paragraph is a typo.	Remove the ditto mark (").	Accept
JP 17.	6	Figure	ed	Figures shall be designated "Figure" and numbered with Arabic numerals, beginning with 1. (Refer to 6.6.5.3 in ISO/IEC Directives, Part 2.)	Give it a figure designation and a title as follows: Figure 1. A Model of Vulnerability Handling by vendors	Accept will add designation and title.
JP 18.	6	2 nd paragraph	ed	Each item in a list shall be preceded by a dash or bullet or, if necessary for identification, by a lower case letter followed by a parenthesis. If it is necessary to subdivide further an item in the latter type of list, Arabic numerals	Reform the list as follows: a) Discovery Phase 1) Discovery: ...	Accepted will update as indicated.

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.

Attachment 1 to SC 27 N8779
NB comments on ISO/IEC 4th WD 29147

Date: 2010-04-22	Document: SC 27 N8779
------------------	------------------------------

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
				followed by a parenthesis shall be used. (See 5.2.5 in ISO/IEC Directives, Part 2.)	2) Notification: ... 3) Acknowledgement: ... b) Verification Phase 1) Initial Investigation: ... 2)	
JP 19.	6	1.b.	ge	It should be described from the viewpoint of vendors in the sense of an introduction to the main part from clause 7 to 9.	Modify it as follows: b. Notification: The vendor is notified of the potential vulnerability either directly by the finder or through a coordinator.	Accept will update the bullet accordingly and add the following sentence "In some instances this might include a user provided malware sample for analysis." Add the following new definition Proposed definition of the term "malware" by the US NB: "malware software designed to infiltrate a computer system without the computer owner's informed consent NOTE 1 This definition was adapted from Wikipedia http://en.wikipedia.org/wiki/Malware . NOTE 2 The term originated from the combination of two words "malicious" and "software". NOTE 3 The term is a general term used by computer professionals to

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 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
						mean a variety of forms of damaging, intrusive, or annoying software or program code. EXAMPLE A maliciously crafted document that contains hidden vulnerability exploit code would be called malware."
JP 20.	6	1	te	In the discovery phase, vendors investigate whether the reported issue should be confirmed as vulnerability, for which a vulnerability handling process should be initiated, before acknowledging receipt of the report. If it is not the case, it would be handled as an ordinal potential malfunction rather than a potential vulnerability. The above mentioned investigation should be called "initial investigation" rather than reproduction in the verification phase.	Add the following item between 1.b and 1.c: (new)c. Initial investigation: Vendors investigate the reported issue and decide whether they confirm it as vulnerability and initiate the vulnerability handling process for it. Change the title of 2.a into "Reproduction."	Accept in principle. 1.c to be updated to be "Vendor communicates to the finder that they have received the submitted vulnerability report." The title change will NOT be implemented.
JP 21.	6	2.b 2.c	te	When the vulnerability is caused by malfunction of an underlying or embedded module which another vendor has developed, it should be reported to the vendor if the malfunction is believed to be vulnerability.	Add the following description at the end of 2.b or 2.c: If it is caused by a vulnerability of an underlying or embedded modules which another vendor has developed, it should be reported to the vendor directly or through a coordinator.	Accepted will be appended to current 2.b.
JP 22.	6	3	te	The development and the installation of resolution, i.e. production system update, should be clearly separated. The later should be moved to next phase. This phase should be called "Resolution Development Phase" rather than "Resolution Phase."	Replace "Resolution Phase" with "Resolution Development Phase." Move 3.d into next phase. See also	Accept "Resolution Development Phase". Update the figure in this section to reflect this change. Move 3.d to next phase.

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.

Attachment 1 to SC 27 N8779
NB comments on ISO/IEC 4th WD 29147

Date: 2010-04-22	Document: SC 27 N8779
------------------	------------------------------

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
					JP23.	
JP 23.	6	4	te	Taking account of production system update for online services, "Advisory Phase" may not be an appropriate name.	Replace "Advisory Phase" with "Advisory and Resolution Phase."	Accept in principle Editors Note: Update to "Release Phase"
JP 24.	6	5	ge	Since the phase doesn't seem to have few actions except reactive ones, there is no need to be an independent phase.	The phase should be merged with the Advisory phase.	Not accepted see JP 22
JP 25.	6	5.a	ed	The term "closure" contradicts the following description, which says son-and-so might continue.	Replace "Case Closure" with "Case Maintenance."	Accepted will be updated to "Case Maintenance"
JP 26.	7	1 st paragraph	ge	The most important thing about the policy is missing, which is publication.	Modify the 1 st statement as follows: Vendor publicize their vulnerability handling policy in a manner for a potential user to be able to check it.	Accept with modification "Vendor should publicize their vulnerability handling policy or point to an existing public vulnerability handling policy.
JP 27.	7	1 st paragraph	ge	Internet-Drafts have no formal status, and are subject to change or removal at any time; therefore they should not be cited or quoted in any formal document. (See http://www.ietf.org/id-info/)	Delete the 2 nd statement.	Accept quote to be removed
JP 28.	7	1 st paragraph	ed	The title of annex B.1 in the last sentence contradicts with the name of annex B.1 which is referred. See also JP69.	Change both or one of the titles to avoid the contradiction.	Accept will change will be updated to point to "B.1 Sample Vulnerability Disclosure"
JP 29.	7	2 nd paragraph	ed	Each item in a list shall be preceded by a dash or bullet or, if necessary for identification, by a lower case letter followed by a parenthesis. (See 5.2.5 in ISO/IEC Directives, Part 2.)	Reform the list as follows: a) How the vendor would like to be contacted b) Expected responses	Accept will update the list to current Directives.

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.

Attachment 1 to SC 27 N8779
NB comments on ISO/IEC 4th WD 29147

Date: 2010-04-22	Document: SC 27 N8779
------------------	------------------------------

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
					
JP 30.	7	3 rd list item of 2 nd paragraph	ed	The "Finder" with upper case F should be "finder" in lower case.	Change "Finder(s)" into "finder(s)."	Accept will update as requested
JP 31.	7	4 th list item of 2 nd paragraph	ed	The four word string "Sanction against legal action" as a title should be independent form the following part.	Feed a line immediately after it as follows: 4. Sanction against legal action Vendors should declare	Accept
JP 32.	7	5 th list item of 2 nd paragraph	ge, te	The JP national body doesn't believe this item has to be included in any vulnerability handling policies because the subject is too special. The topic can be discussed elsewhere such as in clause 9 for disseminating of vulnerability information, which seems more appropriate. See also JP61.	Delete it.	Accept remove section 6. {determine best location where the concepts might be moved to in the document 7 1st para}
JP 33.	8	1 st paragraph	ed	"Hanging paragraphs" shall be avoided since reference to them is ambiguous. (See 5.2.4 in ISO/IEC Directives, Part 2.)	Delete it or rewrite it as follows: 8.1 General This clause presents a guideline for vendors to receive information on potential vulnerability from either a finder or a coordinator.	Accept will add the new sub clause and sentence. Remove the 1st hanging paragraph.
JP 34.	8	1 st paragraph	ge	Because all the actions for receipt of vulnerability information are not necessarily described in the vulnerability handling policy, this clause should be independent from clause 7 for the policy.	Delete it. See also JP33.	Accept see JP 33
JP 35.	8.1		ed	Policy should not be discussed in this clause.	Delete it or move it into somewhere in the clause 7.	Not accept see FI 10

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.

Attachment 1 to SC 27 N8779
NB comments on ISO/IEC 4th WD 29147

Date: 2010-04-22	Document: SC 27 N8779
------------------	------------------------------

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
JP 36.	8.2		te	Clarification of a window receiving vulnerability information should come at first rather than its security model.	Change the subclause or introduce a new subclause for a window receiving vulnerability. A candidate description of the new subclause is: 8.x Contact window Vendors should be clarify a window where information of potential vulnerability is received for each their product throughout its lifecycle. A single window for all the products is preferable.	Accept the sentence will be added to current section 8.5 after 1st paragraph.
JP 37.	8		te	It is a very important step, which is completely missing in the 4 th WD, for vendors to inspect reported potential vulnerability information, decide whether it should be handled as vulnerability, and then open a case if it is the case. Although it is an internal process which is out of scope of this IS, it is essential since results of the decision influence the way how to respond to the reporter (finder or coordinator). See also JP38.	Introduce a new subclause. A candidate description of the new subclause is: 8.x Confirmation of vulnerability Vendors should inspect the reported potential vulnerability information and decide whether it should be handled as vulnerability. If they decide so, they open a case.	Accept with a title of "Initial Investigation of Vulnerability". New clause possibly as 8.2
JP 38.	8		te	As a reverse case described in JP37, some issues reported as malfunctions may be vulnerabilities. It should be noted how vendors manage such cases.	Add the following statements to the new subclause proposed to insert by JP37: Vendors should check all bug reports, and initiate vulnerability handling if they find vulnerability in them.	Accept with the creation of a new clause 8.3 title of "Confirmation of Vulnerability"

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.

Attachment 1 to SC 27 N8779
NB comments on ISO/IEC 4th WD 29147

Date: 2010-04-22	Document: SC 27 N8779
------------------	------------------------------

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
JP 39.	8.3	2 nd paragraph	ed	The paragraph is not appropriate in subclause 8.3.	Move it into either somewhere in clause 7 or the new subclause which JP36 proposes to introduce.	Accept in principle see JP 36
JP 40.	8.3	3 rd paragraph	ed	The paragraph is not appropriate in subclause 8.3.	Move it into the new subclause which JP36 proposes to introduce.	Review after section rebuild
JP 41.	8.4		te	The most important thing is not assigning an identifier but opening a case of vulnerability handling.	Modify the title of the subclause into "Opening a Vulnerability Handling Case."	Accepted Editors Note: Add some text to add the distinction between an internal vs. external identifier assigned by coordinator
JP 42.	8.3 8.4		ed	Acknowledgement of receipt described in clause 8.3 should be issued with some identification described in clause 8.4.	Change the order of the two subclauses.	Not accepted see JP 37
JP 43.	8.4		te	Because CVE identifies vulnerable "implementation," it can't be assigned at this stage.	Delete the last sentence mentioning CVE.	Accept in Principle Editors Note: See JP 41 as a CVE is known industry identifier.
JP 44.	8.3	1 st paragraph	te	The case should also be mentioned that a vendor has already started handling the reported case as vulnerability based on other reports or findings by themselves.	The 1 st statement should be replaced with the following: The vendor should issue a receipt to the finder or coordinator when they decide to start handling the case as vulnerability or have already started handling the case.	Accept with modification current 8.3 remove "and assigning an internal tracking number." from the 1st sentence. Move the 1st sentence of the 2nd paragraph to the end of the 1st paragraph. Then add a new 2nd paragraph with the following "In the case, where a finder reports a vulnerability that has already been discovered. The vendor should communicate to the finder this is a duplicate issue.
JP 45.	8.3	1 st	te	The case should also be mentioned that a vendor possibly decides it will not handle the reported case as	The following paragraph should be added after the 1 st paragraph:	Accept append as point under 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.

