



Security Management Maturity Questionnaire (SMMQ)

Questionnaire v1.0
July 27, 2011

Department of Homeland Security
Federal Network Security Branch



This document was prepared for the United States Department of Homeland Security.

SEI Administrative Agent
ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2100

The ideas and findings in this report should not be construed as an official U.S. Government or U.S. Agency (including, but not limited to DoD or DHS) position. It is published in the interest of scientific and technical information exchange.

This work is sponsored by the U.S. Department of Homeland Security. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

Copyright 2011 Carnegie Mellon University.

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

Internal use. Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use. This document may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

This work was created with the funding and support of the U.S. Department of Homeland Security under the Federal Government Contract Number FA8721-05-C-0003 between the U.S. Department of Defense and Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this page.



Introduction

This document contains statements and questions about the implementation of important security program management practices in your organization. The Department of Homeland Security (DHS), Federal Network Security Branch (FNS) sponsored the development of this questionnaire, which is intended to be used as part of the annual FISMA data gathering process executed by FNS. Specifically, this questionnaire examines several domains of an organization's management of its security program. The scoring of this survey yields a Maturity Indicator Level (MIL) for each domain. The nine domains examined are listed below:

1. Compliance Management
2. Policy Development and Enforcement
3. Governance and Oversight
4. Security Program Planning
5. Human Resource Management
6. Training and Awareness
7. Financial Management
8. Risk Management
9. Security Operations Management

A short description of each domain precedes each group of statements.

For each domain, the first set of statements deals with base practices specific to that domain. The following sets of statements address increasing indications of maturity in each of the domains. The base practice statements are unique to each domain. The maturity indicator questions are common across each domain.



Maturity Indicator Levels Defined

The following defines each MIL and describes the questions used to test for indicators of maturity at each level.

MIL0 Incomplete

Indicates that at least one base practice is not being performed as measured by responses to the relevant questions. If MIL0 is assigned, no further assessment of maturity is performed.

MIL1 Performed

Indicates that all base practices are being performed as measured by responses to the relevant questions. MIL1 means that there is sufficient and substantial support for the existence of the practices. Once MIL1 is attained, questions related to higher MIL levels are asked.

MIL2 Planned

Indicates that the base practices of the domain are performed and the activities of the domain are supported by planning, stakeholders, and relevant standards and guidelines. The activities of a planned domain are

- conducted according to a documented plan
- supported by stakeholders (Are the stakeholders of the domain known and are they aware of their roles in domain activities?)
- supported by relevant standards and guidelines (Have the standards and guidelines that support the practice been identified and implemented?)
- governed by organizational policy

MIL3 Managed

Indicates that the base practices of the domain are performed, the activities of the domain are planned, and there is basic infrastructure in place to support the activities of the domain. The activities of a managed domain

- are governed by the organization (Is there appropriate oversight over the performance of the activities of the domain?)
- are appropriately staffed and adequately funded (Are the staff and funds necessary to perform the activities of the domain as intended available?)
- are assigned to staff who are responsible and accountable for their performance (Have staff been assigned to perform the activities of the domain and are they responsible and accountable for that performance?)
- are performed by staff who are adequately skilled and trained
- produce work products that are expected from performance of those activities, which are placed under appropriate levels of configuration control



- are managed for risk (Are risks related to the performance of the practice identified, analyzed, dispositioned, monitored, and controlled?)

MIL4 Measured

Indicates that the base practices of the domain are performed and the activities of the domain are planned, managed, and measured. The activities of a measured domain are

- periodically evaluated for effectiveness (Are the activities of the domain periodically reviewed to ensure that they are effective and producing intended results?)
- monitored and controlled (Are appropriate implementation and performance measures identified, applied, and analyzed?)
- objectively evaluated against practice descriptions and plans (Are the activities of the domain periodically evaluated to ensure that they adhere to related practice descriptions and the plans for those practices?)
- periodically reviewed with higher level managers (Are higher level managers aware of any issues related to the performance of the activities of the domain?)

MIL5 Defined

Indicates that the base practices of the domain are performed and the activities of the domain are planned, managed, measured, and consistent across all internal constituencies who have a vested interest in the performance of those activities. A defined domain ensures that the organization reaps the benefits of consistent performance of its activities across organizational units and that all organizational units can benefit from improvements realized in any organizational unit. At MIL5, the activities of the domain

- are defined by the organization and tailored by organizational units for their use (Is there an organization-sponsored definition of the domain's activities from which organizational units can derive activities that fit their unique operating circumstances?)
- are supported by improvement information that is collected by and shared among organizational units for the overall benefit of the organization (Are improvements to activities documented and shared across internal constituencies so that the organization as a whole reaps benefits from these improvements?)



