SYSTEM SECURITY ENGINEERING CAPABILITY MATURITY MODEL

ORGANIZATION PROFILES

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

ABSTRACT

For many years it has been well understood that an organization's ability to perform a particular activity is dependent upon the maturity of the processes that the organization uses to perform the activity. Many organizations have long had the problem of differentiating between a product or service offered by one supplier and that of another when the functionalities of the products are largely similar. The value of many products and services are much more than an assessment of the functionality of the product or service and it is essential to include the support aspects that the vendor or service providers offers as well as the confidence that the purchaser may have in the supplier organization and its products or services. In the security community confidence is a contributory factor to assurance.

In the last few years, within the information technology (IT) community, considerable effort has been devoted to the development of Capability Maturity Models (CMM). The Software and System Engineering CMMs are well established. Nearing completion is the System Security Engineering (SSE) CMM. The SSE-CMM includes provision for organization profiles based on the premise that different types of organization do not require the same level of maturity in all the process that the organization uses, and yet can still deliver products and services that the purchaser may have a high level of confidence in. This paper presents an number of profiles, based on the SSE-CMM for different types of organizations, along with the associated profile rationale.

© COPYRIGHT EWA-Canada 1996

DESCRIPTION OF THE SSE-CMM MODEL

The SSE-CMM has been developed taking as a starting point the System 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.

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 system 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.

PROCESS AREAS

Security Engineering Process Areas

PA 01: 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 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 applicable parties, including the customer.

PA 02: 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, analysed, provided to and coordinated with the appropriate organization members based on the security needs identified in PA01 Specify Security Needs.

Goals
- Needed security input is identified.
- Timely and accurate security input is provided to appropriate parties.

PA 03: 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 applicable security requirements.
- Solutions meet the customer's operational security needs.

PA 04: Attack Security

Summary description: The purpose of Attack Security, sometimes referred to as penetration testing, is to identify existing system vulnerabilities and validate their potential for exploitation. Vulnerabilities are discovered through active attacks against the system.

Goals
- System vulnerabilities are identified and their potential for exploitation is determined.

PA 05: Assess Operational Security Risk

Summary description: The purpose of Assess Operational Security Risk is to identify the security risks involved with relying on an operational system in a defined environment. This process area focuses on ascertaining these risks based on an established understanding of how operational capabilities and assets are vulnerable to threats. This includes activities that assess the operational impact that results from a successful exploitation of a vulnerability. 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 reached.

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 degree to which work products and processes meet customer security needs is clearly conveyed.

PA 07: Monitor System Security Posture

Summary description: The purpose of Monitor System 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.
- Unwanted incidents are responded to in an appropriate manner.

PA 08: 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 used and configured.

PA 09: Coordinate Security

Summary description: The purpose of Coordinate Security is to ensure that the appropriate 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
- Appropriate parties are aware of and involved with security engineering activities.
- Decisions and recommendations related to security are appropriately communicated and coordinated.

PA 10: Determine Security Vulnerabilities

© COPYRIGHT EWA-Canada 1996

Summary description: The purpose of Determine Security Vulnerabilities is to determine analytically the security vulnerabilities associated with a system. This process area includes such activities as analysing system assets, defining specific susceptibilities and 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, susceptibilities refer to exploitable vulnerabilities, security holes, or implementation bugs within a system that are likely to be attacked by a threat. These susceptibilities are independent of any threat instantiation or attack. Once these susceptibilities are associated with a specific threat and a likelihood of being exploited, they are referred to as vulnerabilities. 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 reached.

Project Process Areas

PA 11: Ensure Quality

Summary description: The purpose of Ensure Quality is to address not only the quality of the system, but also the quality of the process being used to create the system and the degree to which the project follows the defined process. The underlying concept of this process area is that high-quality systems can only be consistently produced on a continuous basis if a process exists to continuously measure and improve quality. In addition, this process must be adhered to rigorously and throughout the system life cycle. Key aspects of the process required to develop high-quality systems are measurement, analysis, and corrective action.

PA 12: Manage Configurations

Summary description: The purpose of Manage Configurations is to maintain data on and status of identified configuration units, and to analyse and control changes to the system and its configuration units. Managing the system configuration involves providing accurate and current configuration data and status to developers and customers. This process area is applicable to all work products that are placed under configuration management. An example set of work products that may be placed under configuration management could include hardware and software configuration items, design rationale, requirements, product data files, or trade studies.

PA 13: Manage Program Risk[1]

Summary description: The purpose of Manage Risk is to identify, assess, monitor, and mitigate risks to the success of both the systems engineering activities and the overall technical effort. This process area continues throughout the life of the project. Similar to the Plan Technical Effort (PA12) and Monitor and Control Technical Effort (PA11) process areas, the scope of this process area includes both the systems

[1] Note: This PA addresses Program Risk only. Operational Risk is addressed by PA05.