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
		paragraph		vulnerability.	The vendor should inform the finder or coordinator of it with rational reasons when they decide not to handle the case as vulnerability.	section referenced in JP 37.
JP 46.	8.5		ed	While recommended vendor actions for receipt of vulnerability information should be listed in clause 8, this clause does not describe an action.	Move either somewhere in clause 7 or the new subclause proposed to insert by JP36.	Accepted in principle will seek to align this to over all restructuring of section 8
JP 47.	8.6		te, ed	Considering that correspondence between a finder and vendor often goes back and forth several times, it seems peculiar for this subclause description to be placed here.	Move this subclause description into subclause 8.3.	Accepted Editors Note: Move this subclause to section "Acknowledgement of receipt from finder"
JP 48.	8.7		ge	Not only because it is out of scope of this IS to define the role of coordinators but also because clause 8 should describes a guideline for vendors to receive vulnerability information, the title and some contents of this subclause is not appropriate.	Change the subclause title into "Support from coordinators", "Possible help by coordinators" or something like those.	Accept with modification Editors Note: Will change title name to "Support from Co-coordinators"
JP 49.	8.7	1st ^d paragraph	ed	There is a typo in the 4 th line: vender.	Replace it with "vendor."	Accepted
JP 50.	8.7	3 rd paragraph	ge	For the same reason as JP47, it is not appropriate.	Delete it.	Accepted as the coordinator role is out of scope of this document.
JP 51.	8		te	It should also be mentioned that vendors try to gather information to prioritize the vulnerability case.	Introduce such a new subclause as follows: 8.x Prioritization Vendors should prioritize the vulnerability for handling appropriately based on information gathered so far. The following list includes items which may be considered to decide the prioritization:	Accept as new section 8.4. JP to provide content to guide a vendor for each of these points.

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 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
					<ul style="list-style-type: none"> Finder's agenda to publicize the vulnerability Population with the knowledge about the vulnerability Nature of possible attacks Existence and maturity of exploit codes Estimated probability of successful exploit Nature of potential damage caused by attack 	
JP 52.	8		te	It should also be mentioned how vendors communicate with a finder or a coordinator when they can't reproduce the vulnerability in their test bed.	Introduce such a new subclause as follows: 8.x Communication for Reproduction Vendors may possibly fail to reproduce the vulnerability in their test environment based on the information initially reported by the finder. In such a case, vendor should cooperate with the finder in order to clarify what brings the difference and ask him/her to do so paying their respects. Vendors can make the communication by asking a finder about their environment with standard vulnerability reporting form such as ones shown in Annex B.3.	Accept as new section 8.4 replace with the following: "8.x Communication for Reproduction Vendors may possibly fail to reproduce the vulnerability in their test environment based on the information initially reported by the finder. In such a case, the vendor should ask if the finder can produce further evidence that the issue is a security vulnerability. Vendors should ask the finder about their environment using a standard vulnerability reporting form such as ones shown in Annex B.3.
JP 53.	8		te	It should also be mentioned that it is important for vendors to maintain a relationship of mutual trust with a finder or a coordinator.	Introduce such a new subclause as follows: 8.x Mutual Trust Maintenance with a Finder or a Coordinator	Accept with modification update title to "Relationship Management with a Finder and/or Coordinator". Update content as follows: "It is very important for vendors to maintain a good

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.

Attachment 1 to SC 27 N8779
NB comments on ISO/IEC 4th WD 29147

Date: 2010-04-22	Document: SC 27 N8779
------------------	------------------------------

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
					It is very important for vendors to maintain a good relationship of mutual trust with a finder or a coordinator, especially in the case that it takes long time to finish to handle the vulnerability. Vendors should keep track of each vulnerability case status so that they can timely reply to inquiry from the finder or the coordinator. Vendors had better inform them about the major status change of the case, if it may possibly impact them.	relationship of mutual trust with a finder or a coordinator, especially in the case that it takes long time to handle the vulnerability. Vendors should keep track of each vulnerability case status so that they can provide a timely reply to inquiries from the finder or the coordinator. Vendors should inform them about major case status changes, as this may impact finder or coordinator timelines."
JP 54.	9		ed	The clause number should be 9 but 9.0.	Replace 9.0 with 9.	Accept
JP 55.	9		ge	In order to develop resolution, vendors sometimes have to share reported vulnerability information with other parties, for example with other vendors who developed an imported module causing the vulnerability as their product. It is our consensus at the Kyoto meeting that such information sharing should be included in dissemination of vulnerability information. However, 4 th WD is not the case. Since dissemination of advisory is very different from dissemination of vulnerability information in nature, it seems that we had better make a new independent clause for the latter.	Change the title of clause 9 into "Disseminating of Advisory", and ahead of it, insert a new clause with the title "Disseminating (or Sharing) of Vulnerability Information" for sharing vulnerability information with other vendors and coordinators in the phase of resolution development.	Accept Editors Note: Will add a new section and rename the current section title
JP 56.	9	1 st paragraph	ed	"Hanging paragraphs" shall be avoided since reference to them is ambiguous. (See 5.2.4 in ISO/IEC Directives, Part 2.)	Change it into a subclause with the title " 8.1 General. "	Accept will update
JP 57.	9	1 st paragraph	ed	The "Vendor" with upper case V should be "vendor" in lower case.	Change "Vendor(s)" into "vendor(s)" unless it appears at the begging of a sentence.	Accept

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 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
JP 58.	9	1 st paragraph	te	Because a CVE is assigned to an implementation causing vulnerability, two independent implementations can't have a common CVE even if they cause the same vulnerability in nature.	Delete the last sentence.	Accept Editors Note: Add new definitions for both "public disclosure" and "private customer notification".
JP 59.	9	1 st paragraph	ge	The two terms "public disclosure" and "private customer notification" may be interpreted in many ways depending on readers of this document. At least, it should be clarified which of them is described in this clause.	Please define the terms "public disclosure" and "private customer notification" and explain what the two have in common as well as in what aspects each of them is differentiated from another.	Accept will add this to the section
JP 60.	9	1 st paragraph	te	Some guidelines should be provided about the conditions in which public disclosure is recommended and the conditions in which private customer notification is.	Describe some criteria for the decision. The following description is an example: Public disclosure and/or private customer notification are/is chosen considering the following aspects of conditions: <ul style="list-style-type: none"> ● Shipping and user support scheme for the product. ● Availability of communication channels with which a vendor can rapidly and securely notify all the users of the product without omission. ● A period of estimated time which it takes to finish installing the resolution at each user site. ● Prevalence of activities exploiting the vulnerability. 	Accept will add this to the 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.

Attachment 1 to SC 27 N8779
NB comments on ISO/IEC 4th WD 29147

Date: 2010-04-22	Document: SC 27 N8779
------------------	------------------------------

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
JP 61.	9	1 st paragraph	te	It is described as if the timing of releasing advisories is affected only by whether the vulnerability is related to multiple vendors or not, which is not true. In order to choose an appropriate timing vendors have to take many conditions into account.	<p>Please elaborate on what conditions should be taken into account for choosing timing of advisory release in addition to whether the case is related to multiple vendors.</p> <p>The following items are some examples:</p> <ul style="list-style-type: none"> ● Readiness for customer support staff of call centers and sales divisions etc. ● Finder's agenda for publication ● Prevalence of activities exploiting the vulnerability 	Accept in principle Editors Note: This content to be added to section 9.2 appended to end
JP 62.	9.1	1st paragraph	ed	The "Advisory/Advisories" with upper case A should be "advisory/advisories" in lower case.	Change "Advisory/Advisories" into "advisory/advisories" unless it appears at the begging of a sentence.	Accept
JP 63.	9.1	2 nd paragraph	ed	The title of annex B.4 "Sample Advisories" in the last sentence is similar but different from the name of annex B.4 "Advisory Examples" which is referred.	Change both or one of the titles to make them exactly same.	Accept Editors Note: Make titles consistent
JP 64.	9.1		ge	<p>The title "Dissemination Formatting" of the subclause is not appropriate in the following sense:</p> <ul style="list-style-type: none"> ● The subject is advisories but not dissemination. <p>What should be discussed is contents but not format nor formatting.</p>	<ul style="list-style-type: none"> ● Change the title into "Contents of Advisories." 	Accept
JP 65.	9.2		ed	There are two subclauses numbered as 9.2.	Renumber the 2 nd one of subclause 9.2 as 9.3.	Accept

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.

Attachment 1 to SC 27 N8779
NB comments on ISO/IEC 4th WD 29147

Date: 2010-04-22	Document: SC 27 N8779
------------------	------------------------------

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
JP 66.	9.3 (or 2 nd 9.2)		te	The subject relating to issues that affect multiple vendors is more appropriate to be discussed in the new clause proposed to introduce by JP55.	Move it into the new clause proposed to introduce by JP55.	Accept Editors Note: This section to be moved to section JP55
JP 67.	B.1		ed	The title "Sample Vulnerability Disclosure" is not appropriate.	Change the title into "Sample of Vendor Policy," for example.	Accept in Principle Editors Note: Change to "Sample Vendor Reporting Policy". This would include removing the section title after the 1st paragraph.
JP 68.	B.1	All paragraphs after the 2 nd	ed	The type of contents should be clearly designated. The part should be displayed as other than ordinary text.	Convert the part into a figure or a sample by inserting "EZAPLE" immediately before the part or Figure #" at the bottom of the part with "Figure # (continued)" at the bottom of the page.	Accepted Editors Note: Will put this section into a "box"
JP 69.	B.1	2 nd paragraph	ed	The title " Security Vulnerability Reporting Policy " of the sample is not appropriate.	Change the title into "Security Vulnerability Handling Policy" or "Policy on Reported Security Vulnerability."	Not Accepted JP 67
JP 70.	B.3	7 th paragraph	ed	The 1 st sentence of the 7 th paragraph beginning with "Provide contact information" includes unnecessary long space between "information" and "about."	Make the long space appropriately short.	Accept
JP 71.	B.3		ed	The separation between the two examples should be clearer.	Separate it into two subclauses such as: B.3.1 CERT/CC Vulnerability Reporting Form and B.3.2 IPA and JPCERT/CC Vulnerability Reporting Form.	Accepted Editors Note: Will create two new section titles
JP 72.	B.6		ge	Since we have our lifecycle chart of vulnerability in clause 6, it doesn't seem to need its NIAC version any more. In addition to that, partial excerpt may be misleading.	Delete clause B.6.	Accepted Editors Note: Diagram to be removed.

