Motorola Secure Software Development Model

Francis MAHENDRAN
Motorola Software Group
Singapore

and

Margaret NADWORNY
Motorola Software Group
Schaumburg, IL 60196, USA

ABSTRACT

In today's world, the key to meeting the demand for improved security is to implement repeatable processes that reliably deliver measurably improved security. While many organizations have announced efforts to institutionalize a secure software development process, there is little or no industry acceptance for a common process improvement framework for secure software development. Motorola has taken the initiative to develop such a framework, and plans to share this with the Software Engineering Institute for possible inclusion into its Capability Maturity Model Integration (CMMI®). This paper will go into the details of how Motorola is addressing this issue. The model that is being developed is designed as an extension of the existing CMMI structure. The assumption is that the audience will have a basic understanding of the SEI CMM® / CMMI® process framework.

The paper will not describe implementation details of a security process model or improvement framework, but will address WHAT security practices are required for a company with many organizations operating at different maturity levels. It is left to the implementing organization to answer the HOW, WHEN, WHO and WHERE aspects. The paper will discuss how the model is being implemented in the Motorola Software Group.

Keywords: Security, SEI, CMMI, Assessment, Model

1. INTRODUCTION

The number of malicious attacks on applications increases from year to year. Addressing this issue requires multiple solutions and resources which can have multiple impacts throughout the software development lifecycle. Software security vulnerabilities can be caused by defective specification, design, implementation, inefficient testing, and even in operation. Having high maturity software development practices for quality does not guarantee a secure product, but it does increase the probability of having a more secure product.

It is possible, however, for developers to use processes that consistently produce software which is more secure. This, in turn, requires that development organizations acquire a higher level of security expertise by, identifying processes for producing secure software, adopting them, and consistently using them when they produce, enhance, maintain, and rework the software. Improving software security requires commitment, time and resources for achieving the benefits outlined. However, following the data for quality, these costs are expected to be less than the identification and correction of security vulnerabilities after the software has been released.

In order to have a good set of secure software development processes, it is important to have a good security framework or model. This model can help the organization create and improve secure software development processes.

The Motorola Software Group is an integral part of Motorola providing the technical leadership and expertise to drive next generation software and to deliver cutting edge solutions for Motorola businesses. As a commitment to enhancing Motorola's security software development, the Motorola Software Group has a Software Security program and training initiative that will embed security measures across the whole software development life cycle. The Motorola Software Group has multiple sites across the globe certified for Software Engineering Institute's Capability Maturity Model (CMM®) Level 5 and Capability Maturity Model Integration (CMMI®) Level 5. The input for this security model was a collaborative effort between a cross business team representing Motorola's business units and the Motorola Software Group.

Rather than monitoring whether individual organizations within a specific business unit were conducting security training, reviewing security metrics, and following other security related practices, this team agreed to identify a secure software development model which would inherently measure the organizations ability to follow these recognized practices consistently across the company. This model was created to be compatible with the SEI's CMMI® model while being able to stand on its own if an organization had not adopted the CMMI®. Within the Motorola Software Group, the organizational culture which readily conformed to the CMM® ideal and adoption of the CMMI®, viewed the model as a means to speed up acceptance and deployment across the organization. As Motorola Software Group produces easily 50% of Motorola's software, it was a strategy to quickly introduce these practices throughout Motorola.

2. CURRENT SITUATION

Currently there are several organizations implementing a secure life cycle process, including Microsoft. However, there is no widely accepted common process improvement model for secure software development in the industry. The current, more popular security related models such as the Systems Security

Engineering Capability Maturity Model (SSE-CMM©), the Federal Aviation Administration Integrated Capability Maturity Model (FAA-iCMM®), the INFOSEC Assurance Capability Maturity Model (IA-CMM3.1®), and the BSI British Standards (BS 7799®) do not focus on the software life cycle, and how to make it more secure. The emphasis is more on identifying and removing security vulnerabilities in the product, the environment, controls, platform and the support structure around the application or product. The existing models studied and their objectives will be discussed in more detail below.

SSE-CMM©: **Systems Security Engineering Capability Maturity Model[5].**
This model has 11 security base practices and does address some aspects of the software development life cycle. The model's emphasis, however, is on controls, threats, and discovering and eliminating vulnerabilities. All these practices are not incorporated into a software life cycle approach. This is the reason this particular model was not adopted by Motorola. Some of the practices for the Motorola model, such as "Select the methods, techniques, and criteria by which security system vulnerabilities in a defined environment are assessed analyzed and compared." are borrowed from the SSE-CMM©. This model is very easily compatible with the SEI CMMI®. The base practices, however, are not classified according to the capability levels.