© COPYRIGHT EWA-Canada 1996

engineering activities and the overall technical project effort, as the systems engineering effort on the project cannot be considered successful unless the overall technical effort is successful.

PA 14: Monitor and Control Technical Effort
Summary description: The purpose of Monitor and Control Technical Effort is to provide adequate visibility of actual progress and risks. Visibility encourages timely corrective action when performance deviates significantly from plans. Monitor and Control Technical Effort involves directing, tracking and reviewing the project's accomplishments, results, and risks against its documented estimates, commitments, and plans. A documented plan is used as the basis for tracking the activities and risks, communicating status, and revising plans.

PA 15: Plan Technical Effort
Summary description: The purpose of Plan Technical Effort is to establish plans that provide the basis for scheduling, costing, controlling, tracking, and negotiating the nature and scope of the technical work involved in system development, manufacturing, use, and disposal. System engineering activities must be integrated into comprehensive technical planning for the entire project. Plan technical effort involves developing estimates for the work to be performed, obtaining necessary commitments from interfacing groups, and defining the plan to perform the work.

Organization Process Areas

PA 16: Define Organization's Security Engineering Process
Summary description: The purpose of Define Organization's Systems Engineering Process is to create and manage the organization's standard systems engineering processes, which can subsequently be tailored by a project to form the unique processes that it will follow in developing its systems or products. Define Organization's Systems Engineering Process involves defining, collecting, and maintaining the process that will meet the business goals of the organization, as well as designing, developing, and documenting systems-engineering process assets. Assets include example processes, process fragments, process-related documentation, process architectures, process-tailoring rules and tools, and process measurements.

PA 17: Improve Organization's Security Engineering Processes
Summary description: The purpose of Improve Organization's Systems Engineering Processes is to gain competitive advantage by continuously improving the effectiveness and efficiency of the systems engineering processes used by the organization. It involves developing an understanding of the organization's processes in the context of the organization's business goals, analysing the performance of the processes, and explicitly planning and deploying improvements to those processes.

PA 18: Manage Security Product Line Evolution
Summary description: The purpose of Manage Product Line Evolution is to introduce services, equipment,

and new technology to achieve the optimal benefits in product evolution, cost, schedule, and performance over time as the product line evolves toward its ultimate objectives. An organization must first determine the evolution of a product. Then the organization has to decide how it will design and build those products including critical components, cost-effective tools, and efficient and effective processes.

PA 19: Manage Security Engineering Support Environment
Summary description: The purpose of Manage Systems Engineering Support Environment is to provide the technology environment needed to develop the product and perform the process. Development and process technology is inserted into the environment with a goal of minimizing disruption of development activities while upgrading to make new technology available. The technology needs of an organization change over time, and the efforts described in this process area must be re-executed as the needs evolve.

PA 20: Provide Ongoing Skills and Knowledge
Summary description: The purpose of Provide Ongoing Skills and Knowledge is to ensure that projects and the organization have the necessary knowledge and skills to achieve project and organizational objectives. To ensure the effective application of these critical resources that are predominantly available only from people, the knowledge and skill requirements within the organization need to be identified, as well as the specific project's or organization's needs (such as those relating to emergent programs or technology, and new products, processes, and policies).Needed skills and knowledge can be provided both by training within the organization and by timely acquisition from sources external to the organization. Acquisition from external sources may include customer resources, temporary hires, new hires, consultants, and subcontractors. In addition, knowledge may be acquired from subject matter experts.

PA 21: Coordinate with Suppliers
Summary description: The purpose of Coordinate with Suppliers is to address the needs of organizations to effectively manage the portions of product work that are conducted by other organizations. Decisions made as a part of this process area should be made in accordance with the Analyse Candidate Solutions process area (PA01). The general term supplier is used to identify an organization that develops, manufactures, tests, supports, etc., a component of the system. Suppliers may take the form of vendors, subcontractors, partnerships, etc., as the business organization warrants. In addition to coordination of schedules, processes, and deliveries of work products, affected organizations must have a shared a vision of the working relationship. Relationships can range from integrated developer / supplier product teams, to prime-contractor / subcontractor, to vendors, and more. A successful relationship between an organization and a supplier depends on the capability of both organizations, and on a mutual understanding of the relationship and expectations.

CAPABILITY MATURITY LEVELS

© COPYRIGHT EWA-Canada 1996

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.

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 analysed. 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.

© COPYRIGHT EWA-Canada 1996

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.

