Type of Submission: Paper.

# THE RELATIONSHIP BETWEEN THE SSE-CMM AND IT SECURITY GUIDANCE DOCUMENTATION

John P. Hopkinson, CISSP, ISP, CDRP
Principal Engineer, Security Architect
EWA-Canada Ltd
275 Slater Street
OTTAWA
ON, K1P 5H9
Phone: 613-230-6067
FAX: 613-230-4933
E-mail: jhopkinson@ewa-canada.com
John.Hopkinson@sympatico.ca

## ABSTRACT

In recent years an number of Guideline Documents have been developed to assist organizations, both Public and Private Sector, in establishing and maintaining their IT Security programs. Examples of these documents include the NIST Handbook, the CSE Guide, BSI 7799, ISO/IEC 13335, and many others. The Systems Security Engineering Capability Maturity Model (SSE-CMM) may be thought by some to be simply another of this genre of documents. However this perspective would be incorrect. The SSE-CMM examines the maturity of the IT Security processes implemented by an organization, perhaps in conformance with one or more of the above Guides. Thus the SSE-CMM can and does work in conjunction with any of the above guideline documents, and is in fact complimentary to them.

This paper examines the relationship between the SSE-CMM and several of the above guides. It identifies how they can work together and what accommodations, if any, need to be considered. The use of the SSE-CMM in conjunction with one of the above Guides can greatly enhance their implementation, effectiveness and the return achieved from implementing the guidance within the organization.

© Copyright EWA-Canada Ltd, 1999

draft

# THE RELATIONSHIP BETWEEN THE SSE-CMM AND IT SECURITY GUIDANCE DOCUMENTATION

draft

## ABSTRACT

In recent years an number of Guideline Documents have been developed to assist organizations, both Public and Private Sector, in establishing and maintaining their IT Security programs. Examples of these documents include the NIST Handbook, the CSE Guide, BSI 7799, ISO/IEC 13335, and many others. The Systems Security Engineering Capability Maturity Model (SSE-CMM) may be thought by some to be simply another of this genre of documents. However this perspective would be incorrect. The SSE-CMM examines the maturity of the IT Security processes implemented by an organization, perhaps in conformance with one or more of the above Guides. Thus the SSE-CMM can and does work in conjunction with any of the above guideline documents, and is in fact complimentary to them.

This paper examines the relationship between the SSE-CMM and several of the above guides. It identifies how they can work together and what accommodations, if any, need to be considered. The use of the SSE-CMM in conjunction with one of the above Guides can greatly enhance their implementation, effectiveness and the return achieved from implementing the guidance within the organization.

© Copyright EWA-Canada Ltd, 1999

# INTRODUCTION

A number documents exist to provide guidance to organizations and individuals on developing, implementing and maintaining security programs for organizations. The majority of these documents place a strong emphasis on IT aspects of Security. With one exception, the International Organization for Standardization's ISO/IEC 13335 series called Guidelines for the Management of IT Security[1] or GMITS for short, all the other documents are domain and jurisdiction specific, to a greater of lesser degree.

The GMITS series is domain and jurisdiction neutral, having been specifically written to be capable of being applied in any jurisdiction. GMITS is applicable to all cultures and domains and can be applied to organizations both large and small. GMITS starts at the conceptual level and is refined to a level beyond which it would be necessary to include domain and jurisdictional aspects. Thus, as a base international standard, it does not do this, and has consequently has not been further refined.

The other documents of this genre do provide more specific guidance. However, to achieve this more specific guidance they must integrate aspects of the domain and jurisdiction in which they are intended to function. Examples of these documents include:

- The NIST Handbook[2],
- Canadian Handbook on Information Technology Security[3], and
- Information Security Management[4].

Several other examples of these types of documents exist, some specific to a particular business sector domain[1].

All of these documents provide help and guidance related to the topics that should be addressed and the different aspects that need to be considered. They all provide suggestions as to approaches that could be used, but they also recognize that the guidance provided will need to be customized to the needs and situation of the target organization and the environment in which it functions. Each of the documents uses a somewhat different structure and organization. The structure and organization is that which is comfortable for the community for which and within which they were written. In addition the culture within the document is intended to be used, while not diametrically opposed, is more appropriate to the target audience, and is influenced by the culture of the originators. All of the above means that, with the exception of the ISO standard, the documents are not easily transposed to a different culture, domain and jurisdiction. This does not mean that it cannot be done, just that it is not easy. This in no way detracts from the documents themselves, but is a consequence of making

[1] Throughout the remainder of this paper the term IT Security Guidance documents will be used to refer to these documents as a group.

