P^{3}I – PROTECTION PROFILE PROCESS IMPROVEMENT

Jeffrey R. Williams, Karen M. Ferraiolo
Arca Systems, Inc.
Phone: 703-734-5611
FAX: 703-790-0385
william@arca.com, ferraiolo@arca.com

ABSTRACT

Development of a protection profile under the Common Criteria is a demanding task, requiring difficult engineering decisions, complex analyses, and detailed knowledge about the intended environment and use for a product or system. We believe that building a protection profile is essentially a security engineering problem and is best approached by applying the Systems Security Engineering Capability Maturity Model (SSE-CMM). This paper describes how the process areas of the SSE-CMM match the activities needed to create an effective protection profile. Further, the paper shows how protection profile developers can use the assurance argument process to structure and manage the rationale for each requirement. The paper concludes that the use of the SSE-CMM will greatly enhance the likelihood of producing a high quality protection profile on schedule and within budget.

Keywords: *Common Criteria, Systems Security Engineering Capability Maturity Model, SSE-CMM, Protection Profile*

1. Introduction

The advent of the Common Criteria for Information Technology Security Evaluation [1] marks a significant milestone for the security community. The ability to develop a variety of protection profiles drastically increases the usefulness of the evaluation process for developers and consumers. Yet the process for writing high quality protection profiles has not been thoroughly described.

A quality protection profile will capture the security requirements that are in demand by consumers. The profile will include a detailed and supportable description of the security environment for the target of evaluation and will include only the necessary functionality and assurance requirements. The security objectives will be precise and clearly linked to the security environment, perceived threat, and security policy. The rationale for each objective will clearly show why that objective was selected and which parts of the security environment are addressed. Finally, the requirements will be clearly mapped to one or more objectives. Each requirement's rationale will rest on enough evidence to establish why it is necessary. The protection profile will also show how each security objective has been achieved and why the overall set of requirements is sufficient.

Poorly crafted protection profiles are likely to overlook needed functional and assurance requirements or may include unnecessary requirements. The rationale for these requirements may point to some vague, misunderstood, or underappreciated security objective, which may, in turn, point to a high level and poorly described threat or policy. Products and systems built to meet these profiles may not meet consumer demand. Even worse, the credibility of the evaluation process is likely to be damaged, since "evaluated" products may be insecure for their intended environments and may have useless but costly security features.

In this paper, we show how the practices described in the SSE-CMM fit into the process of developing a protection profile and how using the process greatly increases the likelihood of producing a high quality protection profile on schedule and within budget.

Incidentally, the SSE-CMM process also applies to the process of developing a Common Criteria security target. Since security targets involve a specific system in a particular environment, the SSE-CMM practices may be even more helpful in the security target context. In this paper, however, we focus on protection profile development, as that issue seems to be the most pressing.

2. What is a Protection Profile?

A protection profile contains a set of security requirements based on the functional and assurance requirements contained in the Common Criteria. User communities, product developers, integrators, or government agencies could develop protection profiles. Consumers benefit by having a common metric against which to measure competing products.

The development of a protection profile looks simple. Protection profiles must, at a minimum, meet the requirements in Chapter 3 of the Common Methodology for Information Technology Security Evaluation (CEM) [2]. According to CEM requirements, protection profiles must include:

- a description of the target of evaluation (the product or system to be evaluated), including the type of product or system and its general features
- a description of the intended security environment, including intended use assumptions, known or presumed threats, and organizational security policies
- a description of the security objectives for the target of evaluation and its environment. A rationale for each objective must be included and traced back to the appropriate part of the security environment. The protection profile must demonstrate completeness by tracing each aspect or element of the intended security environment to one or more objectives
- a set of security requirements, including functional, assurance, and environment requirements, with a rationale demonstrating all of the security objectives are addressed

The CEM requirements are not too demanding, and a developer could probably meet them with a vague description of the product, threat and environment, and objectives along with a convenient set of requirements from the "catalog" of requirements in the Common Criteria. Once a protection profile has passed an evaluation against these requirements by an independent evaluation organization, the protection profile is eligible to be included in a registry. The protection profile can then be as the basis for the evaluation of information technology.

3. What's Involved in Building a Protection Profile?

The process of developing a protection profile is described in CEM Part 2, "Evaluation Methodology" Annex C, "PP Development Background" as follows:

> "From the perspective of developing a PP, security requirements are derived, in brief, by performing analyses in a step-wise refinement manner. Analysis begins with the security environment to derive the security objectives, and then with the security objective to derive the security requirements. The security requirements form the basis of the TOE security services, the TOE development, and the TOE evaluation."

The idea here is that a protection profile developer can somewhat mechanically proceed through the process, starting with analysis of the "security environment" to determine threats, organizational security policies, and secure usage assumptions. From this information, the developer can identify both technology and non-technology "security objectives." Finally, the "security requirements" can be derived from these objectives. The Common Criteria provides only limited guidance on how to develop a protection profile that reflects this linkage [3].

Far from being mechanical, the process of developing a quality protection profile is complex and involves all aspects of the security engineering process. A deep understanding of the market, security needs, and the technology involved are required. The protection profile developer must make difficult tradeoffs involving security features, assurance evidence, complexity, and cost. Quality protection profiles depend on the process used to create them. Evaluation of protection profiles helps to ensure compliance, but cannot ensure real quality. A mature process will help to ensure the development of high quality protection profiles.