ORGANIZATIONAL PROFILES

The SSE-CMM is applicable to all organisations that have any involvement with security engineering, or any part thereof, regardless of size or the type of the organization. Thus it is applicable to product developers, system developers and integrators, information technology services providers, specialist service providers such as trusted third parties, and information technology user organizations. It is also intended that the SSE-CMM can and will be used in acquisitions to differentiate between suppliers of products or services, and also as a contract requirement. However, it is recognized that not all types of organization will require that same level of maturity for all of the process areas. To address this aspect the model includes the concept of organizational profiles. Current thinking is that profiles will be applicable to types of organizations such a product vendors or system integrators, rather than individual organizations. This does not preclude any organization having all its process areas at the same level of maturity or defining its own unique profile.

One important aspect is that although process area are logical groupings of base practices they do not define or mandate a particular organizational structure. Dependencies exist between BPs and PAs and must be born in mind, and taken into account in the development of profiles. An organizational profile then defines the level of maturity, by process area, for all process areas for a type of organization. The remainder of this paper identifies a number of organization profile and describes the rationale for each profile.

SSE-CMM ORGANIZATION PROFILES

The SSE-CMM does not include any actual organization profiles, although as has been identified, it does include the concept of organization profiles. Profiles are considered an important aspect of the SSE-CMM. What follows are the suggested profiles for five organization types. It is anticipated that many more organization profiles can and will be developed. The organization types selected are:

- A security product developer,
- A systems integrator,
- A service bureau,
- A certification authority for public key certificates, and
- An IT user organization.

The profile for each of these organizations is introduced below along with the associated rationale.

In constructing the profiles set out below use has been made of the SSE-CMM model and also information and guidance on the development of profiles and guidance to organizations on enhancing their maturity set out in the SE-CMM.

SECURITY PRODUCT DEVELOPER

The SSE-CMM profile for a developer of security products is set out in figure 1.