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.

Attachment 3 to SC 27 N8672
[UK] comments on ISO/IEC 4th WD 29147

Date: 2010-03-10	Document: SC 27 N8126
------------------	------------------------------

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
UK 1	Introduction	para 2	Te	Replace the first sentence with the following text to maintain consistency with the rest of the text.	A vulnerability is defined as a set of conditions that leads or may lead to an implicit or explicit failure of the confidentiality, integrity, or availability of an information system.	Not Accepted as the US 4 references the change to the "introduction" section of the document.
UK 2	Introduction	para 5	Te	Remove the sentence "As defined by reference 15 in the bibliography, "The goals of responsible disclosure include:" and all seven bullets that follow it. Instead use the proposed text. Strictly speaking helping academia is not a goal. It is a fortunate consequence of the disclosure but not a goal.	<p>The goals of responsible disclosure include:</p> <ol style="list-style-type: none"> 1) Ensure that vulnerabilities can be identified and eliminated effectively and efficiently for all parties. 2) Minimize the risk to customers from vulnerabilities that could allow damage to their systems 3) Provide customers with sufficient information for them to assess the risk to their systems. 4) Minimise the amount of time and resources required to manage vulnerability information 5) Minimise the amount of antagonism that often exists between parties as a result of different assumptions and expectations, due to the lack of consistency and explicit disclosure process. 	Not accepted as this section is to be removed as per JP2 with details in US 4.

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 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
UK 3	3 Terms and definitions	3.1	Te	The sentence “An advisory may be published by a vendor, finder, or coordinator.” Can imply that only one of them can publish an advisory while, in reality, any of them can and, occasionally, do.	Remove “a” from the sentence to read “An advisory may be published by vendor, finder, or coordinator”	Not Accepted see JP 4.
UK 4	3 Terms and definitions	3.3 finder	te	Use definition from NIAC document	Finders include individuals or organizations that find vulnerabilities. Subgroups include researchers, security companies, users, governments, and coordinators.	Accept will update accordingly. Editor will check with SC7 to correct identification of this def. usage since it is verbatim from NIAC.
UK 5	3 Terms and definitions	3.4 product	Te	Product does not have to be commercial. Also, according to the Scope services are also included in this IS.	Replace the existing text with this “Item or service developed, manufactured or refined be it commercial or not.”	Accept with modifications will update definition to be "software, hardware, or online services developed, manufactured, or refined whether it is for sale or offered as free". Remove all current NOTE 1 & 2 only.
UK 6	3 Term and definitions	3.7	Te	Term “update” is overloaded and it not always clear are we talking about updated software of updating an advisory.	Use term “remedy” for software updates, fixes and configuration change. Make this change throughout the document.	Accept in principle see BE 4
UK 7	4 Abbreviated terms	Title	Ed	remove ‘)’ from the title		Accept will remove
UK 8	4 Abbreviated terms		Te	The list of abbreviated terms is not consistent. IPA and JPCERT are present but not CERT/CC. We also feel that listing organization names is not required.	Remove entries for IPA and JPCERT	Accept in principle to remove IPA, CERT and JPCERT based on rules of inclusion of abbreviated terms in body and/or annexes.
UK 9	5 Responsible vulnerable disclosure	second para	Te	“vulnerability handling” can be viewed as insufficient broad definition	Use “vulnerability management” instead. Make change throughout the document.	Not Accepted refer to ZA 3. This could be a section to be added.

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 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
UK 10	5 Responsible vuln disclosure	second bullet	Te	The bullet contains subjective expressions	Replace with the following text “It can minimize the risk posed by security vulnerabilities, by enabling them to be identified, investigated, and resolved in a way that produces a timely and effective remedy”	Accepted bullet 2 will be updated.
UK 11	5 Responsible vuln disclosure	last para	Te	Current text implies that vendor cannot accept vulnerability report unless it has vulnerability policy. That is not correct.	Replace with the following text: “A vendor must create vulnerability management policy and it must be shared with vendor customer base. While optional, vendors are strongly encouraged to make this policy public. Having a vulnerability managing policy defined is not requirement for responsible vulnerability disclosure. However, the policy helps in setting right expectations.”	Accept with modification. Will add the 1st paragraph only. And change "management" to handling to align to document.
UK 12	6 Life cycle	first para	Te	It has to be noted that sub-phases in the life cycle are not necessarily in chronological order.	Replace the sentence with this “The following lifecycle aligns these common phases (sub-phases may not be in a chronological order).”	Accept will update
UK 13	6 Life cycle	2 verification phase	Te	“reproduction” implies that vendor will always develop an exploit for a vulnerability which is not always the case	Replace word “reproduce” with “confirm”	Accept
UK 14	6 Life cycle	3 resolution phase b)	Te	Replace “update” with “remedy” and remove the rest of the text as the remedy is already defined.	Produce remedy.	Accept in principle
UK 15	6 Life cycle	4 advisory phase a)	Te	A reference to extraordinary circumstances should be added	Add the following sentence “Under extraordinary circumstances a vendor can release an advisory even if a remedy is not available.”	Accept

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.

Attachment 3 to SC 27 N8672
[UK] comments on ISO/IEC 4th WD 29147

Date: 2010-03-10	Document: SC 27 N8126
------------------	------------------------------

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
UK 16	7 Vulnerability Handling policy	first para	Te	Remove the reference to IETF draft. Examples are given in Annex B so this one should be no exception.	Remove the second sentence from the paragraph.	Accept see JP 27
UK 17	7 Vulnerability Handling policy	bullet 1	Te	The number of co-ordinators can change and vendor may not even be aware of the existence of some of the co-ordinators. Vendors should give their contact information to co-ordinators but that is on the best effort basis.	Add sentence "Vendors will do their best effort to provide their contact information to the coordinators"	Accept in principle Editors Note: Editor will consider other changes in this section and add where appropriate.
UK 18	7 Vulnerability Handling policy	bullet 4	Te	The spirit of this bullet is good but it only protects finders and not vendors. Finders may be collecting information and provide it to its advantage against the vendor or give it to a competitor of the vendor. As long as this bullet provides only one way assurance it is not acceptable.	Remove the bullet 4	Not Accepted Editors Note: The standard does in no way address the actions of finders so this is not in scope.
UK 19	8.1 Simplified Policy	first sentence	Ed	Use affirmative voice.	Rewrite the sentence to read "The vulnerability handling policy should be simple and clear to enable easy reporting of product vulnerabilities to the vendor"	Accept this is now in section 7 list item 1.
UK 20	8.1 Simplified Policy		Te	Vendors should be encouraged to use intuitive place for this policy and other security-related information. Adoption of NIAC recommendation of /security page should be encouraged.	Add sentence "Vendors should consider intuitive placement of information related to product security management. Usage of /security web page for this purpose is recommended."	Accept will be added to section 7 list item 1 as 2nd sentence.
UK 21	8.3 Ack of receipt from finder	second para	Te	The last sentence talks about 'pre-disclosure'. This term have specific, but different meaning, for different parties. To prevent confusion on what is exactly meant by pre-disclosure in this context we should use different term.	Rewrite the sentence as follows "When exchanging sensitive information in e-mail messages, they shall be protected by mutually agreed encryption mechanism like PGP."	Accept with modifications replace "pre-disclosure" with "When exchanging sensitive information,"

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 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
UK 22	8.3 Ack of receipt from finder	Examples of exmail aliases	Ed	The example of e-mail aliases used for receiving vulnerability information feels a bit misplaced here.	Move this example into section 8.5 under e-mail bullet	
UK 23	8.4 Assign unique ID		Te	<p>CVEs are assigned in a sequential fashion and, as such, may reveal certain amount of information. CVEs should be protected in transit.</p> <p>It is also possible to encounter a situation that single CVE entry will be later split into multiple CVE entries during the subsequent review. Vendors and finds must be warned about that possibility to set the right expectations.</p> <p>Many vendors would also assign a case (tracking) number to the report. This will be done much sooner than assigning a CVE number. Distinction between these two IDs must be made.</p>	<p>Add the following text "While every care is taken that CVE identifier is unique a situation may occur where an CVE candidate is split into a multiple CVE entries during the subsequent review. This is a rare situation but it can occur.</p> <p>CVE identifiers, by itself, reveal a certain amount of information and they should be treated as any other sensitive information and not transmitted in cleartext.</p> <p>Vendors may also assign a case (tracking) number to the report. This can happen before CVE ID is assigned. Vendor tracking number is unique for that vendor and it does not replaces CVE identifier."</p>	Accept Editors Note: This will moved to section 7.3 along with this clause.
UK 24	8.7 Role of a Coordinator	whole section	Te	This section misrepresents the role of a coordinator. As the name suggest coordinator helps with coordination and is not an arbiter. In practice it is hard to imagine how a coordinator, with no jurisdiction, can perform arbitrage.	<p>Remove completely section 8.7 and replace it with the following text "Coordinator can play multiple roles in vulnerability management process:</p> <ul style="list-style-type: none"> • Act as trusted introducer between involved parties • Coordinate advisory public release date • Enabling communication between involved parties 	Accept in principle Editors Note: The editor does not agree that this "must happen" before working on a vulnerability. As a finder can deal directly with a vendor.

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 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
					(vendors and finders) <ul style="list-style-type: none"> Provide environment where experts from different organizations can work jointly on addressing the vulnerability Vendors and finders are encouraged to establish relationship with a coordinator (or more than one coordinator) before start working on a vulnerability. Which coordinator they choose to establish a relationship would depend on various factors as geographical proximity, language and acceptable operation model."	
UK 25	8.7 Role of a Coordinator		Te	In addition to comment UK 24 add the following text at the end of the section.	"Implicitly, an assumption is that coordinators exchange some information among themselves and that certain level of cooperation within the group exists. Vendors and finders are encouraged to discuss this topic with their preferred coordinator. Document " Guidelines for Vendor - Coordinators relationship " (available at https://members.first.org/vendor-sig/vendor-coordinators-guidelines-public-v1.0.pdf) produced by FIRST Vendor SIG, can be used to set a basic level of expectations."	Not accepted as this seems to refer documents out of scope of document.

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.

