Considering the Case for Security Content in CMMI for Services

PART ONE, BY EILEEN FORRESTER

Eileen Forrester

Kieran Doyle

October 2010

Introduction

When the original CMMI for Services model team worked on the scope and architecture for the first CMMI-SVC draft in 2006, we considered whether and how to include security content. We ultimately decided against normative model content on security.

However, as use of the CMMI-SVC model grows, we frequently hear from users who would prefer, as they say, that we had simply "given us a PA or two on security," rather than asking them to look outside the model. This is not an issue for those users already combining CMMI-SVC and ITIL or ISO or RMM, but is more acute for those using CMMI-SVC alone and wanting to include security in their improvement program. We did not receive sufficient change requests on this topic to add security content to CMMI-SVC for V1.3, and even if we had, such a change would also have been beyond the scope of the V1.3 revision. Nonetheless, we often and increasingly hear a request from users for CMMI model content more directly on security, especially for CMMI-SVC.

We often and increasingly hear a request from users for CMMI model content about security, especially for CMMI-SVC.

Background

Among the reasons for the decision against normative model content on security were the preferences of the CMMI Architecture Team and the larger CMMI Product Team. In their view at the time, security can be conceived of during development as a class of requirement and a type of risk, and therefore already covered by process areas treating those topics. In addition, several existing models such as ISO 20K and 27K, Cobit, and ITIL have security content available. At that time we also knew that another SEI CERT team was building the Resilience Management Model and including considerable security content. That team has now published their model. Further, in 2008 a team chartered by the CMMI Steering Group began writing an assurance focus topic for the CMMI models. We already regarded these frameworks and materials as complementary to CMMI-SVC and as we worked we did not attempt to include everything they include. We considered them excellent sources of practice information likely to cover the security landscape and chose not to write anything like a process area

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

Phone: 412-268-5800
Toll-free: 1-888-201-4479

www.sei.cmu.edu

for security—or even a goal and practices in an existing PA—in CMMI-SVC V1.2.

Encoding Security Content in a CMMI-Like Form

In the first edition of *CMMI for Services, Guidelines for Superior Service*, Kieran Doyle wrote an essay at my invitation about including security in a SCAMPI appraisal on CMMI-SVC, which garnered attention and praise, and requests to take his work further. A revised essay will appear in the second edition. In addition, during the years before I worked on CMMI-SVC, I was working with colleagues in the SEI CERT program and elsewhere on including security content in CMMI. I still see a need for that content. Kieran and I have also worked as a subteam to a larger team I lead that works on combining CMMI-SVC effectively with other models and approaches. In the course of that work, we have experimented with the idea of what normative model content about security could look like. What follows is a work product from that subteam.

Given the persistence of the requests for fuller content on security to be used with CMMI models, we provide an initial draft here to get community comments and input on whether this content is useful and should be taken further.

We took Kieran's idea of how to shape content from any model into something appraisable and proceeded a step or two further to experiment with model-like or "pseudo PA" content on security. Clearly, this is far from full model content, nor is it presumed to be CMMI content.

We chose an information security scope, though security concerns go beyond information. For example, physical security is often considered as an entire discipline of its own, though it clearly has a relationship to information security. When working with security risk analysis at the SEI, we frequently see how physical security breaches can lead to information security risks. In our view, models like RMM already cover the larger security space admirably, and so we chose a tighter scope for our recent experiments with what CMMI model content would look like.

We have to date experimented only with purpose statement, one note, goals, specific practice statements, some subpractices, and generic practice elaborations. Entirely missing is the informative content that serves as explanatory material and implementation guidance in a CMMI process area; we have not yet written the notes that are crucial to assist with comprehension, implementation, and improvement, for example. Our purpose on the subteam was to examine whether credible content on security could be created at all in a smaller footprint than models like RMM.

Given the persistence of the requests for fuller content on security to be used with CMMI models, we provide it here to begin to get community comments and input. Should this work be taken further? Is the scope useful for improvement? What could be done next to make it more credible? Would you participate in developing it into something fuller? Our call to action is to ask you to take a look

at the example below and provide us with comments by writing to cmmi-comments@sei.cmu.edu.

PART TWO, BY KIERAN DOYLE AND EILEEN FORRESTER

SECURITY MANAGEMENT

A work product to experiment with an example process area structure for CMMI for Services

Purpose

The purpose of Security Management (SM) is to establish and maintain a security management system that safeguards the essential assets of the organization.

Introductory Notes

Essential assets cover such things as the essential functions and resources on which service and the organization depend. They can include, for example, staff and intellectual property of the organization. Some assets may be stored in many different forms, including physical documents, databases, websites, and other forms. Essential assets may also incorporate the computing systems themselves (e.g., servers) and even personnel. See the Service Continuity process area for more information on the essential functions and resources on which services depend. See the Resilience Management Model for more information on defining and safeguarding a range of assets.