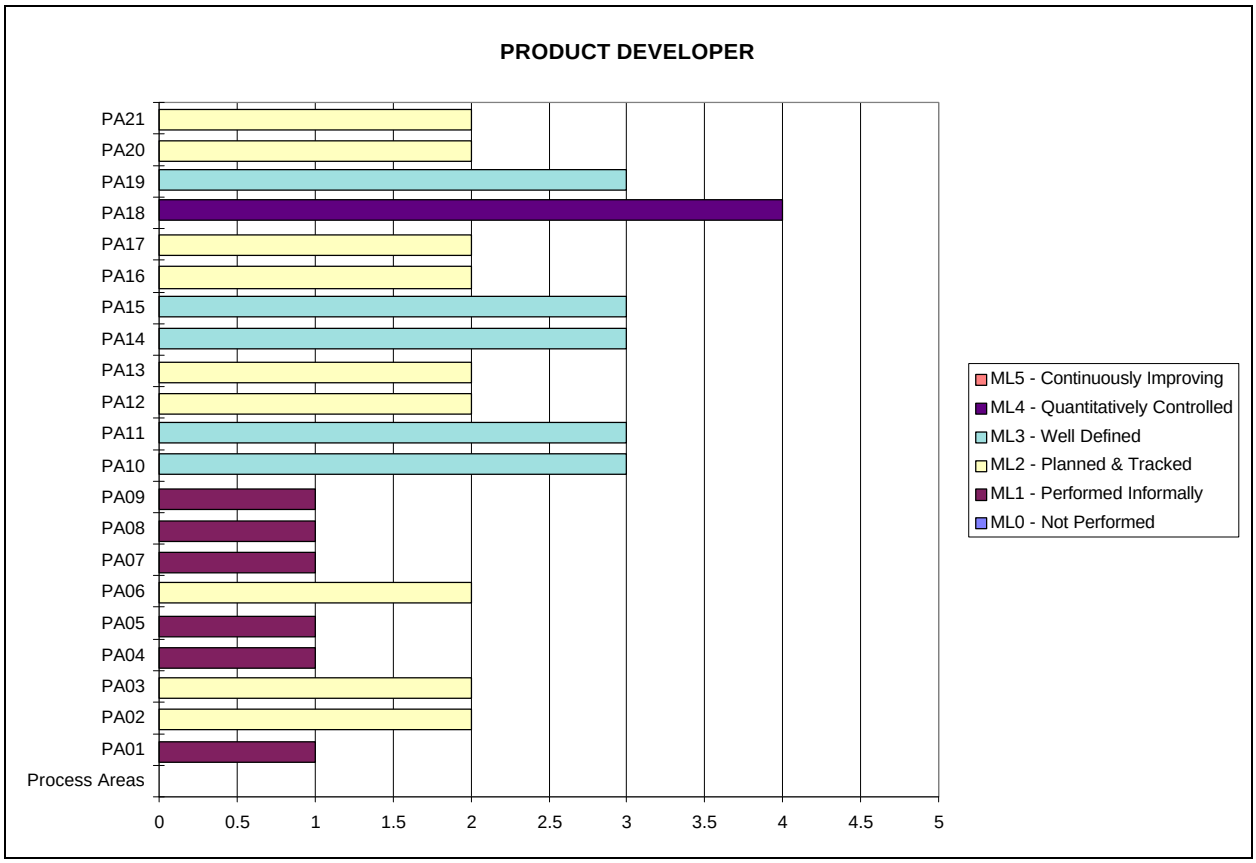

Figure 1 - Profile for a Security Products development Organization

As can been seen process areas related to product development activities are set at a higher level of maturity, as would be expected. The security engineering PAs are generally assigned a reduced level of maturity. The rationale for this is that while they are important activities they are not mainstream activities for the organization, and are not constantly in use. If however, the product developer only produces security products, this may well change and the security engineering PAs would be assigned a higher level of maturity. The exceptions to this are PA02, PA03, PA06 and PA10. In this case these PAs focus on identifying any vulnerabilities of the product, providing the security input to the product and verifying that the security has been correctly and appropriately implemented. These, in the case of a security product, are very important, particularly from the customer's perspective. PA06 is included as assurance relates to the trust that the purchaser can have in the security of the product and therefore is important from the perspective of the vendor providing such confidence to the purchaser. This in turn will help the vendor sell the product.

A SYSTEMS INTEGRATOR

The profile for an Systems Integration organization is shown in figure 2. The profile is independent of the nature of the systems integration being performed, or whether the organization specialises on the integration of security systems.