Instructions

To the right of each statement, there are boxes for the six possible responses: Yes, Likely Yes, Equally Likely, Likely No, No, and Don't Know.

Use the following criteria to determine which option to check based upon your knowledge of the organization:

- **Yes:** The statement describes an activity that is definitely performed in the organization.
- **Likely Yes:** The statement describes an activity that is most likely performed in the organization (~ 75% probability of yes).
- **Equally Likely:** The statement describes an activity that is equally likely to be performed or not performed in the organization (~50% probability of yes).
- **Likely No:** The statement describes an activity that is most likely not performed in the organization (~ 25% probability of yes).
- **No:** The statement describes an activity that is definitely not performed in the organization.
- **Don't Know:** You are not aware of or are uncertain about the existence of the practice.

Begin with the Base Practices questions in Domain Area 1. Check one of the boxes for each statement. Follow the instructions at the end of the section to record your MIL score and proceed through the questionnaire. (MIL0 is selected by default for each domain.)

If you wish to comment on any statements or questions or qualify your answers, please use the comments space provided at the end of this document with an appropriate statement or question reference number.



Organization Information – for the Organization Being Assessed

Organization Name (include division if applicable)

Address Line 1

Address Line 2

City

State

Postal Code

Web Site

Contact Information – for Person Completing the Assessment

First Name

Last Name

Title

Address Line 1

Address Line 2

City

State

Postal Code

Phone

Email

Functional Area



Domain Area 1: Compliance Management

Compliance management addresses the activities related to managing compliance with externally imposed information security obligations such as standards, policies, regulations, and legislation.

	Yes	Likely Yes	Equally Likely	Likely No	No	Don't Know
Base Practices	1. There is an up-to-date inventory of compliance obligations.					
	2. The inventory of compliance obligations is analyzed for conflicts and duplicate obligations.					
	3. Data collected to satisfy compliance obligations is stored in a repository and can be accessed for other business purposes.					
MIL2-Planned	4. There is a plan for performing compliance activities.					
	5. The stakeholders for compliance activities have been identified.					
	6. Compliance activities are supported by relevant standards and guidelines.					
	7. There is an organizational policy for compliance.					
MIL3-Managed	8. There is oversight over the performance of compliance activities.					
	9. Appropriate staff are assigned to perform compliance activities.					
	10. There is adequate funding to perform compliance activities.					
	11. Risks related to the performance of compliance activities are identified, analyzed, dispositioned, monitored, and controlled.					



	Yes	Likely Yes	Equally Likely	Likely No	No	Don't Know
MIL4-Measured						
MIL5-Defined						



Domain Area 2: Policy Development and Enforcement

Policy development and enforcement addresses the activities related to managing internal information security policies, such as policies regarding passwords.

	Yes	Likely Yes	Equally Likely	Likely No	No	Don't Know
Base Practices	1. Information security policies are developed, regularly updated, communicated to constituents, and enforced.					
	2. There is a disciplinary process established for security policy violations.					
	3. There is visible sponsorship from higher level managers for the information security program.					
MIL2-Planned	4. There is a plan for performing policy development and enforcement activities.					
	5. The stakeholders for policy development and enforcement activities have been identified.					
	6. Policy development and enforcement activities are supported by relevant standards and guidelines.					
	7. There is an organizational policy for policy development and enforcement.					
MIL3-Managed	8. There is oversight over the performance of policy development and enforcement activities.					
	9. Appropriate staff are assigned to perform policy development and enforcement activities.					
	10. There is adequate funding to perform policy development and enforcement activities.					
	11. Risks related to the performance of policy development and enforcement activities are identified, analyzed, dispositioned, monitored, and controlled.					



	Yes	Likely Yes	Equally Likely	Likely No	No	Don't Know
MIL4-Measured	12. Policy development and enforcement activities are periodically reviewed to ensure they are effective and producing intended results.					
	13. Policy development and enforcement activities are periodically reviewed to ensure they are adhering to the plan.					
	14. Appropriate measures for policy development and enforcement activities are identified, applied, and analyzed.					
	15. Higher level managers are aware of any issues related to policy development and enforcement.					
MIL5-Defined	16. Policy development and enforcement activities are performed consistently across all internal constituencies.					
	17. Improvements to policy development and enforcement activities are shared across internal constituencies.					



Domain Area 3: Security Governance and Oversight

Security governance and oversight addresses the organization’s practices for ensuring that the goals of security management activities are being achieved as expected.