Example Specific Goal and Practice Summary

ESG 1 Establish a Security Management System

- ESP 1.1 Establish Security Objectives
- ESP 1.2 Establish an Approach to Threat Assessment
- ESP 1.3 Identify Security Threats
- ESP 1.4 Evaluate and Prioritize Security Threats
- ESP 1.5 Establish a Security Management Plan
- ESP 1.6 Obtain Commitment to the Security Management Plan

ESG 2 Provide Security

- ESP 2.1 Operate the Security Management System
- ESP 2.2 Monitor the Security Management System

Example Specific Practices by Example Goal

ESG 1 Establish a Security Management System

A security management system is established and maintained.

ESP 1.1 Establish Security Objectives

Identify the scope and objectives for the security management system.

ESP 1.2 Establish an Approach to Threat Assessment

Establish and maintain an approach to assessing vulnerabilities and threats to essential assets.

Subpractices

1. Select methods for assessing security threats.
2. Define criteria for evaluating and quantifying security threats.
3. Describe responsibility and resources for evaluating vulnerabilities and threats.

ESP 1.3 Identify Security Threats

Identify and record security threats.

Subpractices

1. Identify security threats.
2. Record information about security threats.
3. Categorize security threats.

ESP 1.4 Evaluate and Prioritize Security Threats

Evaluate each identified security threat using defined criteria and determine its relative priority.

ESP 1.5 Establish a Security Management Plan

Establish and maintain a plan for achieving security objectives.

Subpractices

1. Describe responsibility for treating vulnerabilities and threats.
2. Identify resources for treating vulnerabilities and threats.

ESP 1.6 Obtain Commitment to the Security Management Plan

Obtain commitment to the security management system from all relevant stakeholders.

ESG 2 Provide Security

Security is provided using the security management system.

ESP 2.1 Operate the Security Management System

Implement and operate the agreed security management system.

Subpractices

1. Monitor the status of individual security vulnerabilities and threats.
2. Respond to and prevent security incidents. For more information on incident management, see Incident Resolution and Prevention.
3. Maintain and improve the security management system.

ESP 2.2 Monitor the Security Management System

Monitor the security management system.

Subpractices

1. Monitor the performance of the security management system.
2. Evaluate the effectiveness of security.
3. Consult national and international threat agencies on developments in security issues.

Generic Practice Elaborations

GP 2.1 Establish an Organizational Policy

SM Elaboration

This policy establishes the organizational expectation for defining and operating a security strategy and system.

GP 2.2 Plan the Work

SM Elaboration

This plan for performing the security management process can be included in the work management plan, described in the Work Planning process area. This plan encompasses both the strategy for maintaining security and the specific activities to establish, operate, and maintain the security management system.

GP 2.3 Provide Resources

SM Elaboration

Examples of resources provided for IT related security situations may include the following:

- Modeling and simulation tools
- Malware databases
- Firewalls
- Antivirus software

Examples of resources provided for non-IT related situations may include the following:

- Safes
- Restricted access rooms
- Restricted access file cabinets or other physical locations
- Guard and other security staff

GP 2.4 Assign Responsibility

SM Elaboration

Responsibility is assigned for planning, operating, and monitoring the security management system.

GP 2.5 Train People

SM Elaboration

Examples of training topics may include the following:

- Information security management concepts
- Physical security
- Network security
- Cryptography
- Data encryption
- Protocols

GP 2.6 Manage Configurations

SM Elaboration

Example work products placed under control include the following:

- Antivirus software
- Malware databases
- Security Management System representations
- Security Management plans

GP 2.7 Identify and Involve Relevant Stakeholders

SM Elaboration

Example activities for stakeholder involvement include the following:

- Identifying security objectives
- Gathering information on potential security threats
- Prioritizing security threats
- Reviewing the security management plan

GP 2.8 Monitor and Control the Process

SM Elaboration

Examples of measures and work products used in monitoring and controlling include the following:

- Number and type of security breaches
- Pareto analysis of categories of security incidents
- Schedule for conducting security system audits

GP 2.9 Objectively Evaluate Adherence

SM Elaboration

Examples of activities reviewed include the following:

- Identifying and analyzing security threats
- Operating the security management system
- Certifying and accrediting appropriate assets

Examples of work products reviewed include the following:

- Security management strategy
- Security management plans
- Designs for the security management system

GP 2.10 Review Status with Higher Level Management

SM Elaboration

Reviews of the security management system are held on a periodic and event-driven basis. The status of the security management system and the potential for new and developing security threats are typically considered. In the aftermath of specific security threats (e.g., a cyber attack), reviews may be held with appropriate levels of management to assess the damage to knowledge assets and agree on corrective actions.

GP 3.2 Collect Improvement Information

SM Elaboration

Examples of work products, measures, measurement results, and improvement information include the following:

- Reports on trends in security threat developments
- Reports on lessons learned from security breaches

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with 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.

For information about SEI reports, please visit the library section of the SEI website (www.sei.cmu.edu/library).