FAA-iCMM®: The Federal Aviation Administration Integrated Capability Maturity Model [7].
This model has twenty Process Areas (PA's) and four Application Area (AA's) consisting of sixteen Application Practices to meet both Security and Safety considerations. The sixteen AA practices defined in the model are used to determine goal satisfaction. There are four goals that are necessary to meet the FAA security considerations. The same concepts apply to process capability levels and organizational maturity levels. However, in one case, individual process capability is measured and, in the other, the capability levels of selected groups of process areas are measured. Either a project or an organization can achieve either capability levels or maturity levels. That is determined by the scope of the appraisal performed to determine ratings.

Generic practices and common features are defined for levels 1 to 5 to guide process improvement, and are similar to the SEI CMMI® approach. This model is compatible with CMMI®, and is very exhaustive and detailed. An organization can choose to adopt either the Security or Safety aspects of this model or both. However, extensive tailoring would be required to adopt this model for security considerations only. As this is an integrated model, the safety and security aspects are integrated along with the other practices. For an organization that has already adopted a model like CMMI®, it poses a challenge to extract the security aspects of the model. For these reasons, it was found not to be suitable for Motorola's purposes.

IA-CMM®: INFOSEC Assurance Capability Maturity Model [6].

This model is based on the System Security Engineering Capability Maturity Model (SSE-CMM©) and was modified to address the INFOSEC assurance processes. It emphasizes training to the methodology/appraisal method. This particular aspect is detailed using the INFOSEC ASSURANCE TRAINING AND RATING PROGRAM (IATRP).

This model has nine process areas including:

- provide training,
- coordinate with customer organization
- specify initial INFOSEC needs,
- assess threat,
- assess vulnerability,
- assess impact,
- assess INFOSEC risk,
- provide analysis and results,
- manage INFOSEC assurance processes.

In all, there are thirty-five base practices that are detailed to conform to these process areas. Generic practices and common features are defined for levels 1 to 5 to guide process improvement and are very similar to the SEI CMMI® approach. The IA-CMM® is a non-tailorable continuous model. This means that all the process areas are appraised for a given organization and cannot be "tailored out" if irrelevant to the organization. This model is not focused on the lifecycle software development approach important to Motorola. Organizations adopting this model are required to use the IATRP rating program. Due to these reasons, this model was not found suitable for our purposes.

BS 7799®: BSI British Standards [8].
Ten main controls are defined for security out of a total of 148 controls that are required to comply with base practices. No maturity levels are defined. The model has two parts. The first part is a standard code of practice that provides the organization with guidelines on the types of security controls to be implemented to safeguard assets. The second part addresses management. There are specifications for Information Security Management Systems (ISMS). This covers:

a) the identification of assets to be protected
b) the definition of an organizational approach to risk management
c) the definition and identification of the control objectives and the controls
d) the definition of the degree of assurance.

This model can be mapped to the SEI CMMI® model, however, the terminologies differ. Since Motorola and the Motorola Software Group have the policy of using the SEI standards, relating and compatibility to the **BS 7799®** would require additional effort across the company. This model has specific references to protecting organizational information assets (part 2 of the model). Prior to embarking on BS7799 compliancy, an organization should follow the six steps to identify the level of BS7799 compliance to run the business more securely. This was viewed as unnecessarily prohibitive in moving Motorola towards its ultimate goal of making all of our software more secure.

3. WHY EXTEND FROM CMMI®?

The Software Engineering Institute's Capability Maturity Model Integration®, is a very popular software engineering improvement model due to its demonstrated ability to produce high quality results repeatedly. The Capability Maturity Model for Software (also known as the CMM and SW-CMM[3]) has been a model used by many organizations around the world to identify best practices useful in helping them increase the maturity of their processes. In 2000, the SW-CMM

was upgraded to include systems issues and is known as the CMMI® (Capability Maturity Model Integration)[4]

Motorola has used the SEI CMM® model since the late eighties. More recently, the CMMI® model is also widely used and well understood within Motorola. Apart from this reason, the CMMI® was designed for software improvement, whereas the other models described originated from manufacturing. This was the major reason to modify and combine these other models and develop a security capability model as something which could stand alone for those organizations operating at a low maturity level or as an extension to the CMMI® model efforts already employed