Fortunately, there is a way to ensure that security engineering processes are mature. The Systems Security Engineering Capability Maturity Model (SSE-CMM) provides a standard community-wide metric to establish and advance security engineering as a mature, measurable discipline [4]. The model defines the characteristics of a security engineering process that is explicitly defined, managed, measured, controlled, and effective. In addition, the SSE-CMM reflects the best practices of the security engineering community that are necessary to understand and solve all the security engineering issues presented in the development of a protection profile.

Protection profile developers that use a mature process based on the SSE-CMM as a basis for developing a protection profile can expect to improve the predictability of their process, so that the difference between the target and actual results decreases. This applies to predicting the cost and schedule for the effort as well. Further, protection profile developers can also expect the effectiveness of their process to improve, so that future profiles can be developed at less cost, in a shorter period of time, and with higher quality levels.

The SSE-CMM does not, however, give all the answers. The model describes in some detail the general process areas that are needed in every security engineering effort. However, the model is not a process, handbook, or training guide for building a protection profile. There is a wide range of processes that could meet requirements of the SSE-CMM. Finally, the SSE-CMM is not a replacement for evaluating protection profiles. The model increases the likelihood that a quality profile will be developed and should greatly ease the evaluation process, but third party review is still recommended.

4. Using the SSE-CMM to Build a Protection Profile

The SSE-CMM contains eleven security engineering “process areas.” (These process areas, and their constituent processes, are presented in a table in Appendix A.) Each of these areas focuses on a specific aspect of security engineering and contains a number of “base practices” designed to meet the goals for that process area. The SSE-CMM process areas go beyond the idea of “stepwise refinement” and continue throughout the security engineering process. The model recognizes that security engineering is a complex undertaking that requires the interaction of many different processes.

Understanding the Risk

A risk assessment process should be part of any protection profile development effort. Protection profiles are largely based on the known or presumed threats in the security environment. Therefore, it is critical to analyze the threats, potential vulnerabilities, and potential impacts to the security of the evaluation target carefully.

There are four process areas in the SSE-CMM directly related to understanding risk:

- ♦ Assess Threat
- ♦ Assess Vulnerability
- ♦ Assess Impact
- ♦ Assess Security Risk

Many approaches and methodologies can be used to perform these assessments. The selection of an appropriate method depends on many factors, including the type of technology involved, the amount of information available, and the expertise of the protection profile developers. A particularly critical element is the determination of appropriate metrics for the components of risk. Without appropriate metrics, it is impossible to determine the relative severity of the risks [5].

While activities involved with gathering threat, vulnerability, and impact information have been grouped into separate process areas, they are interdependent. The goal is to find combinations of threat, vulnerability, and impact that are deemed sufficiently risky to justify action. Therefore, the search for threats, for example, should be guided to a certain extent, by the existence of corresponding vulnerabilities and their impacts. Also, the protection profile developer should be sure to consider the policy, assumption, and objective information discussed in the following section.

The methodology selected as part of the protection profile development process should include the practices contained within all four PAs. A major goal of considering threat, vulnerability, and impact is to ensure that assumptions are made explicit. The protection profile builder should be wary of making unsubstantiated (or unsubstantiable) assumptions about the likelihood of threats, the severity of vulnerabilities, or the magnitude of impact. A quality protection profile will be able to ground all of the selected requirements with evidence of clear and measurable dangers.

First, the development process should include a methodology for identifying and characterizing threats to the technology. As described in the “Assess Threat” process area, the methodology should identify threats posed by nature as well as accidental and deliberate threats from man-made sources. Although protection profiles reflect the needs of a collection like environments, the characteristics of this environment can be analyzed and documented. Appropriate units of measure should be determined, so that threats can be compared. For threats arising from man-made sources, the capability and motivation of threat agents should be included in the measurements. Finally, to the extent possible, the process should keep abreast of ongoing changes in the threat spectrum in order to ensure that the profile is not based on stale information.

Second, the development process should consider the types of vulnerabilities that are likely to be present in technology under the protection profile. Of course, since the protection profiles are, in theory, implementation independent, there will not be any actual vulnerabilities to consider. A Common Criteria security target, however, will deal with a specific system, and actual vulnerabilities can be analyzed. Even for protection profiles, many security mechanisms have inherent vulnerabilities, such as the strength of an encryption algorithm or the ability to tunnel through a firewall. An understanding of the likelihood of these vulnerabilities and a method of estimating their severity is critical to understanding the risk. The “Assess Vulnerability” process area contains a set of practices designed to achieve these goals.

Third, the protection profile development process should consider the likely impact of successful exploitations of vulnerability by a threat. The selection of requirements is based on assumptions about that environment that should be made as explicit as possible. The “Assess Impact” process area practices will lead the protection profile developer through the process of identifying and characterizing important impacts to operational effectiveness, including both capabilities and assets. The process area ensures that impacts are characterized and measured according to a common metric.

Lastly, the protection profile development process should include some sort of overall risk analysis as described in the “Assess Security Risk” process area. This part of the process is designed to consider combinations of threat, vulnerability, and impact that present a significant risk to the technology in the assumed environment. By prioritizing these risks, the developer will gain insight into which of the requirements are critical and which are merely nice to have.