Attachment 3 to SC 27 N8672
[UK] comments on ISO/IEC 4th WD 29147

Date: 2010-03-10	Document: SC 27 N8126
------------------	------------------------------

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
UK 26	9.0 Disseminating of vulnerability information		Te	To better help consumers of advisories to assess relative impact of different vulnerabilities to their systems vendors should consider using a vendor-neutral scoring system.	Add this sentence at the end of the paragraph "In order to help advisory consumers with assessing relative impact of different vulnerabilities, vendor should consider using a common vulnerability scoring system (CVSS)."	Accept
UK 27	B.1 Sample vulnerability disclosure	When to contact the security incident response team	Te	This text mixes vulnerability management with incident management. They are not the same! In the text CSIRT is mentioned, these teams usually handle incidents and only rarely product vulnerabilities.	Change the title to "When to contact product vulnerability response team"	Accept in principle Editors Note: This section will be updated to and could impact the title change.
UK 28	B.1 Sample vulnerability disclosure	When to contact the security incident response team, first para	Te	Remove the reference to CSIRT in the first sentence.	Use the following sentence "Contact the <company name> Product Vulnerability Response Team (PVRT)." By sending email to security-alert@<company domain name> in the following situations:"	Not accepted Editors Note: We do not use the term PVRT until this point so it not a principle that current accepted.
UK 29	B.1 Sample vulnerability disclosure	Responding to customer incidents	Te	This section talks about helping customers with computer incidents and is not about vulnerability handling. While it is true that some teams may have dual role (vulnerability and incident managing) that is not universally true. To make this example clear we should not mix these two roles.	Remove the section "Responding to customer incidents"	Accepted this section will be removed.
UK 30	B.2 Identifying and managing risk in systems	Whole section	Te	This section does seem a bit out of place here and it could be moved to a separate annex. There are also other models that can be references.	Add references to CERT Resiliency Management Model http://www.cert.org/resiliency/rmm.html and Building Security in Maturity Model http://www.bsi-mm.com/	Accepted will add this reference

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.

Attachment 3 to SC 27 N8672
[UK] comments on ISO/IEC 4th WD 29147

Date: 2010-03-10	Document: SC 27 N8126
------------------	------------------------------

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
UK 31	B.5 Samples of good and bad disclosure	whole section	Te	Referencing outside material is not optimal as it can change without notice, we removed or become unsuitable for the purpose. While using concrete organizations as bad examples is very tempting these organizations may object to that practice.	Remove the current text and produce generic examples without referencing concrete organizations.	Accept in principle see US 68
UK 32	B.7 Coordinators recognized globally	first sentence	Te	The impression document gives right now is that there are only four global coordinators. That is not correct. CPNI from UK is an example of an organization that played coordination role and then scaled back but it may do it again. New coordinators may also appear. We must not give impression that this is a definitive list.	Replace the first sentence with the following text "The following, non-exhaustive, list of globally recognized coordinators is correct at the time this IS was last updated. Since then new coordinators may become active or an existing coordinators may scale back their capabilities."	Accept will update sentence
UK 33	Bibliography		Te	restore full bibliography from the previous WD	Use the bibliography from WD3	Accept in principle Editors Note: Several NBs have requested that the list be reduced.
UK 34	-	-	Ge	In accordance with Resolution 15 of the Redmond WG 3 Meeting, the UK National Body reminds WG 3 of its undertaking to address and respond to the FIRST comments on the 3rd WD contained in SC 27 N8060.		Superseded by events
UK 35	Introduction	-	Ed	Part of the text is not unshaded black in colour.	Change to ISO normal style.	Accept will change colour to black.
UK 36	3	-	Te	Why in the heading do you refer to these definitions as being supplementary to 27000, then repeat the definition of vulnerability word for word from that document? And your model of the relationship between threat and vulnerability as used in A.2 is inconsistent with the definition of threat given in 27000 and incorporated in your document by reference.	Delete reference to 27000 in heading, then credit 27000 as the source of your definition of vulnerability.	Accept will identify definitions that are 27000 and add a NOTE that indicates this.
UK 37	4	-	Ed	You use the abbreviation RVD, but it is not defined here.	Add definition.	Accept in principle based on CA 2

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.

Attachment 3 to SC 27 N8672
[UK] comments on ISO/IEC 4th WD 29147

Date: 2010-03-10	Document: SC 27 N8126
------------------	------------------------------

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
UK 38	5	-	Te	This model is still confusing. Is the user (a term that is not defined) the same as the customer? If not, what is the distinction.	Clarify and rewrite.	Accept will add sentence to ensure if customer or user and terms of reference
UK 39	6	-	Te	The status of this lifecycle model is confusing. Not all finders and vendors follow this model (although it is a good model, and perhaps they should be recommended or mandated to do so).	Clarify status.	Accept in principle see ZA 6.
UK 40	7	-	Ed	Is this policy called a vulnerability policy or a vulnerability handling policy? Both terms are used. Is it the same policy as the vulnerability disclosure policy referred to in clauses 5 and 8?	Make consistent.	Accept will make "vulnerability handling policy" consistent across the document.
UK 41	8	1	Ed	The first sentence is repeated at the end of the paragraph.	Delete one or other copy.	Not accepted see JP 33
UK 42	8.1	Title	Ed	This policy is simplified with respect to what?	Retitle as "Keep the handling policy simple"	Accept update to be "Keep the vulnerability handling policy simple"
UK 43	8.5	1	Ed	The final sentence is irrelevant, both because finder is in the definitions and because finders are not otherwise referenced in this subclause.	Delete.	Accepted will remove this sentence
UK 44	9.0	-	Ed	The structure of headings has gone wrong. There should be a clause 9 heading, then a subheading 9.1	Restructure, then renumber following subclauses.	Accepted see JP 71
UK 45	9	-	Ed	"Vendors" should not be capitalised.	Fix.	Accepted
UK 46	9.1	-	ed	"Advisory" should not be capitalised.	Fix.	Accepted

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.

Attachment 4 to SC 27 N8672
[US] comments on ISO/IEC 4th WD 29147

Date: 2010-MM-DD	Document: SC 27 N8126
------------------	------------------------------

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.	Front page	Title	Ed	<p>The editor did not follow the Disposition of Comments for this section.</p> <ul style="list-style-type: none"> The editor failed to make the accepted editorial change to make the dashes consistent. <p>See Comment ZA 12 from SC27N8127_DoC_3rdWD_29147_N7901.</p>	<p>Follow the editor's instructions for ZA 12 from SC27N8127_DoC_3rdWD_29147_N7901.</p> <p>Replace "techniques -- Responsible" with "techniques – Responsible"</p>	Accept - will change the "dash" accordingly
US 2.	Contents	Page iii	Ed	<p>The Table of Contents is incorrect and missing certain sections (e.g. Clause 6, Annex A.1).</p>	<p>Rebuild the Table of Contents after creating the next draft to ensure correct labelling and mapping to actual headings and sections.</p>	Accept - Will update the ToC accordingly see JP 1
US 3.	Foreword	Para 3	Ed	<p>The editor did not follow the Disposition of Comments for this section.</p> <ul style="list-style-type: none"> The editor removed paragraphs 3 and 4 instead of changing the word "should" to "shall". The editor misinterpreted the DoC to mean that all instances of the word "should" in the draft should be replaced with "shall". This is incorrect outside the Foreword, as the word "shall" is for normative standards, rather than for informative standards such as this one. <p>See Comment UK 1 from SC27N8127_DoC_3rdWD_29147_N7901.</p>	<p>Follow the editor's instructions for UK 1 from SC27N8127_DoC_3rdWD_29147_N7901.</p> <p>Add the following two paragraphs to the end of the Foreword: "Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. ISO/IEC 29147 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, Security techniques."</p>	Accept - Editor will add the foreword and reverse the global "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.

Attachment 4 to SC 27 N8672
[US] comments on ISO/IEC 4th WD 29147

Date: 2010-MM-DD	Document: SC 27 N8126
------------------	------------------------------

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
					See additional US comments for corrections on the misapplication of the word "shall" throughout the rest of the draft.	
US 4.	Introduction	Entire	Te	<p>1. The editor did not follow the Disposition of Comments for this section.</p> <ul style="list-style-type: none"> The editor removed the reference annotation and the quotation marks around the text that is a direct quote from the NIAC framework. <p>2. The editor refers to "reference 15" which no longer exists in the Bibliography.</p> <p>See Comments CA 1, JP 8, and JP 10 from SC27N8127_DoC_3rdWD_29147_N7901.</p>	<p>Follow the editor's instructions for CA 1, JP 8, and JP 10 from SC27N8127_DoC_3rdWD_29147_N7901.</p> <p>Replace entire section with the text</p> <p>"A vulnerability is a weakness in a system which, if exploited, allows the exploiter to violate the security policy for that system.</p> <p>As defined by reference 1 in the bibliography, "Vulnerabilities can be caused by software and hardware design flaws, poor administrative processes, lack of awareness and education, and advancements in the state of the art or improvements to current practices. Regardless of cause, an exploitation of such vulnerabilities may result in real threats to mission-critical information systems."</p> <p>Users, including businesses and</p>	Accept - will replace the current text as indicated. However, due to JP2 the Bibliography will be update to reflect this accepted change. Including several sections that will be removed as they do reference this work.

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.

Attachment 4 to SC 27 N8672
[US] comments on ISO/IEC 4th WD 29147

Date: 2010-MM-DD	Document: SC 27 N8126
------------------	------------------------------

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>governments, rely heavily on hardware and software components used in operating systems, applications, networks, and critical national infrastructure. Vulnerabilities in these components increase risk to users.</p> <p>Vulnerability disclosure is the practice of reporting, coordinating, and publishing information about a vulnerability and its resolution.</p> <p>As defined by reference 3 in the bibliography, "The goals of responsible disclosure include:</p> <ol style="list-style-type: none"> 1) Ensure that vulnerabilities can be identified and eliminated effectively and efficiently for all parties. 2) Minimize the risk to customers from vulnerabilities that could allow damage to their systems. 3) Provide customers with sufficient information for them to evaluate the level of security in vendors' products. 4) Provide the security community with the information necessary to develop tools and methods for identifying, managing, and reducing the risks of vulnerabilities in information technology. 5) Minimize the amount of time 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.