4. THE PROPOSED MODEL

Most Motorola organizations are familiar with the SEI's CMM® and CMMI® process improvement models. Within Motorola Software, it was important to define a model that was closely alligned with the CMMI® model in order to build on the success of the adoption of these models across the software centers around the world. The CMMI® model was used as a reference model, based on which this security model was developed. The five additional process areas identified to be included in the security model are:

1. Secure Development Processes
2. Secure Management Processes
3. Organization Security Focus
4. Discovery Of Security Vulnerabilities and Risks
5. Corrective Security Actions

Each process area has specific goals numbered consistently with the SEI CMMI® numbering format to indicate levels of maturity for security. Every practice is assigned to a particular capability level. The level can be identified by looking at the number after the "-" in the practice identifier. For example, the practice identifier SP3.4-2 denotes that it is a capability level 2 practice.

Secure Development Processes.
This process area encompasses the complete software lifecycle and is thus an important building block for security practices. The purpose of the Secure Development Processes is to ensure that security is built into the development processes. This process area has six specific goals:

SG 1: Elicit security requirements

SP 1.1-2: Security topics are elicited and included in customer documentation.

- Include security topics in the customer documentation.
- Identify and document all functional and performance requirements pertaining to security.
- Make use of threat modelling to identify appropriate security requirements.

SP 1.2-2: Security features are tracked by product release
- Determine regulatory and legal requirements, polices and standards that will be applied to the system, product and its development, operation and support process.
- Test and verify all requirements related to security prior to release of the product/software.
- Generic security text is included in product documentation for installation and use.

SG 2: Analyze security requirements
All five of the specific practices of Requirements Management (REQM) process area in SEI CMMI model are extended for security.

SP 2.1-1 Manage security requirements.

SP 2.2-2 Obtain commitment to security requirements

SP 2.3-1 Manage security requirements changes.

SP 2.4-2 Maintain bi-directional traceability of security requirements.

SP 2.5-1 Identify inconsistencies between product work and security requirements.

SG3: Design for security

SP 3.1-2: Develop alternative security solutions and selection criteria.
- Develop alternative security solutions, making use of security design patterns and anti-patterns as appropriate.
- Document the selection criteria used to select a particular design.

SP 3.2-2: Evolve operational security concepts and scenarios.
- Evolve the operational concept, scenarios, and environments to determine security vulnerabilities for various conditions, operating modes, and operating states specific to each product component.

SP 3.3-2: Select a secure solution.
- Select the most secure solution based on the pre-determined selection criteria.

SG4: Implement secure practices in products.

SP 4.1-2: Implement the secure design according to security standards and guidelines.
- Employ secure design patterns as appropriate.

SP 4.2-2 Product documentation includes applicable specific secure install, use, and caution information. Customer responsibility for a secure installation is also specified.

SG5: Verify secure implementation

SP 5.1-2: Conduct peer reviews according to secure standards and guidelines.
- Updated secure programming guidelines should be available and utlizied during formal peer reviews.
- Security peer review roles should be defined.

SP 5.2-2: Perform secure verification.
- Test the product for security requirements.

SG6: Validate secure implementation

SG 6.1-2: Perform validation to include field test and customer testing.

All the above practices are placed at level 2 because these are requirements at the project level. Organization level requirements will be placed under level 3. For level 3 and 4 practices under Secure Development Processes, see generic practices at maturity level 3 and 4, as there are no specific practices for this process area.

For level 5 practices under this process area, see generic practice 5.1 "Ensure continuous process improvement". In the context of this process area it will take on the following definition.

GP 5.1: Lessons-learned are applied.

- Expand industry benchmarking initiatives to include security information.
- Lessons learned from security short comings after deployment in the field should be tracked, collected and analyzed for appropriate corrective actions on a proactive basis.

Secure Management Processes.
The purpose of these processes is to ensure that security interests are built into management processes.

SG 1: Plan for security

SP 1.1-2: Adequate resources are provided to execute the security plan.

- Emphasis on adequate resocuces at the planning stage.

SP 1.2-2: Develop cost estimates for all technical resources required by the project to incorporate secure engineering practices and procedures.

SP 1.3-2: Develop estimates for the secure product factors that affect the magnitude and technical feasibility of the project.

SP 1.4-2: Ensure security related tasks and efforts are included in the overall project planning.