By encouraging a strong rationale grounded in measurable risk for each requirement, the use of the SSE-CMM will help developers avoid creating poor protection profiles that are too costly to implement, too difficult for users, or full of security holes. By following the process described here, the protection profile designer will not only be able to justify what is necessary, but what can be left out as well. The information gathered during the risk process will form a part of the rationale statements required as part of each protection profile. Consumers will understand that the requirements are based on a measurable existing threat, and are not just the byproduct of security professional paranoia.

Understanding Policy, Assumptions, and Objectives

In conjunction with developing a good understanding of the risk environment, the protection profile developer also needs to consider the other aspects of the intended environment for the technology. The Common Criteria calls out organizational security policies and security usage assumptions.

There are three process areas in the SSE-CMM directly related to policy, assumptions, and objectives:

- Specify Security Needs
- Coordinate Security
- Monitor Security Posture

The protection profile development process should attempt to achieve a true understanding of the needs of the assumed consumers of the technology. The "Specify Security Needs" process area contains the practices required to achieve this goal. The developer should have a clear picture of the purpose of the technology and how it is likely to be used.

To achieve this vision, the policies, laws, standards, and other external influences and constraints on the technology should also be identified. An understanding of the organization, the physical attributes of the environment, the people involved, and the technology involved are all critical. Using this background and the understanding of risk described above, a high level security oriented view of the technology can be created, and high level goals for the protection profile can be identified.

A critical part of the SSE-CMM process is to ensure that these objectives meet the needs of the consumers. The protection profile developer may want to perform market surveys to verify that the protection profile accurately reflects the current need. The "Coordinate Security" process area contains practices describing how protection profile developers should work with the community and consumers to ensure that the profile is valid. Further, the "Monitor Security Posture" process area contains practices that will be helpful to the protection profile developer by ensuring that the background information does not change unnoticed during the development and vetting process.

This background, like the risk information, goes a long way towards justifying the provisions of the protection profile to consumers. By demonstrating that the protection profile fits the intended context, consumer confidence will be greatly improved.

Identifying Requirements

Choosing a complete and consistent set of requirements is the heart of the protection profile development process. Using the background and risk information discussed above, the requirements process selects a set of requirements that balances all the competing interests.

There are four process areas in the SSE-CMM directly related to the requirements process:

- Provide Security Input
- Coordinate Security
- Administer Security Controls
- Specify Security Needs

The "Provide Security Input" process area has an unassuming name but represents a complex process of proposing candidate solutions, evaluating these alternatives, and selecting the best of them. The process area assumes that the technology is being designed and built by an engineering team, not a security organization in isolation. Therefore, the solutions proposed and selected must take into consideration all the constraints of performance, cost, hardware, software, human factors, and other disciplines.

The Common Criteria allows for some refinement and extension of the security requirements presented in the criteria itself. For example, some requirements allow “assignment” and “selection,” where parameters can be created or selected. Also, requirements can be “refined” or “extended” to change the scope of a requirement. All these operations should be accompanied by a strong rationale for the solution chosen. The “Provide Security Input” process area is the appropriate approach to making and justifying these decisions.

The process of selecting the necessary and sufficient set of requirements involves a large amount of communication between a number of different engineering groups. The protection profile developers must be in communication with engineers from a variety of disciplines. The practices in the “Coordinate Security” process area apply here. Proposed solutions from other disciplines should be analyzed to ensure that they are compatible with the security requirements already selected. Also, security engineering solutions should be examined by engineers from other disciplines.

Further, because the security requirements in the Common Criteria cover only the technology, there is a need to select compatible requirements that cover other areas, such as the environment, personnel, and procedures. The base practices in the “Administer Security Controls” process area will be helpful in this process. Although this process area mostly targets the operation of secure technology, some important aspects of working with operational parts of the security environment are captured. This information should be considered as part of the security background for the Common Criteria requirements selected.

The “Specify Security Needs” process area contains several practices relevant to capturing and managing the set of requirements in a protection profile. This process will maintain the set of requirements, ensuring that each requirement is consistently documented, justified by risk and environment information, validated against the market, and verified.

Understanding Assurance

Choosing assurance requirements to include in a protection profile is a complex task. In many cases it will be difficult to determine how much evidence consumers are willing to pay for in order to assure the security of system functions.

There are four process areas in the SSE-CMM directly related to assurance:

- Specify Security Needs
- Build Assurance Argument
- Provide Security Input
- Coordinate Security

The “Specify Security Needs” process area, discussed above, applies equally well to the problem of determining assurance requirements. However, the importance of carefully understanding the market in this context cannot be underestimated. Only by carefully examining the market, security environment, and risk posture can the protection profile developer select a compelling set of assurance requirements. The practices in this process area lead the developer through this process.

The SSE-CMM focuses on the notion of an “assurance argument” to help the developer structure the claims and evidence related to assurance. The “Build Assurance Argument” process area has practices that target the process of identifying the appropriate evidence, managing the development of that evidence, and packaging the evidence into a compelling argument that the technology has achieved a set of claims. The assurance argument approach will allow the developer to structure the inquiry into assurance requirements, ensuring that claims are not overlooked and that each claim is supported by sufficient evidence [6].