Attachment 4 to SC 27 N8672
[US] comments on ISO/IEC 4th WD 29147

Date: 2010-MM-DD	Document: SC 27 N8126
------------------	------------------------------

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>resources required to manage vulnerability information.</p> <p>6) Facilitate long-term research and development of techniques, products, and processes for avoiding or mitigating vulnerabilities.</p> <p>7) Minimize the amount of antagonism that often exists between parties as a result of different assumptions and expectations, due to the lack of consistent and explicit disclosure practices. “</p> <p>Through responsible vulnerability disclosure, vendors can work together diligently with vulnerability finders and produce a timely resolution to reduce users’ risks associated with the vulnerability in accordance with their business strategy.</p> <p>This International Standard provides a guideline for vendors on receiving information about potential vulnerabilities and distributing vulnerability resolution information toward accomplishing responsible vulnerability disclosure.</p> <p>”.</p>	
US 5.	1 Scope	Para 2	Ed	2 nd paragraph list should use colon : not semicolon	replace : with ;	Accept will change accordingly

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 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 6.	1 Scope	Para 3	Ed	The sentence that comprises this paragraph is grammatically awkward and contains an extraneous comma.	Replace “responsible to investigate a potential vulnerability in a product or product component, developed” With “responsible for investigating potential vulnerabilities in a product or product component developed”	Accept will change accordingly
US 7.	1 Scope	Para 4	Ed	The editor did not follow the Disposition of Comments for this section. <ul style="list-style-type: none"> The editor failed to make the accepted editorial change to remove the phrase “to all interested parties” as indicated in the Resolution for ZA 19, which cites JP 9. The editor instead replaced the phrase “to all interested parties” with “to all stakeholders”. This is not what the National Bodies agreed to during the ad hoc editing sessions. See Comment ZA 19 from SC27N8127_DoC_3rdWD_29147_N7901.	Follow the editor’s instructions for ZA 19 from SC27N8127_DoC_3rdWD_29147_N7901. Remove the phrase “to all stakeholders” from the end of the last sentence in this section.	Accept will change accordingly.
US 8.	2 Normative references	Entire	Te	No normative references seem appropriate for this standard.	The editor should either remove this section, or create a list of normative references for the next draft.	Accepted see ZA 2 Editors Note: No normative reference to be included.
US 9.	3 Terms and Definitions	Para 1	Te	The draft does not use terms as they are defined in ISO/IEC 27000, but instead uses the terms as defined specifically for the purposes of this standard. In cases where a term used in this draft exists in ISO/IEC 27000, it should be noted in the definition specifically for	Remove “For the purposes of this document, the following terms given in ISO/IEC 27000, and the following apply.” Instead, make appropriate notes within	Accepted see UK 36.

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 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
				that term, e.g., the term “vulnerability” should contain the following: “NOTE Adapted from ISO/IEC 27000:2009”.	specific definitions to indicate whether the definition is adapted from ISO/IEC 27000.	
US 10.	3 Terms and definitions	3.1 advisory	Te	The editor did not follow the Disposition of Comments for this section. <ul style="list-style-type: none"> The editor failed to make the accepted technical change to replace the definition of advisory with the text agreed upon by the National Bodies during the ad hoc editing sessions. See Comment JP 23 from SC27N8127_DoC_3rdWD_29147_N7901.	Follow the editor’s instructions for JP 23 from SC27N8127_DoC_3rdWD_29147_N7901. Replace the definition and NOTE section text with “(noun) information about a vulnerability NOTE A vulnerability advisory may include advice on how to deal with the vulnerability. An advisory typically contains a description of the vulnerability including a list of vulnerable software, potential impact, resolution and mitigation information, and references. An advisory may be published by a vendor, finder, or coordinator.”	Accept in Principle see JP 4
US 11.	3 Terms and definitions	3.2 Coordinator	Te	The editor did not follow the Disposition of Comments for this section. <ul style="list-style-type: none"> The editor failed to make the accepted technical change to the definition that all National Bodies agreed to during the ad hoc editing sessions. See Comment US 9 from SC27N8127_DoC_3rdWD_29147_N7901.	Follow the editor’s instructions for US 9 from SC27N8127_DoC_3rdWD_29147_N7901. Replace the definition for this term with “an optional participant that can assist vendors and finders in managing and disclosing vulnerability information”.	Accept will update accordingly.

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.

Attachment 4 to SC 27 N8672
[US] comments on ISO/IEC 4th WD 29147

Date: 2010-MM-DD	Document: SC 27 N8126
------------------	------------------------------

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 12.	3 Terms and definitions	3.4 product	Te	A product, in the sense of this document, can include freeware that is not for sale. For the purposes of this document, a service can be included in the definition of a product (e.g. Software as a Service).	Replace the current definition with “software, hardware, or online services NOTE 1 A product can be for sale or free.”	Accept see UK 5
US 13.	3 Terms and definitions	3.4 product and 3.5 online services	Ed	The editor did not follow the Disposition of Comments for this section. <ul style="list-style-type: none"> The editor failed to make the accepted editorial change to order the terms alphabetically. See Comment JP 11 and UK 3 from SC27N8127_DoC_3rdWD_29147_N7901.	Follow the editor’s instructions for JP 11 and UK 3 from SC27N8127_DoC_3rdWD_29147_N7901. Switch the term “product” to be listed after “online services”.	Accept will change to alphabetical order
US 14.	3 Terms and definitions	3.5 online services	Te	The definition for online services is incorrect where it states that online services are an organization or a service provider. It is the service being provided that is the online service.	Replace current definition with “applications or services provided over the Internet EXAMPLES Internet-hosted email, software as a service”	Accept in principle JP 7 will add the EXAMPLES appended to the beginning of the current EXAMPLE. Including removal of "and application service providers" from the list.
US 15.	3 Terms and definitions	3.6 security incident	Te	The editor did not follow the Disposition of Comments for this section. <ul style="list-style-type: none"> The editor failed to delete this term. See Comment JP 21 from SC27N8127_DoC_3rdWD_29147_N7901.	Follow the editor’s instructions for JP 21 from SC27N8127_DoC_3rdWD_29147_N7901. Delete the term “security incident”.	Accept see JP 9
US 16.	3 Terms and definitions	3.7 update	Te	The editor did not follow the Disposition of Comments for this section. <ul style="list-style-type: none"> The editor failed to insert “documentation change” and “hotfix” to the appropriate places in 	Follow the editor’s instructions for US 11 from SC27N8127_DoC_3rdWD_29147_N7901.	Accept in principle to reflect BE 4 change of "update" to "remediation"

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 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 text of this definition. See Comment US 11 from SC27N8127_DoC_3rdWD_29147_N7901.	Replace current definition with "patch, fix, upgrade, configuration or documentation change to address a vulnerability NOTE A change intended to resolve or mitigate a vulnerability. An update typically takes the form of a configuration change, binary file replacement, hardware change, or source code patch, etc. Updates are usually provided by vendors. Vendor use different terms including patch, fix, hotfix, and upgrade."	
US 17.	3 Terms and definitions	3.8 vendor	Te	The editor did not follow the Disposition of Comments for this section. <ul style="list-style-type: none"> The editor failed to make the accepted technical change to the definition that all National Bodies agreed to during the ad hoc editing sessions. See Comment ZA 25 and ZA 26 from SC27N8127_DoC_3rdWD_29147_N7901.	Follow the editor's instructions for ZA 25 and ZA 26 from SC27N8127_DoC_3rdWD_29147_N7901. Replace the current definition with "person or organisation that developed the product, or is responsible for maintaining it"	Accept will update the definition
US 18.	3 Terms and definitions	3.8 vendor	Ed	A period (".") should not end the definition, since the definition text is supposed to be a phrase that could replace the term in a sentence, not a complete sentence itself	Remove the period (".") at the end of the definition.	Accept see JP 10
US 19.	3 Terms and definitions	3.8 vulnerability	Te	The editor did not follow the Disposition of Comments for this section. <ul style="list-style-type: none"> The editor failed to make the accepted technical change to the definition that all National Bodies 	Follow the editor's instructions for ZA 29 from SC27N8127_DoC_3rdWD_29147_N7901.	Accept will update accordingly this references 3.9 NOT 3.8 including the addition of the NOTE. Replace first sentence of "Introduction" with this definition.

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 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
				agreed to during the ad hoc editing sessions. See Comment ZA 29 from SC27N8127_DoC_3rdWD_29147_N7901.	Replace the current definition with "weakness of software, hardware, or online service that can be exploited by a threat NOTE Adapted from ISO/IEC 27000:2009"	
US 20.	3 Terms and definitions	3.8 vulnerability	Te	An additional note for clarity of what types of errors can become vulnerabilities should be added as a NOTE in the definition.	Add an additional note to the definition of vulnerability as follows: "NOTE Vulnerabilities can be architecture flaws, coding errors, or other implementation errors, or insecure configuration. Vulnerabilities can also result from insufficient or incorrect security documentation, security awareness, or communication."	Accept will update accordingly this references 3.9 NOT 3.8.
US 21.	4 Abbreviated terms	Section title	Ed	Title should not contain a trailing parenthesis ")".	Remove ")".	Accept see UK 7
US 22.	4 Abbreviated terms	First two terms	Te	Abbreviations are listed that are not used elsewhere in the document.	Remove the following abbreviations: "BBS bulletin board system CC common criteria DLL dynamic link library"	Accept will remove the entries listed
US 23.	4 Abbreviated terms	various terms	Te	Include all abbreviated terms used in the standard.	Add and alphabetize among the other terms: "CSIRT Computer Security Incident Response Team PSIRT Product Security Incident	Accept in principle refer to UK 8

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.

Attachment 4 to SC 27 N8672
[US] comments on ISO/IEC 4th WD 29147

Date: 2010-MM-DD	Document: SC 27 N8126
------------------	------------------------------

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
					Response Team”	
US 24.	4 Abbreviated terms	Term JPCERT	Te	JPCERT should be JPCERT/CC.	Change “JPCERT Japan computer emergency response team” to “JPCERT/CC Japan Computer Emergency Response Team/ Coordination Center.”	Accept in principle refer to UK 8
US 25.	5 Responsible Vulnerability Disclosure	Para 1 Sentence 1	Te	The editor did not follow the Disposition of Comments for this section. <ul style="list-style-type: none"> The editor failed to make the accepted technical change to the section that all National Bodies agreed to during the ad hoc editing sessions. See Comment CA 7 from SC27N8127_DoC_3rdWD_29147_N7901.	Follow the editor’s instructions for CA 7 from SC27N8127_DoC_3rdWD_29147_N7901. Replace “Responsible disclosure implies that the vulnerability finder and vendor work together diligently to produce a timely resolution to reduce user’s risks associated with the vulnerability.” with: “A vendor should develop and publish their vulnerability disclosure process.”	Accepted will update
US 26.	5 Responsible Vulnerability Disclosure	End of list	Ed	There is a trailing quotation mark that should be removed.	Remove trailing quotation mark.	Accept
US 27.	5 Responsible	Last Para	Te	The editor did not follow the Disposition of Comments for	Follow the editor’s instructions for CA 7 from	Accept in principle see UK 11.