SG 2: Measure security effectiveness

SP 2.1-2: Measurements are tied to organizational goals. Set organizational goals relating to security.

SP 2.2-2: Each project defines security goals.

SP 2.3-2: Ensure that security goals are tracked against actual results achieved for each project

- Incorporate deviations from intended security goals into the organization's processes for goal deviation.
- Continuously improve the security processes based on the metrics data.

SG 3: Monitor and control security initiatives.

SP 3.1-2: Review each project periodically by the project team from a security perspective.

SP 3.2-2: Objectively use goals and security metrics to manage security processes effectively.

SG4: Supplier agreements are documented,if applicable.

SP 4.1-2: Tailor supplier management and software acquisition process to meet security requirements.

SP 4.2-2: Use a formal evaluation process to determine that security aspects are satisfied for third party software.

SP 4.3-2: Review Commercial Off The Shelf and Open Source products to ensure that security requirements covered under supplier agreements are satisfied.

For level 3, 4 and 5 practices under Secure Management Processes, see the SEI CMMI® generic practices, as there are no specific practices at level 3,4 and 5 for this process area.

Organization Security Focus.
The purpose of this process area is to plan and implement organizational security policy and processes based on a through understanding of the current security vulnerabilities and risks.

SG 1: Establish an organizational policy for security.

SP 1.1-2: Local secure practices and standards have been established.

- Document a security policy.
- Create processes to implement the policy.
- Audit procedures are in place to ensure compliance, and audits are conducted.

SP 1.2-2: Minimum set of product security policies have been created.

- Mandate and scope a minimum set of agreed product security policies & standards for the projects.
- Ensure that the product security policies are well communicated within the project team as well as to customers and suppliers.

SP 1.3-3: A security roadmap for the organization is established.

- Security staffing and funding are in place to address Security Roadmap needs.

SP 1.4-3: Security policies are implemented across the organization.

SP 1.5-3: Institutionalize an organization level security training program.

- This practice will require the organization to have a training program (process, templates, plans, guidelines) at the organizational level which is implemented across all projects

SP 1.6-3: Establish an organization security council.

- The security council will oversee the introduction, and tailoring of security practices. The council will also approve changes to the existing secure practices. The security council is the custodian of the organization's security policy and its security artifacts.

The practices mentioned above are at level 3 as they are targeted at the organization.

SG 2: Establish organizational security assets.

SP 2.1-3: Process assets for security are established, integrated and maintained across the organization in conjunction with the other system development processes.

SG3: Assess organizational security initiatives / processes.

SP 3.1-2: Objectively assess the organization's security process compliance.

The generic practices at level 3 will apply to this process area as follows

GP 3.1 Define guidelines for tailoring security engineering processes.

GP 3.2 Collect and maintain security engineering process assets related to the project.

The Generic practices at level 4 will apply to this process area as follows.

GP 4.1: Security training metrics are statistically managed.

- Training on statistical measures of security performance is in place. Development and market management are trained.
- Funding decisions show basis in performance statistics.

The generic practices at level 5 will apply to this process area as follows.

GP 5.1: A security roadmap is maintained.

- Establish and maintain a security roadmap for process improvement.
- Roadmap reflects both short term and long term focus areas, aligned with the organization and customer business objectives along with directions for security.
- Roadmaps are updated on a periodic basis.
- Roadmaps are reviewed by senior management on a periodic basis.
- Adequate funding and staffing are in place to address security roadmap priorities.
- Establish and maintain collaborations with external organizations promoting systems security.

Discovery Of Security Vulnerabilities and Risks.

The purpose of this process area is to put activities in place to ensure that vulnerabilities are exposed.

SG 1: Perform risk or vulnerability assessments.

SP1.1-2: Select the methods, techniques and criteria by which security risks for the system in a defined environment are analyzed, assessed, and compared.

SP1.2-2: Identify and prioritize risks according to a defined methodology.

SP 1.3-2: Monitor the ongoing changes in the risk spectrum and their characteristics.

SG 2: Perform product security audits.

SP 2.1-2: Objectively assess the project's security process compliance.

SP 2.2-2: Establish audit procedures and plan for the security audit.

SP 2.3-2: Perform audits with necessary tools like security checklist conforming to predefined policies, processes, and standards.

SP 2.4-2: Ensure sufficient audit resources are available with expertise in secure engineering.

SP 2.5-2: Initiate and close corrective actions against secure practices audit non-conformances.