This process lends itself well to the process of selecting evidence requirements from the Common Criteria. The protection profile developer should start with the understanding of the risk and security environment developed in the process described above. If, for some reason, risks related to assurance have not been considered, then the developer should revisit the analysis of threats, vulnerabilities, and impacts. For example, the protection profile developer should consider the likelihood and severity of design and implementation flaws, documentation errors, testing coverage problems, and analysis weaknessses.

The Common Criteria allows refinement, augmentation, and extension of the assurance requirements when necessary. This process should be carefully justified when used, as it makes the process of comparison between products difficult. As with the functional requirements, the base practices of the “Provide Security Input” process will guide the developer through the process of selecting and modifying the assurance requirements.

A traditional problem with developing assurance requirements has been the tendency to develop the evidence after the product or system has already been developed. The SSE-CMM encourages the discussion of the assurance requirements at the earliest stages of a product, so that the other engineering groups will be aware of and involved with the process of developing evidence as described in the “Coordinate Security” process. This early discussion will reduce costs and increase the quality of the assurance efforts.

The Common Criteria comes with seven packages of assurance requirements, called Evaluation Assurance Levels (EAL). These levels represent a uniformly increasing scale that balances the level of assurance obtained with the cost and effort required to attain it. The levels are intended to ease the complexity of creating a new set of assurance requirements for each protection profile and to increase the comparability of evaluations. The process for selecting an assurance level is essentially the same as that for choosing assurance requirements individually, but much less burdensome. Nevertheless, it is important to justify the selection carefully by referencing the characteristics of the risk and security environments.

Checking for Consistency and Completeness

Ensuring that the protection profile is complete, consistent, and meets a measurable market need is an important part of the profile development process. As problems are found, the other parts of the process described above will handle them.

There are two process areas in the SSE-CMM related to consistency and completeness:

- Verify and Validate Security
- Build Assurance Argument

The “Verify and Validate Security” process area contains several practices to verify that a protection profile meets its requirements and is valid with respect to the market. To verify a protection profile, the basic process outlined in the CEM is a good place to start. The CEM process verifies that the protection profile meets the requirements in the protection profile specification contained in the Common Criteria. Essentially, the evaluation checks the profile’s description of the target, security environment, security objectives, and security requirements to ensure that they are complete, consistent, and justified for the intended environment.

The validation part of the SSE-CMM process area involves making sure that the protection profile meets a real market need. This step is critical to ensuring that the profile defines a combination of functional and assurance requirements that consumers really want. Another possibility, of course, is that the developer has designed the profile in order to create a market or to raise the bar for a certain class of security technology. Validating that the profile is likely to accomplish these goals successfully is an important step.

The verification and validation results are an important input to the “Build Assurance Argument” process area, which will ensure that the results of this analysis become part of the assurance argument and thus increase confidence in the protection profile.

The Capability Dimension

The capability of an organization to perform each of the process areas described above can be measured and improved using the capability dimension of the SSE-CMM. The model has five levels, called “capability levels,” that describe increasing levels of organizational capability to perform a process area.

For example, an organization attains Level 1 in a process area simply by performing all the base practices of that area. Level 2 indicates that the organization is planning and tracking those base practices. Level 3 organizations will have a institutionalized process for this area. Level 4 indicates that the organization is quantitatively measuring and controlling the process. Level 5 is characterized by continuous improvement of the practices.

5. Why follow the CMM approach?

The first CMM was the Software CMM, developed by the Software Engineering Institute (SEI) of Carnegie Mellon University. The Software CMM was developed in response to problems in the software development industry, that is late, poor-quality, and over-budget software projects. The model was developed as a guide for software organizations to use in defining and improving software practices. The Software CMM has been in use for over ten years and results in the software community have shown gains in productivity, early software defect detection, product quality, and time-to-market [7]. By using the SSE-CMM, we believe that similar results can be achieved in the development of security related artifacts, including protection profiles.

6. Conclusions

A key benefit of the use of the SSE-CMM in the process of developing protection profiles is that the justification for each of the requirements will be supported by a well-developed argument. The legacy of the TCSEC shows that consumers are not interested in requirements that are not clearly supported by a convincing rationale. High quality protection profiles are key to the success of the Common Criteria. Poor profiles will frustrate developers and consumers alike, who will look to other methods for security and assurance.

In this paper, we have described the process of developing a Common Criteria protection profile as a security engineering problem. We then argued that the SSE-CMM provides insight into the necessary characteristics of that process. Grounding the development in sound security engineering practice greatly increases the likelihood that high quality protection profiles will be developed on time and within budget. This, we conclude, will greatly increase the acceptance of the Common Criteria.

We recommend that:

- Organizations developing protection profiles look to the SSE-CMM for guidance on what activities should be part of the process, and how those practices might be improved.
- Organizations seeking to have protection profiles developed should use the SSE-CMM as a method of selecting prospective developers.
- The Common Criteria team developing protection profile guidance should use the SSE-CMM as a framework.

This, we conclude, will enhance the quality of protection profiles and greatly increase the acceptance of the Common Criteria.