© Copyright EWA-Canada Ltd, 1999

the documents as valuable as possible to the target audience.

The Systems Security Engineering Capability Maturity Model[5] (SSE-CMM) is a very different nature of material. Its intent is to assess the level of maturity of the Systems Security Engineering processes implemented by the organization. The precept of the SSE-CMM is that, all things being equal, the more mature the process the better and more consistent will be the results of that process, regardless of the specifics of the approach or methodology used by that process. Thus the SSE-CMM has been specifically designed to be approach and methodology neutral. Capability Maturity Models (CMM)s are not unique to the SSE-CMM and many exist to address different aspects of IT. Examples include:

- Systems Engineering CMM,
- Software CMM, and
- Personnel CMM.

The veracity of the precept and profs of the claims to enhance results have been amply justified in the literature and will not be further addressed here. Suffice it to say that a more mature process in general will produce a better and more consistent result.

As has been mentioned the SSE-CMM is specifically designed to be approach and methodology neutral. The SSE-CMM does include a set of Process Areas against which the level of maturity can be assessed. The inclusion of these process areas is essential to being able to make an assessment of their level of maturity. The IT Security Guidance documents also include topics that need to be considered and functions that are required, although they do not use the term Process Areas, they are akin. However the specific definitions and demarcations between Process Areas is not the same between different examples of the IT Security Guidance documents themselves, and between the IT Security Guidance documents in general and the SSE-CMM.

In the development of the SSE-CMM Model the problem was recognized that different organizations were likely to be using different combinations of Base Practices and Process Areas to achieve their objectives. Thus the Model was designed such that the organization could restructure the SSE-CMM Process Areas to fit their particular situation. This, of course, also holds true for the IT Security Guidance documents. The Process Areas of the SSE-CMM can be recombined to fit the particular IT Security Guidance document in use. In fact the Process Areas of the SSE-CMM have been established in such a way as to facilitate recombination, and this has been done in all usages of the SSE-CMM. Thus rather than being conflict or in competition, the IT Security Guidance documents and the SSE-CMM are complimentary and enhance one another.

Another area of the SSE-CMM that benefits from some explanation and examination is the usage of some specific terms, for example:

© Copyright EWA-Canada Ltd, 1999

- organization,
- project,
- user,
- customer, and
- system.

As has been said the SSE-CMM was designed for flexibility. These terms have been defined such that they can and should be refined by the organization that is considering using the SSE-CMM.

The model is based on, and can be seen as representing a standard framework for security engineering covering:

- the entire life cycle, including development, operation, maintenance, and decommissioning activities;
- the whole organization, including management, organizational, and engineering activities;
- concurrent interactions with other disciplines, such as system, software, hardware, human factors, and test engineering; system management, operation, and maintenance; and
- interactions with other organizations, including acquisition, system management, certification, accreditation, and evaluation.

Some examples of different refinements of the key terms used in the SSE-CMM Model are given in the table below.

| | Organization | Project | User | Customer | System |
|---|---|---|---|---|---|
| Developer of Secure Products | The larger organization that supports the development effort. | The development of each different product in a production line. | The engineers, technicians, etc. that work on the development system. | The one who pays for the product | The systems security engineering support environment being used to develop the product. |
| Operating a system for a secure mission or business application | The larger organization that supports the smaller operational unit | deploy a unit, launch a new product | The staff that rely on the mission critical system to perform their job. | Those that ultimately benefit from the service provided by the mission | The mission critical system. |

© Copyright EWA-Canada Ltd, 1999

| | Organization | Project | User | Customer | System |
|---|---|---|---|---|---|
| | | | | critical system | |
| Test and evaluation of a product | The larger organization that the test and evaluation unit is part of | The test and evaluation of the product | The testers and evaluators | Those who caused the product to be tested and evaluated | The system being used by the testers and evaluators |
| Test and evaluation of a product | The larger organization that the test and evaluation unit is part of | The test and evaluation of the product | Those who will use the tested and evaluated product | Those who will purchase the tested and evaluated product | The system being tested |

As can be seen the definitions are interdependent and care needs to be exercised to ensure that the intended definition is used otherwise the results will not be as expected.