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.

Attachment 4 to SC 27 N8672
[US] comments on ISO/IEC 4th WD 29147

Date: 2010-MM-DD	Document: SC 27 N8126
------------------	------------------------------

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
	e Vulnerability Disclosure			<p>this section.</p> <ul style="list-style-type: none"> The editor used proposed text from a comment that was rejected and replaced by consensus during the ad hoc editing sessions. <p>See Comment CA 7 from SC27N8127_DoC_3rdWD_29147_N7901.</p>	<p>SC27N8127_DoC_3rdWD_29147_N7901.</p> <p>Remove the last paragraph:</p> <p>“Before responsible vulnerability disclosure between a finder and vendor can begin, the vendor first must ensure they have established and made publically available their vulnerability disclosure policy.”</p>	
US 28.	6 Lifecycle of a Vulnerability	First sentence	Te	<p>The first sentence does not add any pertinent information to the clause or the IS as a whole and should be removed.</p>	<p>Remove the sentence “Regardless of the nature of a vulnerability, each one being unique, some elements of reporting and identifying are identical. The following lifecycle aligns these common phases.”</p>	Accept sentence will be removed.
US 29.	6 Lifecycle of a Vulnerability	Diagram	Te	<p>The Resolution phase may not proceed in all cases to releasing an advisory, e.g. if the issue is investigated by the vendor and found not to be a security vulnerability.</p> <p>In those cases, the process would end with the Resolution phase and the case would be closed by the vendor at that point.</p>	<p>Change solid line between “Resolution” and “Advisory” to a dotted line to indicate that the path is not followed in all cases.</p> <p>The solid line between “Advisory” and “Post Release” should remain solid, since once an advisory is released, there will always be a post-release phase.</p>	Accept will update diagram as indicated.
US 30.	6 Lifecycle of a Vulnerability	2 Verification Phase	Te	<p>Add language to support the case when a vulnerability cannot be reproduced, or the issue has been investigated and is found not to be a security vulnerability.</p>	<p>Add the following subsection, and re-label subsequent items in the list:</p> <p>“b. If the potential vulnerability either cannot be verified or reproduced, or the vendor determines that the issue does not violate the security policy of the</p>	Accept create new 2.b titled "Non-Vulnerability" and add the provided text.

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.

Attachment 4 to SC 27 N8672
[US] comments on ISO/IEC 4th WD 29147

Date: 2010-MM-DD	Document: SC 27 N8126
------------------	------------------------------

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
					product, then the vendor should communicate the results of their investigation to the finder as part of the Resolution Phase. As part of the Verification Phase, the vendor should ask if the finder can produce further evidence that the issue is a security vulnerability before making their final resolution decision.”	
US 31.	6 Lifecycle of a Vulnerability	3 Resolution Phase	Te	Add language to support the resolution of an issue that turns out not to be a security vulnerability.	Add the following subsection and re-label subsequent items in the list: “b. If the vendor decides not to issue an advisory, either because they could not reproduce the issue or they disagree that the issue is a security vulnerability, the vendor should communicate this decision to the finder. The vendor would not execute subsequent phases of the lifecycle in this case.”	Accept add new step 3.b titled "Non Vulnerability Resolution" and include the provided text.
US 32.	6 Lifecycle of a Vulnerability	4 Advisory Phase	Ed	There is a comma (“,”) missing.	Insert a comma (“,”) between the words “effective” and “it.”	Accept will add comma.
US 33.	6 Lifecycle of a Vulnerability	Last Para Sent 2	Ed	There is a colon (“:”) missing.	Insert a colon (“:”) between the words “functions” and “receiving”.	Accept will add colon.
US 34.	6 Lifecycle of a Vulnerability	Last Para Second list item	Ed	This list item contains awkward grammar.	Remove the word “aspect” from the list item.	Accept to remove "aspect" from this sentence

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.

Attachment 4 to SC 27 N8672
[US] comments on ISO/IEC 4th WD 29147

Date: 2010-MM-DD	Document: SC 27 N8126
------------------	------------------------------

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 35.	6 Lifecycle of a Vulnerability	Last Para Last Sent	Ed	The word “aspects” is missing from this sentence, and there is also an extraneous space between the last word of the sentence and the period at the end.	Return the word “aspects” to this sentence, and remove the extraneous space between the last word of the sentence and the period at the end. The sentence should be: “The remainder of this document focuses on these aspects.”	Accept to return word "aspects" to the end of this sentence.
US 36.	7 through end of document	Entire	Ge	At this point, the US National Body stopped looking for grammar and spelling errors in the document. It should be noted that there are many spelling and grammar errors remaining that are not documented in the rest of the US comments.	Review the entire document for spelling and grammar and make corrections to the next draft.	Not accepted Editors Note: The editor acknowledges the comment however would ask that specific examples be used in the future.
US 37.	7 Vulnerability Handling Policy	Para 1 Sent 1	Te	The editor did not follow the Disposition of Comments for this sentence. <ul style="list-style-type: none"> The editor misinterpreted the DoC to mean that all instances of the word “should” in the draft should be replaced with “shall”. This is incorrect outside the Foreword, as the word “shall” is for normative standards, rather than for informative standards such as this one. See Comment UK 1 from SC27N8127_DoC_3rdWD_29147_N7901.	Replace the word “shall” with “should” in this sentence.	Accepted in Principle see ZA 6
US 38.	7 Vulnerability Handling Policy	Para 1 Sent 2	Te	The editor did not follow the Disposition of Comments for this sentence. <ul style="list-style-type: none"> The editor misinterpreted the DoC to mean that all instances of the word “should” in the draft should be replaced with “shall”. This is incorrect outside the Foreword, as the word “shall” is for normative standards, rather than for informative 	Replace the word “shall” with “should” in this sentence.	Accepted in Principle see ZA 6

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.

Attachment 4 to SC 27 N8672
[US] comments on ISO/IEC 4th WD 29147

Date: 2010-MM-DD	Document: SC 27 N8126
------------------	------------------------------

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
				standards such as this one. See Comment UK 1 from SC27N8127_DoC_3rdWD_29147_N7901.		
US 39.	7 Vulnerability Handling Policy	Para 2 Sent 1	Te	The editor did not follow the Disposition of Comments for this sentence. <ul style="list-style-type: none"> The editor misinterpreted the DoC to mean that all instances of the word “should” in the draft should be replaced with “shall”. This is incorrect outside the Foreword, as the word “shall” is for normative standards, rather than for informative standards such as this one. See Comment UK 1 from SC27N8127_DoC_3rdWD_29147_N7901.	Replace the word “shall” with “should” in this sentence.	Accept will change "shall" to "should"
US 40.	7 Vulnerability Handling Policy	2. Expected responses Sent 1	Te	The editor did not follow the Disposition of Comments for this sentence. <ul style="list-style-type: none"> The editor misinterpreted the DoC to mean that all instances of the word “should” in the draft should be replaced with “shall”. This is incorrect outside the Foreword, as the word “shall” is for normative standards, rather than for informative standards such as this one. See Comment UK 1 from SC27N8127_DoC_3rdWD_29147_N7901.	Replace the word “shall” with “should” in this sentence.	Accept will change "shall" to "should"
US 41.	8.3 Acknowledgement of receipt from finder	Para 1 Sent 2	Te	The editor did not follow the Disposition of Comments for this sentence. <ul style="list-style-type: none"> The editor misinterpreted the DoC to mean that all instances of the word “should” in the draft should be replaced with “shall”. This is incorrect outside the Foreword, as the word “shall” is for 	Replace the word “shall” with “should” in this sentence.	Accept change of "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.

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
				normative standards, rather than for informative standards such as this one. See Comment UK 1 from SC27N8127_DoC_3rdWD_29147_N7901.		
US 42.	8.3 Acknowledgement of receipt from finder	Para 2 Sent 1	Te	The editor did not follow the Disposition of Comments for this sentence. <ul style="list-style-type: none"> The editor misinterpreted the DoC to mean that all instances of the word “should” in the draft should be replaced with “shall”. This is incorrect outside the Foreword, as the word “shall” is for normative standards, rather than for informative standards such as this one. See Comment UK 1 from SC27N8127_DoC_3rdWD_29147_N7901.	Replace the word “shall” with “should” in this sentence.	Accept change of "shall" to should. Note: This sentence is being moved to paragraph 1 of this section.
US 43.	8.3 Acknowledgement of receipt from finder	Para 2 Sent 2	Te	The editor did not follow the Disposition of Comments for this sentence. <ul style="list-style-type: none"> The editor misinterpreted the DoC to mean that all instances of the word “should” in the draft should be replaced with “shall”. This is incorrect outside the Foreword, as the word “shall” is for normative standards, rather than for informative standards such as this one. See Comment UK 1 from SC27N8127_DoC_3rdWD_29147_N7901.	Replace the word “shall” with “should” in this sentence.	Accept change of "shall" to should
US 44.	8.3 Acknowledgement of receipt from finder	Para 2 Sent 3	Te	The editor did not follow the Disposition of Comments for this sentence. <ul style="list-style-type: none"> The editor misinterpreted the DoC to mean that all instances of the word “should” in the draft should be replaced with “shall”. This is incorrect 	Replace the word “shall” with “should” in this sentence.	Accept change of "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.

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>outside the Foreword, as the word “shall” is for normative standards, rather than for informative standards such as this one.</p> <p>See Comment UK 1 from SC27N8127_DoC_3rdWD_29147_N7901.</p>		
US 45.	8.3 Acknowledgement of receipt from finder	Para 2 Sent 4	Te	<p>The editor did not follow the Disposition of Comments for this sentence.</p> <ul style="list-style-type: none"> The editor misinterpreted the DoC to mean that all instances of the word “should” in the draft should be replaced with “shall”. This is incorrect outside the Foreword, as the word “shall” is for normative standards, rather than for informative standards such as this one. <p>See Comment UK 1 from SC27N8127_DoC_3rdWD_29147_N7901.</p>	Replace the word “shall” with “should” in this sentence.	Accept change of “shall” to should
US 46.	8.3 Acknowledgement of receipt from finder	Para 2 Sent 5	Te	<p>The editor did not follow the Disposition of Comments for this sentence.</p> <ul style="list-style-type: none"> The editor misinterpreted the DoC to mean that all instances of the word “should” in the draft should be replaced with “shall”. This is incorrect outside the Foreword, as the word “shall” is for normative standards, rather than for informative standards such as this one. <p>See Comment UK 1 from SC27N8127_DoC_3rdWD_29147_N7901.</p>	Replace the word “shall” with “should” in this sentence.	Accept change of “shall” to should
US 47.	8.3 Acknowledgement of receipt from finder	Last Para Sent 2	Te	<p>The editor did not follow the Disposition of Comments for this sentence.</p> <ul style="list-style-type: none"> The editor misinterpreted the DoC to mean that all instances of the word “should” in the draft 	Replace the word “shall” with “should” in this sentence.	Accept change of “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.