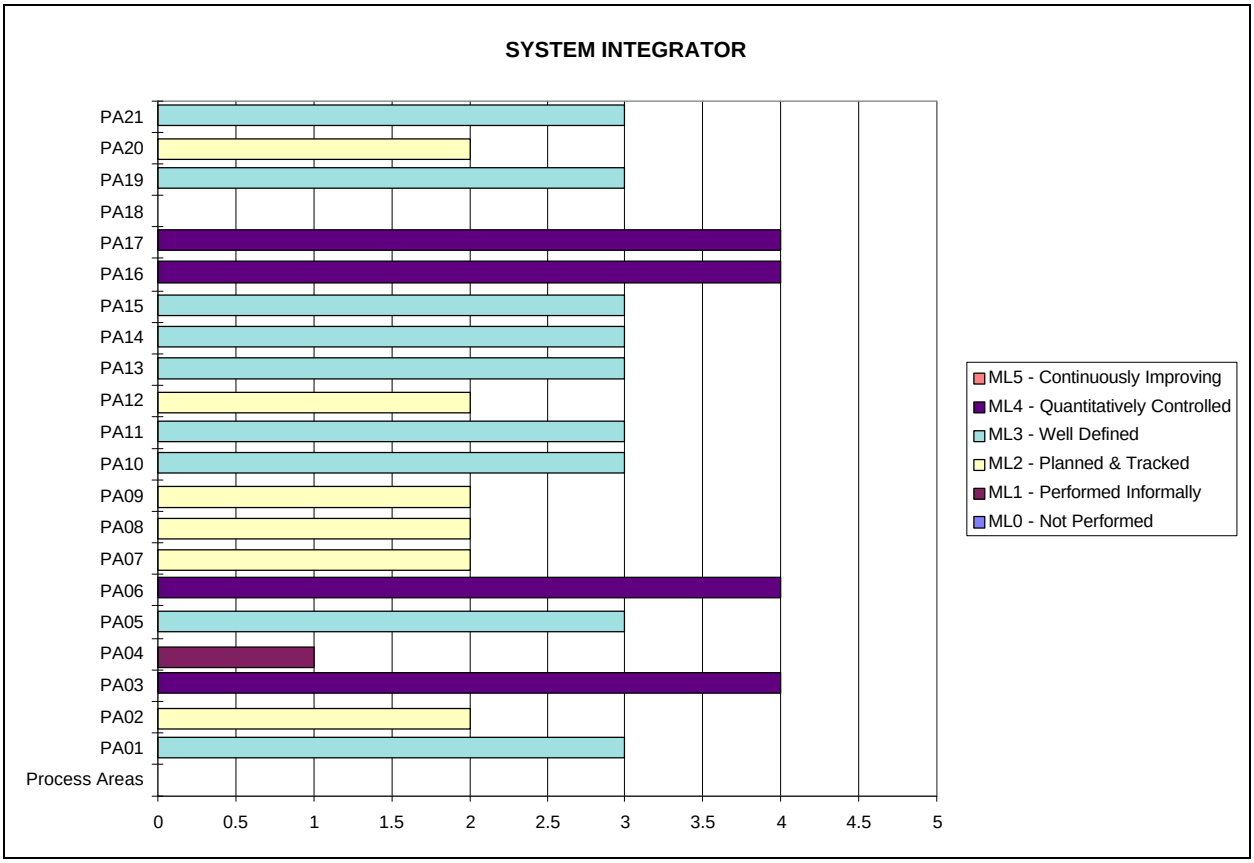

Figure 2 - Profile for a Systems Integration Organization

In this case the highest level of maturity is required in those process areas that contribute most significantly to fulfilling the customers expectations. Thus, PA16 and PA17 which relate to the maturity of the organizations security engineering processes are given the greatest attention along with PA06, Building Assurance arguments and thus providing the customer with confidence, and finally PA03 validating and verifying that the security requirements have been fulfilled. All other PAs are assigned to moderate levels of maturity on the premise that the purchaser will ultimately be relying on the results of the integrators efforts and thus the security of the result must be adequate and reliable.

The PAs do not only apply to the results of the undertaking but also the environment within which the integration is undertaken. This is because if the environment within which the integration is performed is not secure, then vulnerabilities could be introduced into the result via the integration environment. The only exception to this general approach is PA04, Attach Security. In this case it is postulated that this activity should be more a function of the final product in the operational environment. Thus it should fall to the purchaser in the environment in which the system will ultimately be used.

A SERVICE BUREAU

A service bureau performs some particular set of functions on behalf of the contracting organization. The profile for a service bureau is shown in figure 3. Because the service bureau tends to specialise in a particular type of business function, for example payroll, they can perform these function more effectively and cheaply than the individual organization. A service bureau would normally perform similar sets of functions for multiple organizations. The traditional view of service bureau operations is changing. In some cases the service bureau is assuming responsibility for large parts of, or all of, the organizations IT operations. This significantly increases the client dependence upon the service bureau. This in turn raises the requirement for trust and confidence from the clients perspective, and the need to supply that confidence from the service bureau's perspective.

Trust must exist between the client and the service bureau that the client organizations information and particular processes will be safeguarded from disclosure and corruption, and that the service will be performed in an appropriate time frame. There are many examples of organizations that could be considered to fall into this group including vendors of recovery facilities (hot site and cold sites), banks,