# COMPARISON OF THE SSE-CMM AND IT SECURITY GUIDANCE DOCUMENTS

A comparison of the SSE-CMM and a number of the IT Security Guidance document will be made. As a preliminary and brief introduction to the structure and content of the SSE-CMM is provided[2].

## INTRODUCTION TO THE SSE-CMM

The SSE-CMM has been developed taking as a starting point the Systems Engineering CMM (SE-CMM). One of the underlying concepts of the SSE-CMM is that, to perform a particular activity well and in a repeatable manner, certain processes must be present. How well that activity is performed is dependent, at least in part, on the maturity of the process used to perform the activity, or part thereof. However, the how of the process is not critical, there are many ways of achieving a particular objective or performing a particular activity. What is important are the objectives of the activity and what is achieved. The details of the particular methodology are not important, but the maturity of the methodology, i.e. the maturity of the process is important. It is the maturity of the process that the SSE-CMM attempts to measure.

[2] Additional details of the SSE-CMM Model can be obtained from the SSE-CMM Web Site at http://sse-cmm.org.

© Copyright EWA-Canada Ltd, 1999

The model for the SSE-CMM is made up of a number of Process Areas (PAs). These PAs are considered to be the basic fundamental parts of the majority, if not all, activities. The PAs that go to make up the SSE-CMM model, are themselves divided into a number of parts called Base Practices (BPs). Again it is not the how of the BP that is important, it is the fact that the BP is performed. Each of the identified BPs is considered to contribute towards the effective performance of the PA, and therefore all BPs within a particular PA must be performed. However, it is considered that some organizations will have no need to perform some PAs, due to the nature of their activities, and thus PAs are not mandatory for compliance with the model.

The PAs themselves are divided into three categories, the engineering PAs, the project PAs, and the organizational PAs. The project and organizational PAs are essentially the same as those of the SE-CMM. In some a change of focus has taken place such that they are dealing with security engineering specifically rather than systems engineering as a whole. It should also be pointed out at this juncture that a fundamental tenant of the SSE-CMM is that security engineering should be integrated with Systems engineering rather than a separate entity. The engineering PAs have been specifically developed for the SSE-CMM.

The PAs are described below. In each case the title, description and objective of the PAs is included. Additional information related to each PA can be found in the SSE-CMM itself listed in the reference section of this paper[3].

## PROCESS AREAS

PA 01 - Administer Security Controls
Summary Description: The purpose of Administer Security Controls is to ensure that the intended security for the system that was integrated into the system design, is in fact achieved by the resultant system in its operational state.
Goals Security controls are properly configured and used.

PA 02 - Assess Impact
Summary Description: The purpose of Assess Impact is to identify impacts that are of concern with respect to the system and to assess the likelihood of the impacts occurring. Impacts may be tangible, such as the loss of revenue or financial penalties, or intangible, such as loss of reputation or goodwill.
Goals The security impacts of risks to the system are identified and characterized.

PA 03 - Assess Security Risk

[3] Only the Systems Security Engineering Process Areas are included as they are the ones of primary interest in this paper. The Capability Maturity level descriptions are also included.

© Copyright EWA-Canada Ltd, 1999

Summary Description: The purpose of Assess Security Risk is to identify the security risks involved with relying on a system in a defined environment. This process area focuses on ascertaining these risks based on an established understanding of how capabilities and assets are vulnerable to threats. Specifically, this activity involves identifying and assessing the likelihood of the occurrence of exposures. "Exposure" refers to a combination of a threat, vulnerability, and impact that could cause significant harm. This set of activities is performed any time during a system's life cycle to support decisions related to developing, maintaining, or operating the system within a known environment.
Goals An understanding of the security risk associated with operating the system within a defined environment is achieved.
Risks are prioritized according to a defined methodology.

PA 04 - Assess Threat
Summary Description: The purpose of the Assess Threat process area is to identify security threats and their properties and characteristics.
Goals Threats to the security of the system are identified and characterized.

