Comments on SP-800-137 Initial Public Draft

Date: 2011-MM-DD	Document: **SP-800-137 Initial Public Draft**

1	2	(3)	4	5	(6)
MS	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[1]	**Comment (justification for change) by Microsoft**	**Proposed change by Microsoft**
[MS] 1	1.5	Page 4	Te	The description of Ch 2 below is not consistent with the actual writing in Ch 2. "Chapter Two describes the fundamentals of ongoing management of information security in support of risk management"	Please replace "ongoing management" with "ongoing monitoring"
[MS] 2	2.1	Page 11	Te	Potential missing text after the word "to" in the below. "promotes ongoing control of operations to within organizational risk tolerances"	Please provide the missing text after the word "to" in the below. "promotes ongoing control of operations to within organizational risk tolerances"
[MS] 3	Ch 3	Page 19	Te	The first and the second sentences are not in-sync. "A well designed information security continuous monitoring strategy encompasses security control assessment, security status monitoring, and security status reporting in support of timely risk-based decision making throughout the organization. The five tenets key to any continuous monitoring program described above in Chapter 2 and in Appendix G of NIST SP 800-37 are: configuration management and change control; security impact analysis; security control assessments; security status reporting; and active involvement of management."	Please replace "security status monitoring" with "security impact analysis" in the first sentence.
[MS] 4	3.1.1	Page 21	Te	We are not sure what the "organization-wide tools" mentioned in the below are. "Policy and procedures for implementation and use of organization-wide tools"	Please clarify what the "organization-wide tools" mentioned in the sentence are. They may be the tools for automation in continuous monitoring, but we are not sure.
[MS] 5	3.1.1	Page 23	Te	It is not clear what these "available tools from OMB lines of business and/or third party vendors" are or where they come from. "Expected Input: Organizational risk assessment and current risk tolerance, current threat information, organizational expectations and priorities, available tools	Please clarify what the "available tools from OMB lines of business and/or third party vendors" are or where they come from.

1 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)
MS	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[1]	**Comment (justification for change) by Microsoft**	**Proposed change by Microsoft**
				from OMB lines of business and/or third party vendors"	
[MS] 6	3.1.1	Page 23	Te	Due to the bullet of "Analyze potential security impact to organization and mission/business functions resulting from changes to information systems and their environments..." in the previous para, it seems that the "Expected Input" should include "changes to information systems and their environments". "Expected Input: Organizational risk assessment and current risk tolerance, current threat information, organizational expectations and priorities, available tools from OMB lines of business and/or third party vendors"	Please include "changes to information systems and their environments" to the "Expected Input".
[MS] 7	3.1.1	Page 23	Te	Due to the bullet of "Take steps to respond to risk as needed (e.g., request new or revised measures and metrics, additional or revised assessments, modifications to existing common or PM security controls, or additional controls)" in the previous para, it seems that the "Expected Output" should include "modifications to existing common or PM security controls, or additional controls)" "Expected Output: Updated information on organizational risk tolerance, organization-wide continuous monitoring strategy and associated policies, procedures, templates, tools"	Please include "modifications to existing common or PM security controls, or additional controls)" to the "Expected Output".
[MS] 8	3.1.2	Page 24	Te	The below bullet seems to be too low level for being part of the "Information System (Tier 3) Continuous Monitoring Strategy". Perhaps, "defining remediation actions based on the potential results of ongoing monitoring activities" may be more appropriate. Leave "conducting" part to the "Respond to findings" process element in Ch 3.6 "Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the plan of action and milestones	Please replace "Conduct remediation actions based on the results of ongoing monitoring activities" with "Define remediation actions based on the potential results of ongoing monitoring activities".

1 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Comments on SP-800-137 Initial Public Draft

Date: 2011-MM-DD	Document: **SP-800-137 Initial Public Draft**

1	2	(3)	4	5	(6)
MS	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[1]	**Comment (justification for change) by Microsoft**	**Proposed change by Microsoft**
				[Respond; RMF Step 6]"	
[MS] 9	3.1.2	Page 24	Te	It seems that the "documented remediation actions" should be part of the "Expected Output". "Expected Output: System-level continuous monitoring strategy that complements the Tier 1 and 2 strategies and the organizational security program and that provides security status information for all tiers and real-time updates to system authorization decision information as directed by the organizational continuous monitoring strategy"	Please include "documented remediation actions" to the "Expected Output".
[MS] 10	Table 3-1	Page 27	Te	"Example" rather than "Sample" in the below. "Sample Metric and Related Measures at Each Tier"	Please replace "Sample" with "Example"
[MS] 11	3.2	Page 27	Te	Please clarify that this process element is about "establishment of measures and metrics" and not the "carrying out of measures and metrics" in the "Expected Output" below. "Expected Output: Measures and metrics to convey security status and security control effectiveness at all three tiers, and to give recipients/users of reports visibility into assets, awareness of vulnerabilities and knowledge of threats"	Please replace "Measures and metrics to convey security status and security control effectiveness at all three tiers, and to give recipients/users of reports visibility into assets" with "Establishment of measures and metrics to convey security status and security control effectiveness at all three tiers for giving recipients/users of reports visibility into assets"
[MS] 12	3.4	Page 33	Te	It is unclear what the security-related information in the "Expected Output is". Perhaps it is the "security-related information resulting from the continuous monitoring program"? "Expected Outputs: Security-related information"	Please replace "security-related information" with "security-related information resulting from the continuous monitoring program"
[MS] 13	3.5	Page 34	Te	It is unclear what the security-related information in the "Expected Input is". Perhaps it is the "security-related information resulting from the continuous monitoring program"?	Please replace "security-related information" with "security-related information resulting from the continuous monitoring program"

1 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)
MS	**Clause No./ Subclause No./ Annex** (e.g. 3.1)	**Paragraph/ Figure/Table/ Note** (e.g. Table 1)	**Type of com-ment**[1]	**Comment (justification for change) by Microsoft**	**Proposed change by Microsoft**
				"Expected Input: Security-related information, organizational continuous monitoring strategy, reporting requirements"	
[MS] 14	3.6	Page 36	Te	It may seem clearer to say "mitigations of identified weaknesses" rather than "mitigated weaknesses" in the below "Expected Output". "Expected Output: Mitigated weaknesses, updated system security information (e.g., system security plans, POA&Ms, security assessment reports), updated security status reports"	Please replace "mitigated weaknesses" with "mitigations of identified weaknesses".
[MS] 15	3.6	Page 36	Te	The removal of the concerned system's authorization potential should be part of the Expected Output. "Expected Output: Mitigated weaknesses, updated system security information (e.g., system security plans, POA&Ms, security assessment reports), updated security status reports"	Please include "concerned system's authorization" in the Expected Output.

1 **Type of comment:** **ge** = general **te** = technical **ed** = editorial
NOTE Columns 1, 2, 4, 5 are compulsory.