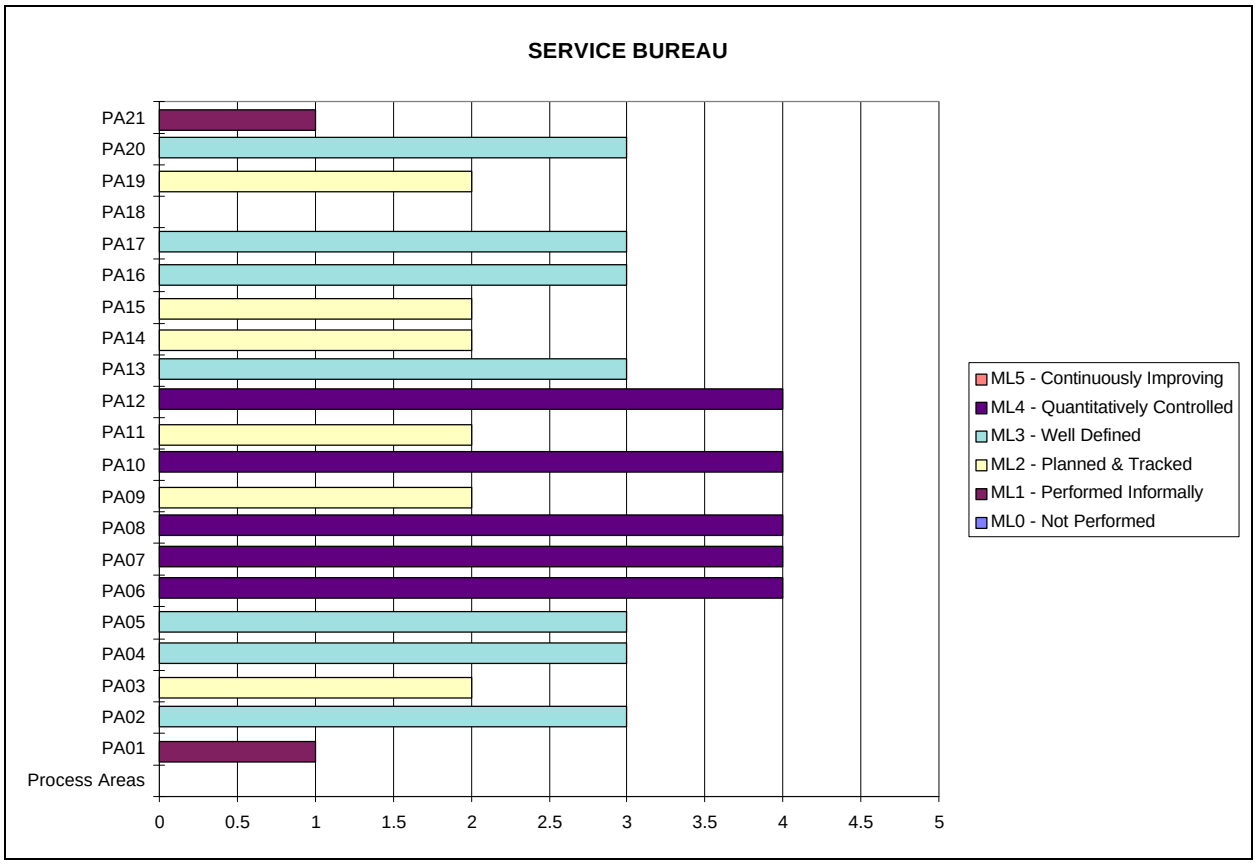

Figure 3 -Profile for a Service Bureau

credit verification organizations, traditional service bureaus, accountants, etc. Thus the PAs that necessitate the highest level of maturity are those that ensure separation and security, and present assurance arguments to the client organization, namely PA06, PA07, PA08, PA10 and PA12. PA01 is considered to be of relatively little concern as the task of identifying security needs should be performed by the client organization and communicated to the service bureau. PA21, Coordinate with suppliers, is considered to be of relatively low importance in this case. PA18 is not considered relevant for similar reasons to those given for the systems integrator. All other PAs are considered to be of moderate concern and in several cases are necessary to support those of higher concern.

A CERTIFICATION AUTHORITY FOR PUBLIC KEY CERTIFICATES

Many security services currently make use of asymmetric cryptographic techniques as part of their underlying mechanism. Examples include digital signatures and non-repudiation. For these services to be effective, it must be possible to prove that a particular entity owns a public key. This is the function provided by a Certification Authority.

A Certification Authority performs the service of binding the public key with the associated entity. In some respects it is related to a service bureau. However, it is different in that it is also performing a service for a general community, in so much as it authenticates the certificate, rather than a specific client. Currently, there is much discussion as to the policies and practices that should be followed by or mandated for CAs. Regardless of the policies and practices that are followed by the CA, it is, and will always be, very important that the assurance and trustworthiness of the CA is maintained. The SSE-CMM offers an advantage in that it does not stipulate a particular process to be followed, leaving that up to the organization itself, but does afford a method of comparing the maturity of the process used, even when it is different. This aspect will be most important as networks of CAs increase and greater cross certification arrises.

The profile shown in figure 4 is generic, applicable to all types of CA. In a hierarchical arrangement of CAs the route CA may be required to be at a higher level of maturity than subordinate CAs. This possibility and flexibility exists within the model.