References

[1] ISO/IEC SC27 N2161. The Common Criteria for Information Technology Security Evaluation. November 15, 1998. Available at http://csrc.nist.gov/cc/ccv20/ccv2list.htm

[2] CEM-97/017. Common Criteria Project. The Common Methodology for Information Technology Security Evaluation. September 17, 1997. Available at http://csrc.nist.gov/cc/cem/cemlist.htm

[3] ISO/IEC JTC 1/SC 27/WG 3 N452, Guide for Production of PP's and ST's, Version 0.6. July 8, 1998. Available at http://csrc.nist.gov/cc/t4/wg3/3n452.pdf

[4] Systems Security Engineering Capability Maturity Model. Model Description, Version 2.0. 1 April 1999. Available at http://www.sse-cmm.org

[5] Williams, Jeffrey R. and George F. Jelen., "A Practical Approach to Improving and Communicating Assurance." Proceedings of the 11th Annual Canadian Information Technology Security Symposium, Ottawa, Canada. May, 1999.

[6] Jelen, George F. and Jeffrey R. Williams. "A Practical Approach to Measuring Assurance." Proceeding of the 14th Annual Computer Security Applications Conference. Los Alamitos, CA: IEEE Computer Society, 1998.

[7] J. Herbsleb, A. Carlton, J. Rozum, and D. Zubrow, Benefits of CMM-based software process improvement: initial results, CMU/SEI-94-TR-13, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 1994.

Appendix A: SSE-CMM Security Process Area Summaries

Each process area (PA) has one or more goals and Base Practices (BP). To successfully achieve Level 1 for a PA, an organization must perform each of the BPs and successfully accomplish the goals. Higher levels are achieved by performing other practices as described in the SSE-CMM.Below, the titles of each of these PAs and BPs. The SSE-CMM model [4] contains a complete description of these practices. The security engineering process areas are organized alphabetically because there is no necessary sequence for the process areas. Additional information about the model can be obtained from the authors or the SSE-CMM web site at http://www.sse-cmm.org.

PA 01	**Administer Security Controls**
Goal 1	Security controls are properly configured and used.
BP.01.01	Establish responsibilities and accountability for security controls and communicate them to everyone in the organization.
BP.01.02	Manage the configuration of system security controls.
BP.01.03	Manage security awareness, training, and education programs for all users and administrators.
BP.01.04	Manage periodic maintenance and administration of security services and control mechanisms.

PA 02	**Assess Impact**
Goal 1	The security impacts of risks to the system are identified and characterized.
BP.02.01	Identify, analyze, and prioritize operational, business, or mission capabilities leveraged by the system.
BP.02.02	Identify and characterize the system assets that support the key operational capabilities or the security objectives of the system.
BP 02.03	Select the impact metric to be used for this assessment,
BP 02.04	Identify the relationship between the selected metrics for this assessment and metric conversion factors if required,
BP 02.05	Identify and characterize impacts.
BP 02.06	Monitor ongoing changes in the impacts.

PA 03	**Assess Security Risk**
Goal 1	An understanding of the security risk associated with operating the system within a defined environment is achieved.
Goal 2	Risks are prioritized according to a defined methodology.
BP.03.01	Select the methods, techniques, and criteria by which security risks, for the system in a defined environment are analyzed, assessed, and compared.
BP 03.02	Identify threat/vulnerability/impact triples (exposures),
BP 03.03	Assess the risk associated with the occurrence of an exposure.
BP 03.04	Assess the total uncertainty associated with the risk for the exposure.
BP 03.05	Order risks by priority.
BP 03.06	Monitor ongoing changes in the risk spectrum and changes to their characteristics.

PA 04	**Assess Threat**
Goal 1	Threats to the security of the system are identified and characterized.
BP 04.01	Identify applicable threats arising from a natural source.
BP 04.02	Identify applicable threats arising from man-made sources, either accidental or deliberate.
BP 04.03	Identify appropriate units of measure, and applicable ranges, in a specified environment.
BP 04.04	Assess capability and motivation of threat agent for threats arising from man-made sources.
BP 04.05	Assess the likelihood of an occurrence of a threat event.
BP 04.06	Monitor ongoing changes in the threat spectrum and changes to their characteristics.

PA 05	**Assess Vulnerability**
Goal 1	An understanding of system security vulnerabilities within a defined environment is achieved.
BP.05.01	Select the methods, techniques, and criteria by which security system vulnerabilities in a defined environment are identified and characterized.
BP.05.02	Identify system security vulnerabilities.
BP.05.03	Gather data related to the properties of the vulnerabilities.

BP.05.04	Assess the system vulnerability and aggregate vulnerabilities that result from specific vulnerabilities and combinations of specific vulnerabilities.
BP.05.05	Monitor ongoing changes in the applicable vulnerabilities and changes to their characteristics.

PA 06	**Build Assurance Argument**
Goal 1	The work products and processes clearly provide the evidence that the customer's security needs have been met.
BP.06.01	Identify the security assurance objectives.
BP.06.02	Define a security assurance strategy to address all assurance objectives.
BP.06.03	Identify and control security assurance evidence.
BP.06.04	Perform analysis of security assurance evidence.
BP.06.05	Provide a security assurance argument that demonstrates the customer's security needs are met.