Attachment 4 to SC 27 N8672
[US] comments on ISO/IEC 4th WD 29147

Date: 2010-MM-DD	Document: SC 27 N8126
------------------	------------------------------

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>should be replaced with “shall”. This is incorrect outside the Foreword, as the word “shall” is for normative standards, rather than for informative standards such as this one.</p> <p>See Comment UK 1 from SC27N8127_DoC_3rdWD_29147_N7901.</p>		
US 48.	8.4 Assigning a Unique Identifier to a Vulnerability	Para 1 Sent 1	Te	<p>The editor did not follow the Disposition of Comments for this sentence.</p> <ul style="list-style-type: none"> The editor misinterpreted the DoC to mean that all instances of the word “should” in the draft should be replaced with “shall”. This is incorrect outside the Foreword, as the word “shall” is for normative standards, rather than for informative standards such as this one. <p>See Comment UK 1 from SC27N8127_DoC_3rdWD_29147_N7901.</p>	Replace the word “shall” with “should” in this sentence.	Accept change of "shall" to should
US 49.	8.4 Assigning a Unique Identifier to a Vulnerability	Para 1 Sent 3	Te	<p>The editor did not follow the Disposition of Comments for this sentence.</p> <ul style="list-style-type: none"> The editor misinterpreted the DoC to mean that all instances of the word “should” in the draft should be replaced with “shall”. This is incorrect outside the Foreword, as the word “shall” is for normative standards, rather than for informative standards such as this one. <p>See Comment UK 1 from SC27N8127_DoC_3rdWD_29147_N7901.</p>	Replace the word “shall” with “should” in this sentence.	Accept change of "shall" to should
US 50.	8.6 Anticipated Response Times and	Para 1 Sent 1	Te	<p>The editor did not follow the Disposition of Comments for this sentence.</p> <ul style="list-style-type: none"> The editor misinterpreted the DoC to mean that 	Replace the word “shall” with “should” in this sentence.	Accept change of "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.

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
	Actions			<p>all instances of the word “should” in the draft should be replaced with “shall”. This is incorrect outside the Foreword, as the word “shall” is for normative standards, rather than for informative standards such as this one.</p> <p>See Comment UK 1 from SC27N8127_DoC_3rdWD_29147_N7901.</p>		
US 51.	8.7 Role of a Coordinator	Last Para Sent 1	Te	<p>The editor did not follow the Disposition of Comments for this sentence.</p> <ul style="list-style-type: none"> The editor misinterpreted the DoC to mean that all instances of the word “should” in the draft should be replaced with “shall”. This is incorrect outside the Foreword, as the word “shall” is for normative standards, rather than for informative standards such as this one. <p>See Comment UK 1 from SC27N8127_DoC_3rdWD_29147_N7901.</p>	Replace the word “shall” with “should” in this sentence.	Accept change of "shall" to should
US 52.	9.0 Disseminating of Vulnerability Information	Para 1 Sent 3	Te	<p>The editor did not follow the Disposition of Comments for this sentence.</p> <ul style="list-style-type: none"> The editor misinterpreted the DoC to mean that all instances of the word “should” in the draft should be replaced with “shall”. This is incorrect outside the Foreword, as the word “shall” is for normative standards, rather than for informative standards such as this one. <p>See Comment UK 1 from SC27N8127_DoC_3rdWD_29147_N7901.</p>	Replace the word “shall” with “should” in this sentence.	Accept change of "shall" to should
US 53.	9.1 Dissemination	Para 1 Sent 1	Te	<p>The editor did not follow the Disposition of Comments for this sentence.</p>	Replace the word “shall” with “should” in this sentence.	Accept change of "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.

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
	Formatting			<ul style="list-style-type: none"> The editor misinterpreted the DoC to mean that all instances of the word "should" in the draft should be replaced with "shall". This is incorrect outside the Foreword, as the word "shall" is for normative standards, rather than for informative standards such as this one. See Comment UK 1 from SC27N8127_DoC_3rdWD_29147_N7901.		
US 54.	9.1 Dissemination on Formatting	Para 2 Sent 1	Te	The editor did not follow the Disposition of Comments for this sentence. <ul style="list-style-type: none"> The editor misinterpreted the DoC to mean that all instances of the word "should" in the draft should be replaced with "shall". This is incorrect outside the Foreword, as the word "shall" is for normative standards, rather than for informative standards such as this one. See Comment UK 1 from SC27N8127_DoC_3rdWD_29147_N7901.	Replace the word "shall" with "should" in this sentence.	Accept change of "shall" to should
US 55.	A.2 Vulnerability Disclosure Format	Para 1 Sent 1	Te	The editor did not follow the Disposition of Comments for this sentence. <ul style="list-style-type: none"> The editor misinterpreted the DoC to mean that all instances of the word "should" in the draft should be replaced with "shall". This is incorrect outside the Foreword, as the word "shall" is for normative standards, rather than for informative standards such as this one. See Comment UK 1 from SC27N8127_DoC_3rdWD_29147_N7901.	Replace the word "shall" with "should" in this sentence.	Accept change of "shall" to should
US 56.	A.2 Vulnerability	Para 2	Te	The editor did not follow the Disposition of Comments for	Replace the word "shall" with "should" in	Accept change of "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.

Attachment 4 to SC 27 N8672
[US] comments on ISO/IEC 4th WD 29147

Date: 2010-MM-DD	Document: SC 27 N8126
------------------	------------------------------

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
	y Disclosure Format	Sent 2		<p>this sentence.</p> <ul style="list-style-type: none"> The editor misinterpreted the DoC to mean that all instances of the word “should” in the draft should be replaced with “shall”. This is incorrect outside the Foreword, as the word “shall” is for normative standards, rather than for informative standards such as this one. <p>See Comment UK 1 from SC27N8127_DoC_3rdWD_29147_N7901.</p>	this sentence.	
US 57.	A.2 Vulnerability Disclosure Format	Last Para Sent 1	Te	<p>The editor did not follow the Disposition of Comments for this sentence.</p> <ul style="list-style-type: none"> The editor misinterpreted the DoC to mean that all instances of the word “should” in the draft should be replaced with “shall”. This is incorrect outside the Foreword, as the word “shall” is for normative standards, rather than for informative standards such as this one. <p>See Comment UK 1 from SC27N8127_DoC_3rdWD_29147_N7901.</p>	Replace the word “shall” with “should” in this sentence.	Accept change of “shall” to should
US 58.	B.5 Samples of Good and Bad Disclosure	various	Te	<p>Per ISO IEC Directives Part 2 section D.1.3: “Trade names (brand names) and archaic and colloquial terms shall be avoided.”</p> <p>Per ISO IEC Directives Part 2 section 6.6.3: “6.6.3 Use of trade names A correct designation or description of a product shall be given rather than a trade name (brand name). Proprietary trade names (i.e. trade marks) for a particular product should as far as possible be avoided, even if they</p>	<p>Remove the following entries in the section: “AppRiver servers as a recent example of excellent disclosure handling: http://holisticinfosec.blogspot.com/2009/08/appriver-saas-security-provider-sets.html Ameriprise/American Express as a example of disclosure handling gone wrong:</p>	Accept in principle see US 58 Editor Note: Editor will remove aspects of trademark names including links but creating references of what not to do are good aspects to avoid

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.

Attachment 4 to SC 27 N8672
[US] comments on ISO/IEC 4th WD 29147

Date: 2010-MM-DD	Document: SC 27 N8126
------------------	------------------------------

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
				are in common use” The brand names of AppRiver and Ameriprise/American Express are used without permission from AppRiver and Ameriprise/American Express in the text, and are also present when the URLs are followed.	http://holisticinfosec.blogspot.com/2009/08/appriver-saas-security-provider-sets.html http://holisticinfosec.blogspot.com/2008/12/online-finance-flaw-american-express.html “	

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.

Attachment 4 to SC 27 N8672
[US] comments on ISO/IEC 4th WD 29147

Date: 2010-MM-DD	Document: SC 27 N8126
------------------	------------------------------

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.

Attachment 5 to SC 27 N8672

ZA comments on ISO/IEC 4th WD 29147

Date: 2010-03-15	Document: SC 27 N8126
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

ZA 1	All	All	ge	<p>It seems strange that the dispositions on comments for the 3rd WD were either “accepted” or “not accepted”.</p> <p>Common dispositions in ISO/IEC committees are:</p> <ul style="list-style-type: none"> - Accepted - Accepted in Principle - Rejected - Withdrawn - Overtaken by events 	Not applicable.	Accept in principle Editors Note: Due to the editors absence it was agreed that comments would only be processed as either “accepted” or “not accepted”.
ZA 2	All	All	ge	<p>This International Standard should be a requirements standard, i.e. it should be possible to claim conformance against requirements stated as “shall”. Normative content must be provided.</p> <p>The resolution for the same comment on the 3rd WD stated: <i>“Not Accepted. The purpose of this IS is to be a guideline, since most implementations of an application security response and vulnerability handling policy are dependent on the business decisions and resources of the vendor.”</i> This does not make sense, because using the same argument, International Standards such as ISO/IEC 27001 and ISO/IEC 12207 also cannot be normative.</p> <p>Also, there are enough guidelines around for this topic. What is necessary is an International Standard that gives specific direction. The requirements can be generic to the same level as management standards such as ISO 9000, ISO/IEC 27001. Other existing guidelines can be used to state the specific detail on how the organisation</p>	<p>Change the purpose to be a requirements standard, not a guideline.</p> <p>Adapt the current content to enable:</p> <ul style="list-style-type: none"> - Conformance by a user/consumer to e.g. processes for vulnerability detection and disclosure. - Conformance by a supplier to processes to e.g. handle vulnerability disclosure, updating of products, dissemination. - Normative content of information items such as policies, receipts, reports, etc. 	Not Accepted Editors Note: The content of this IS strictly a guideline and as such does not have any normative references.

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.