© COPYRIGHT EWA-Canada 1996

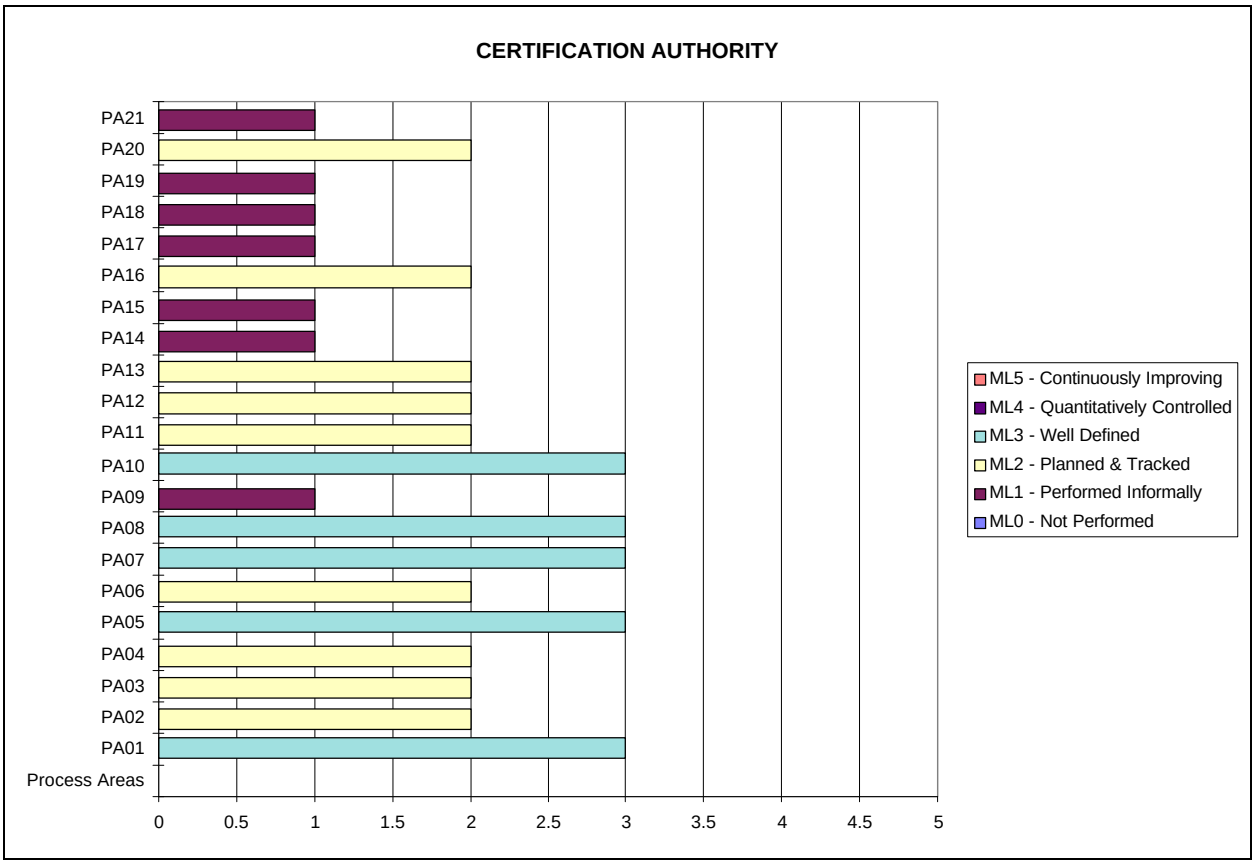

Figure 4 - Profile for a Certification Authority

PA01, PA05, PA07, PA08 and PA10 are considered to be the ones that require the greatest attention, and thus the ones that should be at the highest level of Capability Maturity. The organization will need to make use of these process areas on a regular basis. Capability level 3, Well Defined, is considered appropriate as these PAs focus on security needs, operational risk, security maintenance and administration, and the identification of vulnerabilities.

PA02, PA03, PA04 and PA06 of the security engineering group relate to providing security input, verification and validation of security, advanced vulnerability testing and assurance are still considered to be important, but do not require the same level of maturity. Also included in this middle section are the project group PA11, PA12 and PA13, quality, configuration management and the management of program risk. Organizational group PAs included in the middle section are PA16 and PA20, defining the organizations security engineering practices and providing ongoing shills and knowledge, both of considerable importance. It is considered that the organization will use the processes on a periodic basis.

The remaining PAs PA09 from the security engineering group, security coordination, PA15 and PA16 from

the project group, monitor and control technical effort and planning technical effort, and PA17, PA18, PA19 and PA21, from the organizational group, improve organizations security engineering process, manage security product line evolution, manage security engineering support environment and coordinate with suppliers are assigned to the lowest level of maturity for this profile. This is because PAs are likely to be infrequent activities and thus higher levels of maturity would reap lesser benefits for the organization, even though the activities performed are important.

AN IT USER ORGANIZATION

An IT User Organization is considered to be any organisation that makes use of information technology to support, assist in the management of, or as a part of, its operations. In effect that means the vast majority of organizations. Every organization has information that requires protection to varying degrees. The protection may be from the perspective of confidentiality of the information, from the need for accuracy or integrity of the information, that the information must be available for use within specified time frames, or a combination of the above. This necessitates that the organization uses mature processes for security either from within its own resources or from a third party source. Not to do so is to is to significantly increase