PA 07	**Coordinate Security**
Goal 1	All members of the project team are aware of and involved with security engineering activities to the extent necessary to perform their functions.
Goal 2	Decisions and recommendations related to security are communicated and coordinated.
BP.07.01	Define security engineering coordination objectives and relationships.
BP.07.02	Identify coordination mechanisms for security engineering.
BP.07.03	Facilitate security engineering coordination.
BP.07.04	Use the identified mechanisms to coordinate decisions and recommendations related to security.

PA 08	**Monitor Security Posture**
Goal 1	Both internal and external security related events are detected and tracked.
Goal 2	Incidents are responded to in accordance with policy.
Goal 3	Changes to the operational security posture are identified and handled in accordance with the security objectives.
BP 08.01	Analyze event records to determine the cause of an event, how it proceeded, and likely future events.
BP 08.02	Monitor changes in threats, vulnerabilities, impacts, risks, and the environment.
BP 08.03	Identify security relevant incidents.
BP 08.04	Monitor the performance and functional effectiveness of security safeguards.
BP 08.05	Review the security posture of the system to identify necessary changes.
BP.08.06	Manage the response to security relevant incidents.
BP.08.07	Ensure that the artifacts related to security monitoring are suitably protected.

PA 09	**Provide Security Input**
Goal 1	All system issues are reviewed for security implications and are resolved in accordance with security goals.
Goal 2	All members of the project team have an understanding of security so they can perform their functions.
Goal 3	The solution reflects the security input provided.
BP.09.01	Work with designers, developers, and users to ensure that appropriate parties have a common understanding of security input needs.
BP.09.02	Determine the security constraints and considerations needed to make informed engineering choices.
BP.09.03	Identify alternative solutions to security related engineering problems.
BP.09.04	Analyze and prioritize engineering alternatives using security constraints and considerations.
BP.09.05	Provide security related guidance to the other engineering groups.
BP.09.06	Provide security related guidance to operational system users and administrators.

PA 10	**Specify Security Needs**
Goal 1	A common understanding of security needs is reached between all parties, including the customer.
BP.10.01	Gain an understanding of the customer's security needs.
BP.10.02	Identify the laws, policies, standards, external influences and constraints that govern the system.
BP.10.03	Identify the purpose of the system in order to determine the security context.
BP.10.04	Capture a high-level security oriented view of the system operation.

BP.10.05	Capture high-level goals that define the security of the system.
BP.10.06	Define a consistent set of statements which define the protection to be implemented in the system.
BP.10.07	Obtain agreement that the specified security meets the customer’s needs.

PA 11	**Verify and Validate Security**
Goal 1	Solutions meet security requirements.
Goal 2	Solutions meet the customer's operational security needs.
BP.11.01	Identify the solution to be verified and validated.
BP.11.02	Define the approach and level of rigor for verifying and validating each solution.
BP.11.03	Verify that the solution implements the requirements associated with the previous level of abstraction.
BP.11.04	Validate the solution by showing that it satisfies the needs associated with the previous level of abstraction, ultimately meeting the customer’s operational security needs.
BP.11.05	Capture the verification and validation results for the other engineering groups.

P^3I - Protection Profile Process Improvement

Jeffrey R. Williams
Arca Systems, Inc.
williams@arca.com

Karen M. Ferraiolo
Arca Systems, Inc.
ferraiolo@arca.com

Copyright © 1999 Arca Systems
All rights reserved

Arca
An Exodus Communications Company

I Hope To Show:

- Building a protection profile is an engineering problem
- The SSE-CMM can lead profile developers through the process
- Applying SSE-CMM practices will lead to higher quality profiles

SSE-CMM = Systems Security Engineering
Capability Maturity Model

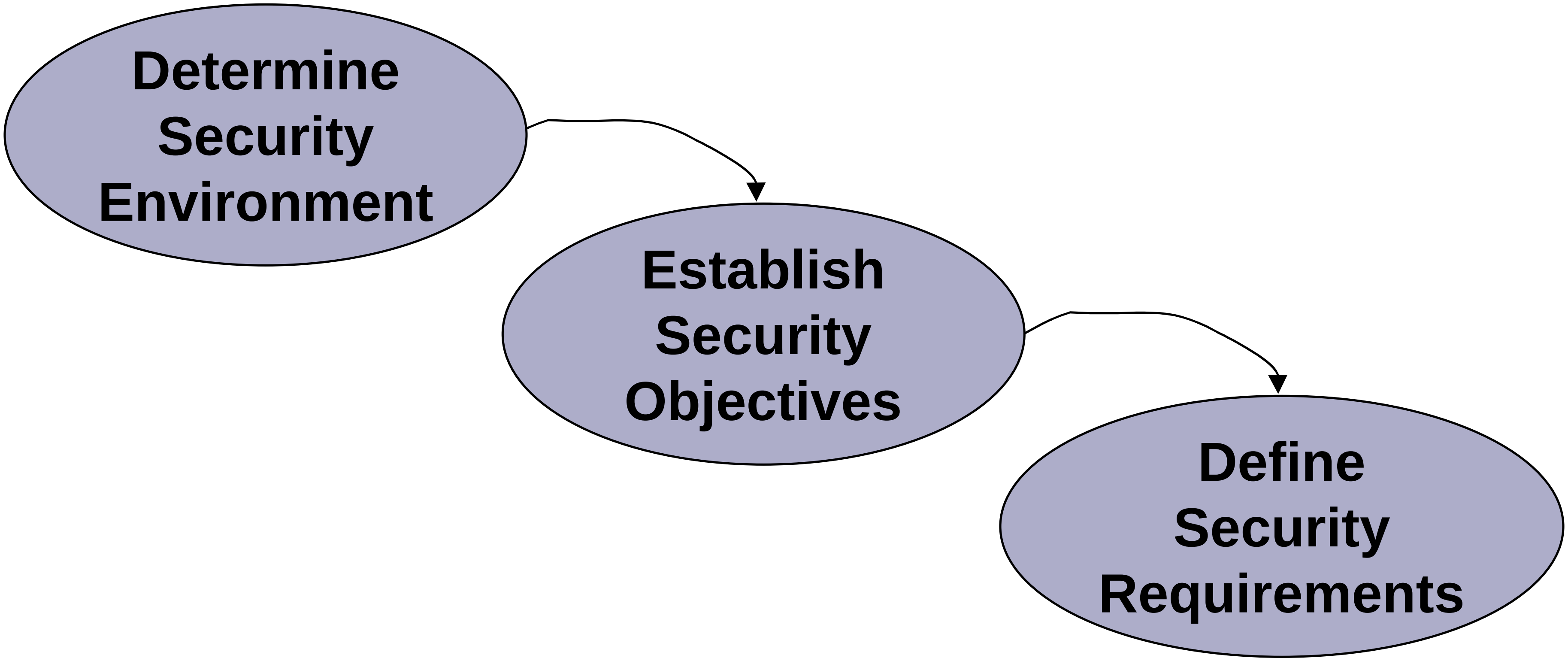
Copyright © 1999 Arca Systems
All rights reserved