PA 05 - Assess Vulnerability
Summary Description: The purpose of Assess Vulnerability is to identify and characterize system security vulnerabilities. This process area includes analyzing system assets, defining specific vulnerabilities, and providing an assessment of the overall system vulnerability. The terms associated with security risk and vulnerability assessment are used differently in many contexts. For the purposes of this model, "vulnerability" refers to an aspect of a system that can be exploited for purposes other than those originally intended, security holes, or implementation bugs within a system that are likely to be attacked by a threat. These vulnerabilities are independent of any particular threat instantiation or attack. This set of activities is performed any time during a system's life-cycle to support the decision to develop, maintain, or operate the system within the known environment.
Goals An understanding of system security vulnerabilities within a defined environment is achieved.

PA 06 - Build Assurance Argument
Summary Description: The purpose of Build Assurance Argument is to clearly convey that the customer's security needs are met. An assurance argument is a set of stated assurance objectives that are supported by a combination of assurance evidence that may be derived from multiple sources and levels of abstraction. This process includes identifying and defining assurance related requirements; evidence production and analysis activities; and additional evidence activities needed to support assurance requirements. Additionally, the evidence generated by these activities is gathered, packaged, and prepared for presentation.
Goals The work products and processes clearly provide the evidence that the customer's

© Copyright EWA-Canada Ltd, 1999

security needs have been met.

PA 07 - Coordinate Security

Summary Description: The purpose of Coordinate Security is to ensure that all parties are aware of and involved with security engineering activities. This activity is critical as security engineering cannot succeed in isolation. This coordination involves maintaining open communications between security groups, other engineering groups, and external groups. Various mechanisms may be used to coordinate and communicate the security engineering decisions and recommendations between these parties, including memoranda, documents, e-mail, meetings, and working groups.

Goals All members of the project team are aware of and involved with security engineering activities to the extent necessary to perform their functions.

Decisions and recommendations related to security are communicated and coordinated.

PA 08 - Monitor Security Posture

Summary Description: The purpose of Monitor Security Posture is to ensure that all breaches of, attempted breaches of, or mistakes that could potentially lead to a breach of security are identified and reported. The external and internal environments are monitored for all factors that may have an impact on the security of the system.

Goals Both internal and external security related events are detected and tracked.

Incidents are responded to in accordance with policy.

Changes to the operational security posture are identified and handled in accordance with the security objectives.

PA 09 - Provide Security Input

Summary Description: The purpose of Provide Security Input is to provide system architects, designers, implementers, or users with the security information they need. This information includes security architecture, design, or implementation alternatives and security guidance. The input is developed, analyzed, provided to and coordinated with the appropriate organization members based on the security needs identified in PA01 Specify Security Needs.

Goals All system issues are reviewed for security implications and are resolved in accordance with security goals.

All members of the project team have an understanding of security so they can perform their functions.

The solution reflects the security input provided.

PA 10 - Specify Security Needs

Summary Description: The purpose of Specify Security Needs is to explicitly identify the needs related to security for the system. Specify Security Needs involves defining the basis for security in the system in order to meet all legal, policy, and organizational requirements

© Copyright EWA-Canada Ltd, 1999

for security. These needs are tailored based upon the target operational security context of the system, the current security and systems environment of the organization, and a set of security objectives are identified. A set of security-related requirements is defined for the system which upon approval becomes the baseline for security within the system.
Goals A common understanding of security needs is reached between all parties, including the customer.

PA 11 - Verify and Validate Security
Summary Description: The purpose of Verify and Validate Security is to ensure that solutions verified and validated with respect to security. Solutions are verified against the security requirements, architecture, and design using observation, demonstration, analysis, and testing. Solutions are validated against the customer's operational security needs.
Goals Solutions meet security requirements.
Solutions meet the customer's operational security needs.

## CAPABILITY MATURITY LEVELS

As was mentioned at the beginning, the SSE-CMM model includes the notion of maturity levels. That is to say, the manner in which an organization preforms, controls, supports and monitors a process determines how mature the process is, and how well the process will be performed, and thus how good and repeatable the results of that process will be.

The SSE-CMM defines six maturity levels. Each of these levels is considered to consist of a number of Generic Base Practices which support the performance of the process areas. Listed below are the titles and descriptions for each of the capability maturity levels. Additional information can be obtained from the SSE-CMM itself.

Capability Level 0 - Not Performed
Description: The Not Performed level has no common features. There is general failure to perform the base practices in the process area. Where there are work products that result from performing the process, they are not easily identifiable or accessible.