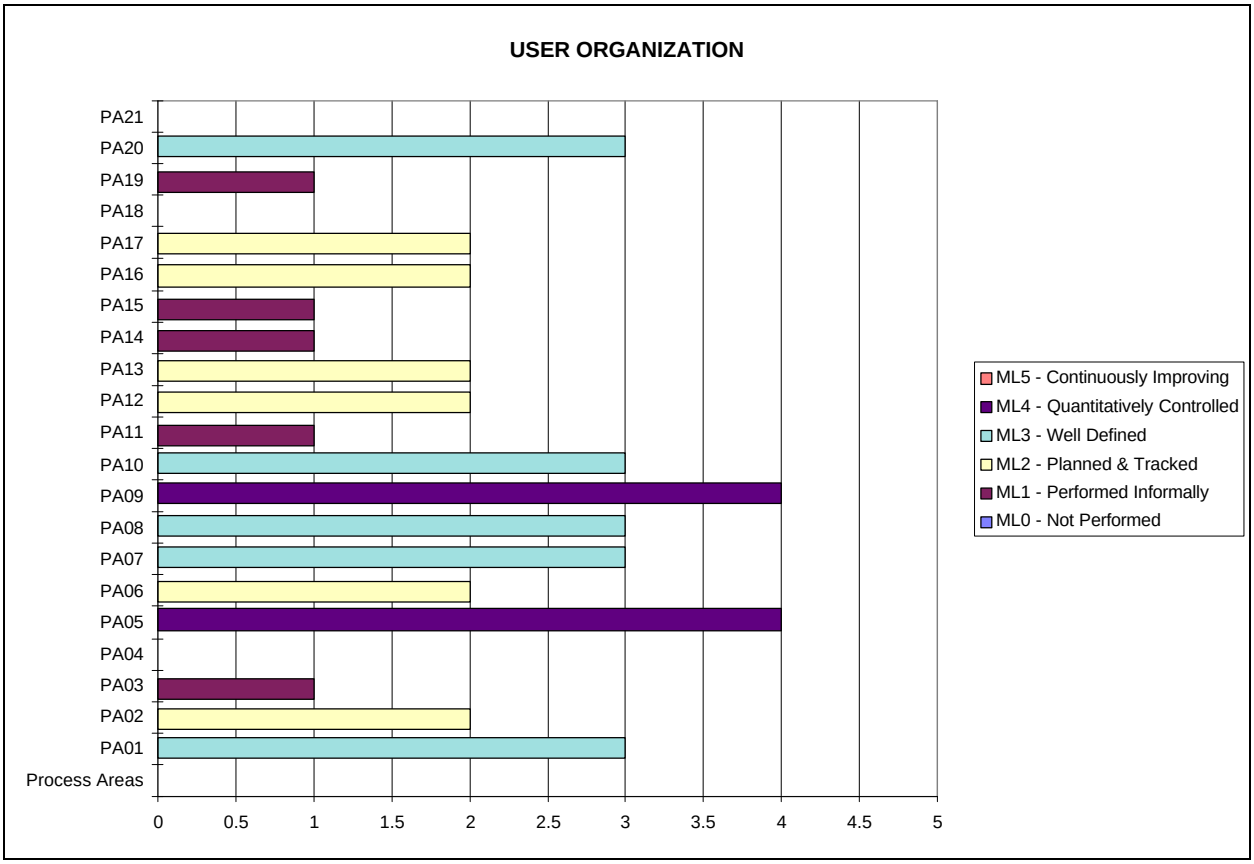

Figure 5 - Profile for a User Organization

the risk and uncertainty related to the ongoing successful operation of the organization. The profile for a user organization is shown in figure 5.

With the preceding in mind it is assessed that PA09 the Coordination of Security and PA05 Assessing the Operational Risks require the highest levels of maturity. They are closely followed by PA01, PA07, PA08, PA10 and PA20 all of which are required to support the ongoing effectiveness of the security established and communicating with the organization about security. The remaining PAs are not considered to be required at the same level of maturity with the least being assigned to the security engineering activities which should, for a user organization, be infrequent activities, and may be obtained from a third party organization. PA04, PA18 and PA21 are not considered applicable in the general case due to their highly specialised nature.

The above represents a generalized model applicable to all types of organization. However, any particular business sector or individual organization may well wish to make adjustments for their own particular situation and business. It is best if this is performed with the assistance of experts who are well versed in the details of the model and its use, to avoid problems with dependencies between PAs. It should be noted that while the intent is that the PAs are independent there is inevitably some level of dependency between PAs, and this aspect needs to be taken into account.

SUMMARY

The SSE-CMM provides a method of assessing ongoing capability in parallel with the life cycle of the product, systems or services rather than as a snap-shot at some discrete point in time during the life cycle. In this sense it is different from all other assessment approaches. That is not to say that it can or should replace other assessment methods, this is not the case. It should be used in conjunction with other snap-shot type techniques. However, its different view of the process does make the results produced uniquely different and those results have to be seen in this light. They can not be compared with or used in the same manner as other assessment results. Potential ways of using these new kinds of results are still being realised, and new ones remain to be recognised. It currently appears that the results of an SSE-CMM assessment can be used to support procurement activities and also cross-certification activities between public-key certificate certification authorities. Other potential uses of this nature are bound to arise.

© COPYRIGHT EWA-Canada 1996

REFERENCES

[SSE-CMM] System Security Engineering - Capability Maturity Model, Model Description, Version 1.0, October 1996

[SE-CMM] Systems Engineering - Capability Maturity Model, Version 1.1 CMU/SEI-95-MM-003, Carnegie Mellon University, November 1995