What is a Protection Profile?

- a set of security requirements
- based on Common Criteria functional/assurance requirements
- common metric to measure products

Copyright © 1999 Arca Systems
All rights reserved

Common Criteria Process


Determine Security Environment
Establish Security Objectives
Define Security Requirements

Copyright © 1999 Arca Systems
All rights reserved

What are good security requirements?

- represent system at a high level
- reflect consumer needs
- part of overall engineering solution

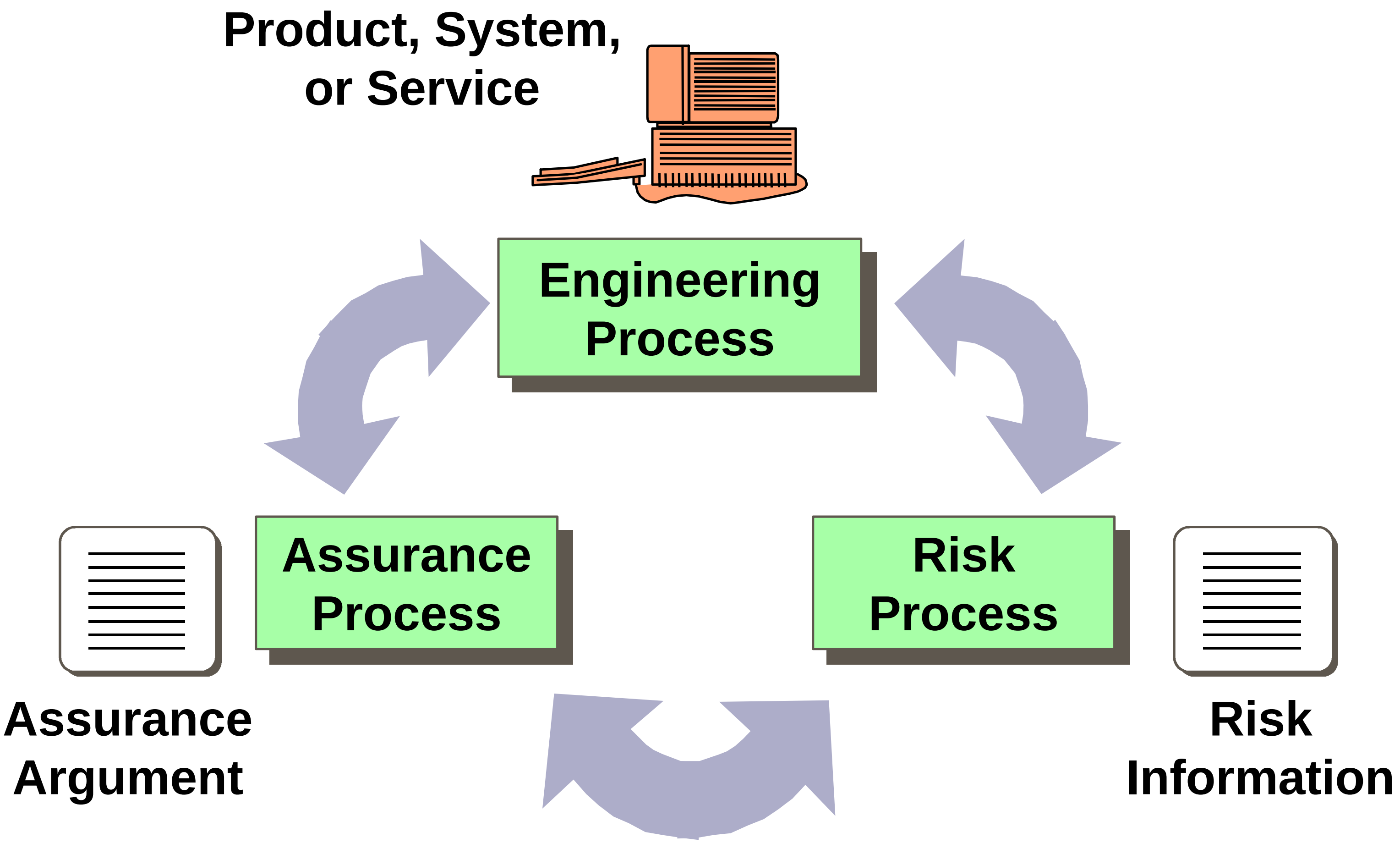
Copyright © 1999 Arca Systems
All rights reserved