Capability Level 1 - Performed Informally
Description: Base practices of the process area are generally performed. The performance of these base practices may not be rigorously planned and tracked. Performance depends on individual knowledge and effort. Work products of the process area testify to their performance. Individuals within the organization recognize that an action should be performed, and there is general agreement that this action is performed as and when required. There are identifiable work products for the process.

© Copyright EWA-Canada Ltd, 1999

Capability Level 2 - Planned and Tracked
Description: Performance of the base practices in the process area is planned and tracked. Performance according to specified procedures is verified. Work products conform to specified standards and requirements. Measurement is used to track process area performance, thus enabling the organization to manage its activities based on actual performance. The primary distinction from the Performed Informally level is that the performance of the process is planned and managed.

Capability Level 3 - Well Defined
Description: Base practices are performed according to a well-defined process using approved, tailored versions of standard, documented processes. The primary distinction from the Planned and Tracked level is that the process is planned and managed using an organization-wide standard process.

Capability Level 4 - Quantitatively Controlled
Description: Detailed measures of performance are collected and analyzed. This leads to a quantitative understanding of process capability and an improved ability to predict performance. Performance is objectively managed, and the quality of work products is quantitatively known. The primary distinction from the Well Defined level is that the defined process is quantitatively understood and controlled.

Capability Level 5 - Continuously Improving
Description: Quantitative performance goals (targets) for process effectiveness and efficiency are established, based on the business goals of the organization. Continuous process improvement against these goals is enabled by quantitative feedback from performing the defined processes and from piloting innovative ideas and technologies. The primary distinction from the Quantitatively Controlled level is that the defined process and the standard process undergo continuous refinement and improvement, based on a quantitative understanding of the impact of changes to these processes.

## SSE-CMM AND GMITS

The first mapping is made between ISO/IEC 13335 Information Technology - Security Techniques - Guidelines for the Management of IT Security (GMITS) and the SSE-CMM, specifically, GMITS - Part 2: Managing and Planning. GMITS Part 2 has been used as the primary linkage for topics between GMITS and the SSE-CMM, however account has been taken of some topics that are explored in considerably greater detail in other parts of the GMITS series.

© Copyright EWA-Canada Ltd, 1999

| SSE-CMM | GMITS Part 2 |
|---|---|
| PA 01 - Administer Security Controls | Clause 17, Follow-up |
| PA 02 - Assess Impact | Clause 10, Corporate Risk Analysis Strategy Options; GMITS Part 3 |
| PA 03 - Assess Security Risk | Clause 10, Corporate Risk Analysis Strategy Options; GMITS Part 3 |
| PA 04 - Assess Threat | Clause 10, Corporate Risk Analysis Strategy Options; GMITS Part 3 |
| PA 05 - Assess Vulnerability | Clause 10, Corporate Risk Analysis Strategy Options; GMITS Part 3 |
| PA 06 - Build Assurance Argument | Clause 14, Implementation of Safeguards |
| PA 07 - Coordinate Security | Clause 13, IT Security Plan |
| PA 08 - Monitor Security Posture | Clause 17, Follow-up |
| PA 09 - Provide Security Input | Clause 8, Corporate IT Security Policy<br>Clause 11, IT Security Recommendations<br>Clause 12, IT System Security Policy<br>Clause 13, IT Security Plan<br>Clause 15 Security Awareness |
| PA 10 - Specify Security Needs | Clause 8, Corporate IT Security Policy<br>Clause 11, IT Security Recommendations<br>Clause 12, IT System Security Policy<br>Clause 13, IT Security Plan |
| PA 11 - Verify and Validate Security | Clause 17, Follow-up<br>Clause 14, Implementation of Safeguards |

Clause 9 of GMITS Part 2 is addressed by two General Practices which are part of Maturity Level 2, GP2.1.1 - Allocate Resources, and GP2.1.2 - Assign Responsibilities. Thus all the topics and aspects that addressed by GMITS are also addressed by the SSE-CMM. It is a relatively simple task to assign the Process Areas of the SSE-CMM to functional areas of GMITS.