Attachment 5 to SC 27 N8672

ZA comments on ISO/IEC 4th WD 29147

Date: 2010-03-15	Document: SC 27 N8126
------------------	-----------------------

1	2	(3)	4	5	(6)	(7)
NB	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				<p>addresses the requirement.</p> <p>Another way to look at this is to use ISO/IEC 15288 as an analogy. ISO/IEC 15288 states normative requirements for system life processes. ISO/IEC 29148 will provide additional information on the requirements engineering specific processes and normative requirements regarding information items for requirement specification. ISO/IEC 27001 mentions vulnerability management. This International should add the requirements for responsible vulnerability disclosure processes and information items.</p> <p>ISO/IEC 27010 can also be used as an example. The document makes provision for both normative requirements and guidelines.</p>		
ZA 3	All	All	te	<p>Some concepts, e.g. system, component, service, are used without an introduction. Also, a number of issues need to be clarified in order to understand the context of the International Standard.</p> <p>A number of stakeholders are mentioned in the document, e.g. finder and vendor. However these entities are not introduced or their relationships with each other explained.</p> <p>In general, the audiences of International Standards are not limited to the arena that the International Standards address. Thus, it would be good practice to clarify concepts before using them.</p> <p>It is important to note that the “Terms and definitions” clause is not the place to do this.</p>	<p>Add a clause</p> <p>5 <i>Concepts</i></p> <p>5.1 Products and services</p> <p>5.2 Vulnerabilities</p> <p>5.3 Stakeholders</p> <p>5.3.1 Supplier</p> <p>5.3.2 Finder</p> <p>...etc.</p>	Accepted ZA to provide the content to the editor.
ZA 4	All	All	te	The scope of this document is the responsible disclosure	Clarify the scope, making clear the	Not Accepted the experts agreed that

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	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				<p>of vulnerabilities in products and services, and probably more specific, products of the shelf and services that are publicly available.</p> <p>Thus, systems and products developed under contract by a supplier for a specific acquirer are not applicable. Services that are supplied under contract are not applicable.</p> <p>Vulnerability disclosure in such cases will be addressed in the contract, support or service contract.</p> <p>Examples for further elaboration:</p> <ol style="list-style-type: none"> 1. a “public” service is provided using a “private” product 2. a “private” service is provided using a public product. <p>In these cases, the “public” side will be addressed using this standard, and the private side through the applicable contract. Thus, in the first example, this standard is used to disclose the vulnerability to the service provider, who will then determine if the vulnerability is due to a vulnerability in the product. This will be addressed further in terms of the applicable contract.</p> <p>In the second example, if a vulnerability is found by the client of the service, and reported via the applicable procedures, the provider can use this standard to disclose any contributing vulnerabilities in the product.</p> <p>See also the requirements for incident management in clause 8.1 of ISO/IEC 2nd FCD 20000-1, <i>Information technology - Service management - Part 1: Service</i></p>	<p>scenarios in which this standard are applicable:</p> <p>“This International Standard is applicable to the responsible disclosure of vulnerabilities in products and publicly available services. Systems and products developed under contract by a supplier for a specific acquirer are not applicable. Services that are supplied under contract are not applicable.”</p>	<p>this aspect is not in scope to the project.</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.

Attachment 5 to SC 27 N8672

ZA comments on ISO/IEC 4th WD 29147

Date: 2010-03-15	Document: SC 27 N8126
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				<i>management system requirements.</i> (Isn't the discovery of a vulnerability an incident?)		
ZA 5	All	All	te	Although the term <i>service</i> is commonly used and understood, it may be necessary to add a definition the make the context of the document clearer.	Propose the definition in ISO/IEC 2 nd FCD 20000-1: service means of delivering value to customers by facilitating results customers want to achieve without the ownership of specific costs and risks NOTE 1 Service is generally intangible. NOTE 2 Service may also be provided by a supplier to the service provider.	Not accepted. Refer to US 14 to merge service definition with current online services definition.
ZA 6	All	All	te	Use of the term "vendor" is misleading, and incorrect. Also, using this term does not fit in with the use of ISO/IEC 12207, remembering that 12207 does not only focus on development, but any form of acquisition of a system, as well as the whole life cycle of a system. The WG is kindly reminded that - this is an International Standard, - ISO/IEC standards should preferably adhere to other ISO standards, - the audience is not limited to English speaking people, - the audience is not limited to people from the "vulnerability disclosure" etc. community, - the audience is not limited to "subject matter experts" who may understand what they mean by a word,	Replace "vendor" with "supplier", giving the ISO/IEC 12207:2008 definition for "supplier".	Accept in principle Editors Note: Editor will add a note in document requesting comments on this change and its potential impact to the overall document.

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	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				<p>although it is used incorrectly, and</p> <p>- the WG has an obligation to ensure that a document is easily translatable.</p> <p>According to the Concise Oxford English dictionary, a vendor is <i>a person or company offering something for sale</i>. This is consistent with the everyday use of the term, i.e., the focus is on <i>selling</i>. Translations for French, Russian and German seem to convey the same meaning.</p> <p>Examples for further clarification:</p> <p>When I go to my local software shop, <i>Pete's software</i>, to buy a copy of <i>Lotus Notes</i>, then <i>Pete's software</i> is the vendor. Potential vulnerabilities in <i>Lotus Notes</i> should be reported to Lotus, not to Pete.</p> <p>The same holds when I buy a Cisco switch from <i>Pete and sons IT suppliers</i>. A potential vulnerability must be reported to CISCO, not to <i>Pete and sons IT suppliers</i>, who is the vendor.</p> <p>(I could have bought the items directly from Lotus or Cisco on their web-site, in which case they would have been the vendor. That is, however, irrelevant.)</p> <p>Even if a support or maintenance contract states that vulnerabilities are to be reported via the vendor or service provider, the organisation that will have to address the vulnerability is the originators of the product.</p> <p>According to the Concise Oxford English dictionary, a supplier is someone who makes something available to someone else. This is a wider concept than vendor.</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.

Attachment 5 to SC 27 N8672
ZA comments on ISO/IEC 4th WD 29147

Date: 2010-03-15	Document: SC 27 N8126
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				<p>ISO/IEC 12207:2008 and ISO/IEC 15288:2008 define <i>supplier</i> as <i>the organization or individual that enters into an agreement with the acquirer for the supply of a product or service</i>, and states that a supplier could be a contractor, producer, seller, or vendor.</p> <p>Within the context of a product life cycle, the agreement processes define the activities necessary to establish an agreement between two organizations. If the Acquisition Process is invoked, it provides the means for conducting business with a supplier of products that are supplied for use as an operational system, of services in support of an operational system, or of elements of a system being developed by a project. If the Supply Process is invoked, it provides the means for conducting a project in which the result is a product or service that is delivered to the acquirer. (See ISO/IEC 12207, clause 5.)</p>		
ZA 7	Front page	Title	ed	Inconsistency in dashes.	Replace "techniques -- Responsible" with "techniques – Responsible"	Accepted see US 1
ZA 8	1	par. 2	te	Possible better sentence construction.	Replace "The vendor can " with "Vendors can "	Accept will change accordingly
ZA 9	1		te	Vulnerability disclosure is part of the larger requirement for information security management. It is crucial to	Add the following to the scope: "In the context of information security	Accept in principle

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.

Attachment 5 to SC 27 N8672
ZA comments on ISO/IEC 4th WD 29147

Date: 2010-03-15	Document: SC 27 N8126
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

				identify this connection in order for users of the International Standard to understand this fact.	management, vulnerability disclosure is part of the information security incident management process. It is also relevant to the management of technical vulnerabilities. See ISO/IEC 27002 for more information.	
ZA 10	3	par. 1	te	Incorrect sentence.	"For the purposes of this document, the terms and definitions given in ISO/IEC 27000, and the following apply."	Not Accepted see UK 36
ZA 11	3.2	vendor	te	As was explained in a previous ZA comment, the term <i>vendor</i> is incorrectly used. A vendor does not necessarily develop the product, or maintains it. Thus the definition is incorrect. Also with reference to the previous comment, it is not even necessary to refer to a vendor, unless the reporting structure requires involvement of the organisation that sold the product.	Remove the definition for vendor. Add a definition for supplier.	Accept in Principle Editors Note: The editor will add a note to the next version to obtain comments on the use of supplier rather than vendor
ZA 12	3.7	update	te	Updates to software are not restricted to addressing vulnerabilities. Rather make distinction between updates and security updates. Also, the current definition is not sufficient. (This proposed distinction is important because the term <i>update</i> is used extensively in everyday "IT language", irrespective of the context in which it is used in this document.)	software update maintenance change or addition to a software product to correct anomalies or improve usability security update software update to correct vulnerabilities or improve security	Not Accepted see BE 4
ZA 13	7	All	ed	Inconsistent use of case when referring to "finder".	Replace "Finder" with "finder"	Accept
ZA 14	8	All	te	Hanging paragraphs shall be avoided since reference to them is ambiguous. (Directives part 2, clause 5.2.4)	Introduce the necessary clause heading to remove hanging paragraphs.	Accept

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.

Attachment 5 to SC 27 N8672
ZA comments on ISO/IEC 4th WD 29147

Date: 2010-03-15	Document: SC 27 N8126
------------------	------------------------------

1	2	(3)	4	5	(6)	(7)
NB	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
ZA 15	8.3	Par. 3	ed	Inconsistent use of bullets in lists.	Use either · or – The preference is – to conform to the ISO template and thus contributing to consistency across ISO publications.	Accept
ZA 16	9	All	te	Hanging paragraphs shall be avoided since reference to them is ambiguous. (Directives part 2, clause 5.2.4)	Introduce the necessary clause heading to remove hanging paragraphs.	Accept will remove hanging paragraphs.
ZA 17	Annex A	All	te	The references to specific suppliers may create the impression of endorsing those suppliers. Even referencing specific CERTs may create a problem. Using existing policies and forms from existing organisations as examples has the risk of becoming outdated. See also the requirements stated in the ISO/IEC directives clause 6.6.3.	Do not use existing policies, forms and advisories as examples. Use them as input to create new generic examples (organisation neutral). This can also contribute to normative information items.	Not accepted See ZA2 No references to normative references
ZA 18	All	All	Ge	A number of references are made to CERT, CSIRT, SIRT, albeit informational. Does this not indicate that some connection exists between this document and ISO/IEC 27035, <i>Information technology – Security techniques – Information security incident management</i> , even if it is just a reference?	Not applicable. Clarification requested.	Accept in Principle
ZA 19	All	All	Ge	How applicable is ISO/IEC 27010, <i>Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications</i> to this document?	Not applicable. Clarification requested.	Accept in Principle

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.