SG3: Analyze security vulnerabilities and risks.

SP 3.1-2: Security vulnerability discovery rates are tracked.

SG4: Use tools for security discovery activities.

SP 4.1-4 Usage of tools for discovery activities.

The generic practices at level 3, 4 and 5 that will take on different definitions in the context of this process area are stated below.

GP 3.1: Define guidelines for tailoring security engineering processes.

GP 3.2: Security vulnerabilities and issues are analyzed at an organization level, Characterized by product / customer

GP 5.1: Proactive approach to security practice and tool improvements.

- Determine specific security processes, practices, methods, and tools that need to be improved across the organization.
- Identify, implement, and track action plans.
- Ensure inclusion of security incidents / breaches / defects while doing defect causal analysis.
- Identify security process automations to reduce common and special causes of variations.
- Identify and correct the root causes of defects at the organizational level.
- Implement new assessment tools and techniques
- Establish process effectiveness goals on security at the organization level.

- Continuously improve the security process by piloting innovative ideas, new technologies and tools to improve organizational capability related to security.
- Use data collected after deployment to make appropriate recommendations to new tool acquisitions.

Corrective Security Actions (CSA).
The purpose of this process area is to identify the causes of security vulnerabilities and to prevent them from reoccurring.

SG 1: Identify valid vulnerabilities and risks

SP 1.1-2: Select methods, techniques and criteria by which security system vulnerabilities and breaches are identified and characterized.

SP 1.2-2: Identify vulnerabilities and breaches and characterize them.

SG 2: Evaluate, select, implement and track alternative corrective actions

SP2.1-2: Actions are taken in response to vulnerabilities and breaches.

- Create risk mitigation plans in response to a breach or incident.

SP 2.2-2: Ensure closure of identified incidents and vulnerabilities

SG 3: Conduct high level reviews of performance and corrective actions. Corrective actions are taken.

SP 3.1-2: Conduct periodic reviews with Senior Management.

SP 3.2-2: Ensure secure process, procedures, and standards are executed as per the documented processes.

- Understand the causes of non-conformities and oversee the implementation of corrective actions

The generic practices at level 3, 4 and 5 that assume a different definition in the context of this process area are stated below.

GP 3.2: Corrective action is taken based on systemic security vulnerabilities and issues at the organizational level.

GP 5.1: Security process improvements that address root causes on security breaches & vulnerabilities are identified, evaluated and deployed.
• Defect Data from static analysis tools are analyzed to make recommendation to improve process capability

Generic Goals and Practices.

Generic goals are common to all process areas and are applied to each of them. Generic practices provide a guide to the institutionalization of a process. They are also used in a process appraisal to determine the capability of any process. The generic practices are grouped according to capability levels. The concept is identical to the CMMI® Version 1.1.

A lot of thought had been put into these practices before they were added to the generic goals as they are applicable for all process areas. Hence, not many changes are proposed in the generic practices areas. The new generic practices added in this model are:

- 2.11 Classify security level of all work products and

- 4.3 Perform cost benefit analysis.

Generic Practices at Maturity Level Two:

2.1 Establish an organization security policy.
2.2 Plan the security process
2.3 Provide security resources
2.4 Assign security responsibility
2.5 Train people in security.
2.6 Manage configurations securely
2.7 Identify and involve relevant security stakeholders
2.8 Monitor and control the security process
2.9 Objectively evaluate security adherence
2.10 Review security status with higher level management.
2.11 Classify security level of all work products

Practice 2.11 is a new practice included in this model. The team felt that it is very important that all work products should be security classified. This was also considered as a basic practice to be incorporated at level 2.

Generic Practices at Maturity Level Three:

3.1. Establish a defined process

- Define guidelines for tailoring these security engineering processes.

3.2. Collect improvement information.

- Collect and maintain security engineering process assets related to the project.
- Security is incorporated into the process improvement efforts which are coordinated and performed across the organization.
- Integrate the standard secure processes with the organizational process asset library in order to ensure availability for all practitioners.
- Extend the software quality assurance (SQA) processes to ensure that secure processes, procedures, and standards are deployed and executed across the organization.
- Incorporate security into the process improvement efforts which are coordinated and performed across the organization.
- Include the secure engineering process assets in the organization's periodic assessment of strengths, weaknesses, and corrective actions.
- End of project postmortems are extended to include security.
- A foundation for process performance is established.
- Define security process performance metrics compliant with the project development plan.
- Gather and analyze data associated with vulnerabilities.
- Stakeholders and participants coordinate with each other.