## SSE-CMM AND NIST HANDBOOK

© Copyright EWA-Canada Ltd, 1999

Comparison between the SSE-CMM and the NIST Handbook resulted in the following mapping.

| SSE-CMM | NIST HANDBOOK |
|---|---|
| PA 01 - Administer Security Controls | Chapter 10, Personnel/User Issues<br>Chapter 14, Security Considerations in Computer Support Operations |
| PA 02 - Assess Impact | Chapter 7, Computer Security Risk Management |
| PA 03 - Assess Security Risk | Chapter 7, Computer Security Risk Management |
| PA 04 - Assess Threat | Chapter 7, Computer Security Risk Management<br>Chapter 4, Common Threats |
| PA 05 - Assess Vulnerability | Chapter 7, Computer Security Risk Management |
| PA 06 - Build Assurance Argument | Chapter 9, Assurance |
| PA 07 - Coordinate Security | Chapter 6, Computer Security Program Management |
| PA 08 - Monitor Security Posture | Chapter 18, Audit Trails<br>Chapter 12, Computer Security Incident Handling |
| PA 09 - Provide Security Input | Chapter 5, Computer Security Policy<br>Chapter 13, Awareness, Training, and Education<br>Chapter 15, Physical and Environmental Security |
| PA 10 - Specify Security Needs | Chapter 8, Security and Planning in the Computer System Life Cycle<br>Chapter 11, Preparing for Contingencies and Disasters<br>Chapter 16, Identification and Authentication<br>Chapter 17, Logical Access Control<br>Chapter 19, Cryptography |
| PA 11 - Verify and Validate Security | Chapter 8, Security and Planning in the Computer System Life Cycle<br>Chapter 18, Audit Trails |

draft

© Copyright EWA-Canada Ltd, 1999

In a similar manner to Clause 9 of GMITS Part 2, Chapter 3, Roles and Responsibilities of the NIST Handbook is addressed by two General Practices which are part of Maturity Level 2, GP2.1.1 - Allocate Resources, and GP2.1.2 - Assign Responsibilities. Thus all the topics and aspects that addressed by the NIST Handbook are also addressed by the SSE-CMM. It is a relatively simple task to assign the Process Areas of the SSE-CMM to functional areas of the NIST Handbook.

**SSE-CMM AND BS 7799**

Comparison between the SSE-CMM and the BS 7799 resulted in the following mapping.

| SSE-CMM | BS 7799 |
|---|---|
| PA 01 - Administer Security Controls | Section 5, Personnel Security<br>Section 6, Communications and operations Management<br>Section 8, Systems Development and Maintenance |
| PA 02 - Assess Impact | Introduction |
| PA 03 - Assess Security Risk | Introduction |
| PA 04 - Assess Threat | Introduction |
| PA 05 - Assess Vulnerability | Introduction |
| PA 06 - Build Assurance Argument | Section 10, Compliance |
| PA 07 - Coordinate Security | Section 2, Security Organization<br>Section 6, Communications and operations Management |
| PA 08 - Monitor Security Posture | Section 10, Compliance |
| PA 09 - Provide Security Input | Section 1, Security Policy<br>Section 3, Asset Classification and Control<br>Section 5, Physical and Environmental Security |
| PA 10 - Specify Security Needs | Section 1, Security Policy<br>Section 7, Access Control<br>Section 8, Systems Development and Maintenance<br>Section 9, Business Continuity Planning |

© Copyright EWA-Canada Ltd, 1999

draft

| SSE-CMM | BS 7799 |
|---|---|
| PA 11 - Verify and Validate Security | Section 10, Compliance |

The aspects of roles and responsibilities is partly dealt with in Section 2. Security Organization of BS 7799, and also in Section 4. Personnel Security. The applicable parts of these two sections are addressed by two the General Practices which are part of Maturity Level 2, GP2.1.1 - Allocate Resources, and GP2.1.2 - Assign Responsibilities. Thus all the topics and aspects that addressed by the BS 7799 are also addressed by the SSE-CMM. It is a relatively simple task to assign the Process Areas of the SSE-CMM to functional areas of BS 7799.

BS 7799 has been recently revised. In the new version the relationship to the UK juristictional environment has been significantly softened. However, BS 7799 still reflects the UK culture and juristictional environment. This makes it difficult to use the document in a different cultural and juristictional environment without significant work. However BS 7799 is ideal in those situations where the culture and juristictional environments are identical or very close.