	Yes	Likely Yes	Equally Likely	Likely No	No	Don't Know
Base Practices	1. A governance structure has been developed and implemented to provide oversight over security activities.					
	2. Roles and responsibilities for security governance have been developed and assigned.					
	3. There is a governance dashboard or scorecard for information security management.					
MIL2-Planned	4. There is a plan for performing governance activities.					
	5. The stakeholders for governance activities have been identified.					
	6. Governance activities are supported by relevant standards and guidelines.					
	7. There is an organizational policy for governance.					
MIL3-Managed	8. There is oversight over the performance of governance activities.					
	9. Appropriate staff are assigned to perform governance activities.					
	10. There is adequate funding to perform governance activities.					
	11. Risks related to the performance of governance activities are identified, analyzed, dispositioned, monitored, and controlled.					



	Yes	Likely Yes	Equally Likely	Likely No	No	Don't Know
MIL4-Measured						
MIL5-Defined						



Domain Area 4: Security Program Management

Security program management concerns the activities associated with designing, building, and implementing a security program.

	Yes	Likely Yes	Equally Likely	Likely No	No	Don't Know
Base Practices	<ol style="list-style-type: none"> 1. Descriptions of security program management activities are established in a service repository or catalog as a service offering to the organization. 2. Critical success factors for security program activities are established (and maintained). 3. There are architecture and design guidelines for the security management program. 					
MIL2-Planned	<ol style="list-style-type: none"> 4. There is a plan for performing security program management activities. 5. The stakeholders for security program management activities have been identified. 6. Security program management activities are supported by relevant standards and guidelines. 7. There is an organizational policy for security program management. 					
MIL3-Managed	<ol style="list-style-type: none"> 8. There is oversight over the performance of security program management activities. 9. Appropriate staff are assigned to perform security program management activities. 10. There is adequate funding to perform security program management activities. 11. Risks related to the performance of security program management activities are identified, analyzed, dispositioned, monitored, and controlled. 					



	Yes	Likely Yes	Equally Likely	Likely No	No	Don't Know
MIL4-Measured						
MIL5-Defined						



Domain Area 5: Human Resource Management

Human resource management deals with the practices for managing the acquisition and deployment of human resources to minimize disruption and exposure. Included are practices for defining and managing job roles for access control purposes.

	Yes	Likely Yes	Equally Likely	Likely No	No	Don't Know
Base Practices	<ol style="list-style-type: none"> 1. There is an established verification and validation program for candidate staff and current staff to evaluate suitability for their role. 2. The community of authorized identities is established and documented. 3. Periodic reviews are performed to identify excessive or inappropriate levels of access granted to an authorized identity. 					
MIL2-Planned	<ol style="list-style-type: none"> 4. There is a plan for performing human resource management activities. 5. The stakeholders for human resource management activities have been identified. 6. Human resource management activities are supported by relevant standards and guidelines. 7. There is an organizational policy for human resource management. 					
MIL3-Managed	<ol style="list-style-type: none"> 8. There is oversight over the performance of human resource management activities. 9. Appropriate staff are assigned to perform human resource management activities. 10. There is adequate funding to perform human resource management activities. 11. Risks related to the performance of human resource management activities are identified, analyzed, dispositioned, monitored, and controlled. 					



	Yes	Likely Yes	Equally Likely	Likely No	No	Don't Know
MIL4-Measured	12. Human resource management activities are periodically reviewed to ensure they are effective and producing intended results.					
	13. Human resource management activities are periodically reviewed to ensure they are adhering to the plan.					
	14. Appropriate measures for human resource management activities are identified, applied, and analyzed.					
	15. Higher level managers are aware of any issues related to human resource management.					
MIL5-Defined	16. Human resource management activities are performed consistently across all internal constituencies.					
	17. Improvements to human resource management activities are shared across internal constituencies.					



Domain Area 6: Training and Awareness

Training and awareness deals with the activities necessary to deliver the training necessary to ensure a broad understanding of the nature and value of security activities and awareness of responsibilities for security.

	Yes	Likely Yes	Equally Likely	Likely No	No	Don't Know
Base Practices	1. Security program management training needs are established.					
	2. Security program management training is provided annually.					
	3. Records of delivered security program management training are maintained.					
MIL2-Planned	4. There is a plan for performing training and awareness activities.					
	5. The stakeholders for training and awareness activities have been identified.					
	6. Training and awareness activities are supported by relevant standards and guidelines.					
	7. There is an organizational policy for training and awareness.					
	8. There is oversight over the performance of training and awareness activities.					
MIL3-Managed	9. Appropriate staff are assigned to perform training and awareness activities.					
	10. There is adequate funding to perform training and awareness activities.					
	11. Risks related to the performance of training and awareness activities are identified, analyzed, dispositioned, monitored, and controlled.					