Generic Practices at Maturity Level Four:

4.1. Establish quantitative security objectives for the project.

4.2. Stabilize the security process performance

4.3. Perform cost benefit analysis

Performing cost benefit analysis is a new practice introduced in this model. The introduction of secure practices and methods require considerable time and resources for achieving the benefits. It is recognized that any amount of secure processes does not make the product 100% secure. The objective is to increase the probability in identifying the security vulnerabilities early in the development lifecycle at a

reduced cost to the organization and to do so in a repeatable manner. Given this reality, projects and organizations should perform a cost benefit analysis to justify the return on investment to senior management.

Generic Practices at Maturity Level Five:

5.1 Ensure continuous process improvement

5.2 Correct root causes of problems.

5. IMPLEMENTATION TO DATE

The Motorola Software Group consists of approximately eighteen software centers world-wide, each with their own process under an organizational wide common process. Each software center was asked to do a self assessment against the model as a baseline. The self assessments involved the preparation of training to introduce the model and the creation of a tool to do the self-assessment. The self-assessment was piloted at two locations before wide distribution. Most locations provided their baselines in late September or early October. As a result of the baselines, each location performed a gap analysis against those process areas which had assets corresponding to the coding phase deployed. All locations have indicated that the relevant gaps were closed by the end of 2006.

In December, the Malaysia Software Center conducted a SCAMPI B CMMI appraisal and agreed to pilot an assessment for the MSSDM. Assessors as well as the local staff were trained on the features of the model and the associated assessment. The purpose of the pilot was to gain an understanding of the time requirements for the assessment and the impact on the SCAMPI CMMI appraisal. The activity was well received by both the assessment team and the Malaysia Software Center. Minor adjustments have been made to the model as a result of this assessment. Organizational policy will include MSSDM assessments in future SCAMPI CMMI appraisals.

6. FUTURE ENHANCEMENTS

Areas that can be further enhanced are the secure practices related to supplier agreement management and integrated process and product management process areas. Supplier agreement management is not addressed in detail in this paper except for SG4 under process area Secure Management Process in this model. There are many more security concerns that must be addressed when a supplier provides a part of any product. There are also concerns when there is a joint development effort with the supplier. These concerns are not addressed in this version of the model.

Currently, the next version of the MSSDM is under review. The updated version will be more aligned with version 1.2 of SEI's CMMI®. Highlights of MSSDM version 1.2 include :

- Common practices re-named as Generic practices applicable to all security process areas
- Generic practices determine the security maturity level
- Clarified practices with certain overlapping practices combined.

This model will continue to evolve within the organization.

7. CONCLUSION

Individuals attacking products and enterprises ccoorperate with one another and practice continuous improvement. It is to the benefit of legitimate software development organizations to cooperate with one another to continuously improve the best practices to provide a defence against such malicious attacks. The attackers benefit from working together as should the defenders. Motorola would like to repeat the success achieved through the adoption of the SEI's CMMI® models with a security capability maturity model. It is clear that secure development practices should be a part of the normal software lifecycle development processes. The next step should be to incorporate these practices into an existing industry standard process improvement framework, like SEI CMMI®. Motorola is currently engaging the SEI towards this cause. Once these types of practices are included into the SEI CMMI®, Motorola plans to retire the MSSDM.

8. REFERENCES

[1] Improving Security Across the Software Development Lifecycle, National Cyber Security Partnership. Task Force Report, April 1, 2004.

[2] Comprehensive, Lightweight Application Security Process, CLASP, Secure software. http://www.securesoftware.com

[3] SEI CMM Capability Maturity Model for Software®, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA. http://www.sei.cmu.edu/

[4] Capability Maturity Model® Integration (CMMI) Version 1.1, http://www.sei.cmu.edu/cmmi/general/general.html

[5] Systems Security Engineering Capability Maturity Model Ver3.0, (SSE-CMM©) http://www.sse-cmm.org/index.html

[6] INFOSEC Assurance Capability Maturity Model ver 3.1 (IA-CMM©) http://www.iatrp.com/iacmm.cfm

[7] FAA-iCMM, The Federal Aviation Administration Integrated Capability Maturity Model Ver 2. http://www.faa.gov/ipg/pif/icmm/index.cfm

[8] BSI British Standards (BS 7799) http://www.bsi-global.com/Global/bs7799.xalter