## SSE-CMM AND THE CANADIAN HANDBOOK ON INFORMATION TECHNOLOGY SECURITY MG-9

Comparison between the SSE-CMM and MG-9 resulted in the following mapping.

| SSE-CMM | MG-9 |
|---|---|
| PA 01 - Administer Security Controls | Chapter 10, Personnel/User Issues<br>Chapter 14, IT Security in Support and Operations |
| PA 02 - Assess Impact | Chapter 7, IT Security Risk Management |
| PA 03 - Assess Security Risk | Chapter 7, IT Security Risk Management |
| PA 04 - Assess Threat | Chapter 4, Common threats<br>Chapter 7, IT Security Risk Management |
| PA 05 - Assess Vulnerability | Chapter 7, IT Security Risk Management |
| PA 06 - Build Assurance Argument | Chapter 9, Assurance |
| PA 07 - Coordinate Security | Chapter 6, IT Security Program Management |
| PA 08 - Monitor Security Posture | Chapter 12, IT Security Incident Handling<br>Chapter 18, Audit trails |

© Copyright EWA-Canada Ltd, 1999

draft

| SSE-CMM | MG-9 |
|---|---|
| PA 09 - Provide Security Input | Chapter 5, IT Security Policy<br>Chapter 13, IT Security Awareness Training and Education<br>Chapter 15, Physical and Environmental IT Security |
| PA 10 - Specify Security Needs | Chapter 8, Planning IT Security into the IT System Life Cycle<br>Chapter 11, Preparing for IT Contingencies and Disasters<br>Chapter 16, Identification and Authentication<br>Chapter 17, Logical Access Control<br>Chapter 19, Cryptography |
| PA 11 - Verify and Validate Security | Chapter 8, Planning IT Security into the IT System Life Cycle<br>Chapter 18, Audit trails |

Roles and responsibilities, Chapter 3 of MG-9 is addressed by two the General Practices which are part of Maturity Level 2, GP2.1.1 - Allocate Resources, and GP2.1.2 - Assign Responsibilities. Thus all the topics and aspects that addressed by the MG-9 are also addressed by the SSE-CMM. It is a relatively simple task to assign the Process Areas of the SSE-CMM to functional areas of MG-9.

## CONCLUSIONS

All of the IT Security Guidance documents cover essentially the same material. However, they do it in different ways and they place different emphasis on various topics. In addition they include different material germaine to the particular culture, jurisdiction and domain for which they are written. The advantages of one are only equaled by the advantages of another within their target area of usage.

All of the IT Security Guidance documents can be used with the SSE-CMM. All of the Process Areas of the SSE-CMM can be relatively easily mapped to the topic areas of the different IT Security Guidance documents. Conversely all of the topic areas of the various IT Security Guidance documents can be related to the Process Areas of the SSE-CMM. The effort to perform the mapping is not significant.

© Copyright EWA-Canada Ltd, 1999

Some differences in terminology exist between the IT Security Guidance documents and the SSE-CMM, however, none of the differences raise major issues. The most important aspect is to ensure consistency in usage.

The primary fundamental difference between the SSE-CMM and the IT Security Guidance documents is one of philosophy in the manner in which they are intended to be used. Unlike the IT Security Guidance documents, the SSE-CMM is not intended to aid its user in establishing an IT Security program, or in helping to ensure that all the appropriate aspects have been taken into consideration, although that may be a spinoff. The primary aim of the SSE-CMM is to assess the level of maturity of the processes implemented by the organization to achieve the appropriate level of security for the organization.

Thus the IT Security Guidance documents and the SSE-CMM are complimentary. The usage of any of the IT Security Guidance documents can significantly benefit from the concomitant usage of the SSE-CMM.

draft

© Copyright EWA-Canada Ltd, 1999

# REFERENCES

[1]. ISO/IEC 13335 Information Technology - Security Techniques - Guidelines for the Management of IT Security - Part 1: Concepts and Models, Part 2: Managing and Planning, Part 3: Management techniques, Part 4: Baseline Control, and Part 5: Safeguards for external connections.

[2]. An Introduction to Computer Security: The NIST Handbook, National Institute of Standards and Technology, Technology Administration, U.S. department of Commerce, 1995.

[3]. Canadian Handbook on Information Technology Security MG-9, Communications Security Establishment, Government of Canada, 1998.

[4]. Information Security Management, British Standard 7799, British Standards Institute, U.K., 1998.

[5]. Systems Security Engineering - Capability Maturity Model, version 2, SSE-CMM Project, http://www.sse-cmm.org, 1999.

draft

© Copyright EWA-Canada Ltd, 1999