	Yes	Likely Yes	Equally Likely	Likely No	No	Don't Know
MIL4-Measured						
MIL5-Defined						



Domain Area 7: Financial Management

Financial management deals with the practices for funding security program needs based on their requirements and determining an acceptable level of return on investment.

	Yes	Likely Yes	Equally Likely	Likely No	No	Don't Know
Base Practices	<ol style="list-style-type: none"> 1. Cost of controls implementation, monitoring, and maintenance is known. 2. The security program has an established budget. 3. There is planning for unexpected or off-budget security program financial needs resulting from disruption or incident. 					
MIL2-Planned	<ol style="list-style-type: none"> 4. There is a plan for performing financial management activities. 5. The stakeholders for financial management activities have been identified. 6. Financial management activities are supported by relevant standards and guidelines. 7. There is an organizational policy for financial management. 					
MIL3-Managed	<ol style="list-style-type: none"> 8. There is oversight over the performance of financial management activities. 9. Appropriate staff are assigned to perform financial management activities. 10. There is adequate funding to perform financial management activities. 11. Risks related to the performance of financial management activities are identified, analyzed, dispositioned, monitored, and controlled. 					



	Yes	Likely Yes	Equally Likely	Likely No	No	Don't Know
MIL4-Measured						
MIL5-Defined						



Domain Area 8: Risk Management

Risk management deals with the organization’s practices for incorporating security risk considerations into its overall risk management process. In other words, how does the organization integrate security risk management into enterprise risk management?

	Yes	Likely Yes	Equally Likely	Likely No	No	Don't Know
Base Practices	1. Security requirements that align with the enterprise operational risk strategy are identified or developed.					
	2. Security requirements that align with the enterprise operational risk strategy are implemented.					
	3. An organizational statement of risk tolerance has been established.					
MIL2-Planned	4. There is a plan for performing risk management activities.					
	5. The stakeholders for risk management activities have been identified.					
	6. Risk management activities are supported by relevant standards and guidelines.					
	7. There is an organizational policy for risk management.					
MIL3-Managed	8. There is oversight over the performance of risk management activities.					
	9. Appropriate staff are assigned to perform risk management activities.					
	10. There is adequate funding to perform risk management activities.					
	11. Risks related to the performance of risk management activities are identified, analyzed, dispositioned, monitored, and controlled.					



	Yes	Likely Yes	Equally Likely	Likely No	No	Don't Know
MIL4-Measured						
	12. Risk management activities are periodically reviewed to ensure they are effective and producing intended results.					
	13. Risk management activities are periodically reviewed to ensure they are adhering to the plan.					
	14. Appropriate measures for risk management activities are identified, applied, and analyzed.					
15. Higher level managers are aware of any issues related to risk management.						
MIL5-Defined						
	16. Risk management activities are performed consistently across all internal constituencies.					
17. Improvements to risk management activities are shared across internal constituencies.						



Domain Area 9: Security Operations Management

Security operations management addresses the roles, responsibilities, and authority for executing day-to-day security activities.

	Yes	Likely Yes	Equally Likely	Likely No	No	Don't Know
Base Practices	1. Key security roles within the organization have been identified.					
	2. Responsibilities for security operations have been documented and assigned.					
	3. The services provided by security operations are identified and documented.					
MIL2-Planned	4. There is a plan for performing security operations management activities.					
	5. The stakeholders for security operations management activities have been identified.					
	6. Security operations management activities are supported by relevant standards and guidelines.					
	7. There is an organizational policy for security operations management.					
MIL3-Managed	8. There is oversight over the performance of security operations management activities.					
	9. Appropriate staff are assigned to perform security operations management activities.					
	10. There is adequate funding to perform security operations management activities.					
	11. Risks related to the performance of security operations management activities are identified, analyzed, dispositioned, monitored, and controlled.					



	Yes	Likely Yes	Equally Likely	Likely No	No	Don't Know
MIL4-Measured	12. Security operations management activities are periodically reviewed to ensure they are effective and producing intended results.					
	13. Security operations management activities are periodically reviewed to ensure they are adhering to the plan.					
	14. Appropriate measures for security operations management activities are identified, applied, and analyzed.					
	15. Higher level managers are aware of any issues related to security operations management.					
MIL5-Defined	16. Security operations management activities are performed consistently across all internal constituencies.					
	17. Improvements to security operations management activities are shared across internal constituencies.					