SSE-CMM Overview

- defines essential characteristics of security engineering process
- metric for measuring performance of security engineering principles
- guide for improving performance

Copyright © 1999 Arca Systems
All rights reserved

Security Engineering Process Components



Product, System, or Service

Engineering Process

Assurance Process

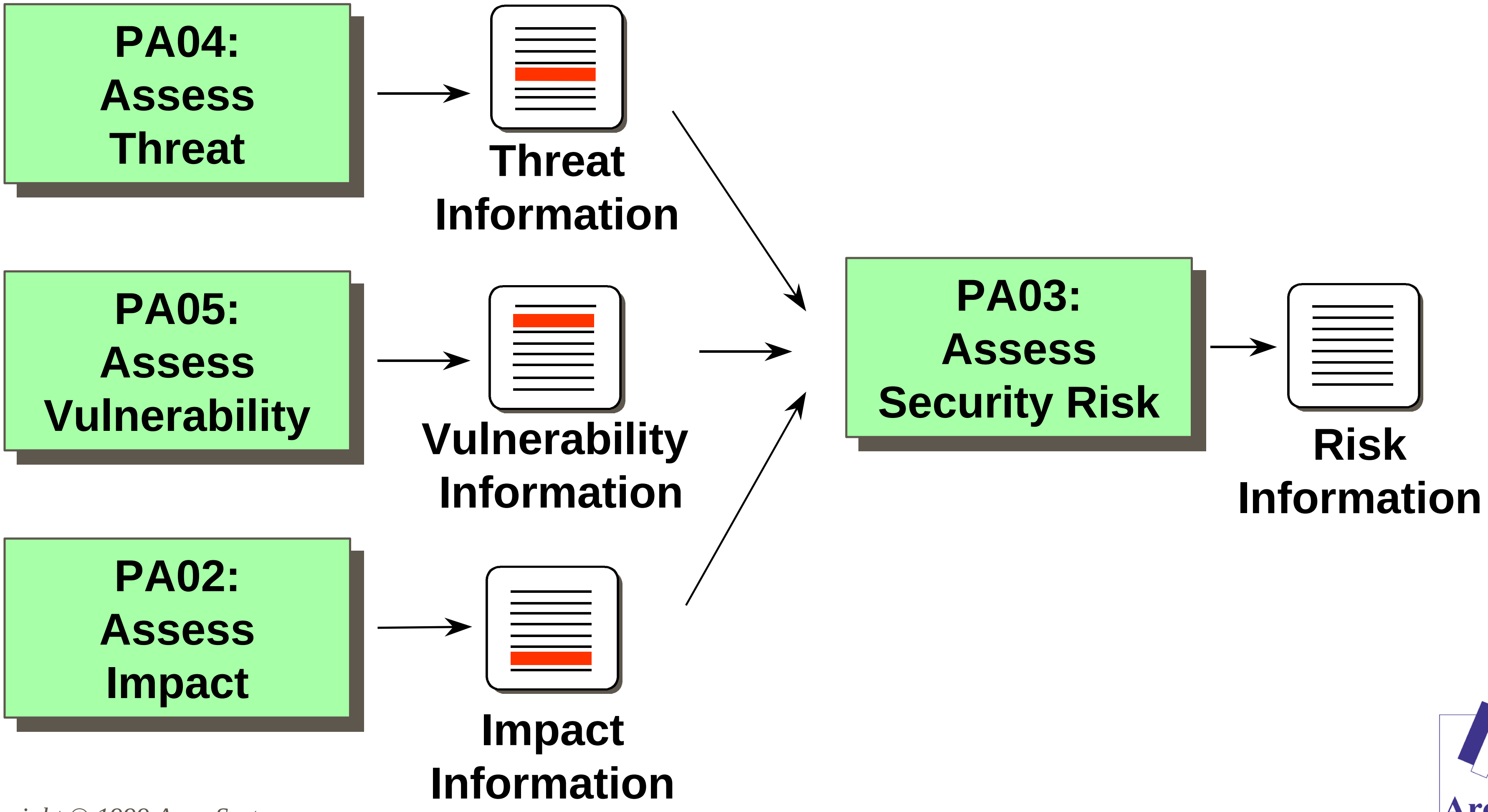
Risk Process

Assurance Argument

Risk Information

Copyright © 1999 Arca Systems
All rights reserved

Understanding the Risk



PA04: Assess Threat

Threat Information

PA05: Assess Vulnerability

Vulnerability Information

PA02: Assess Impact

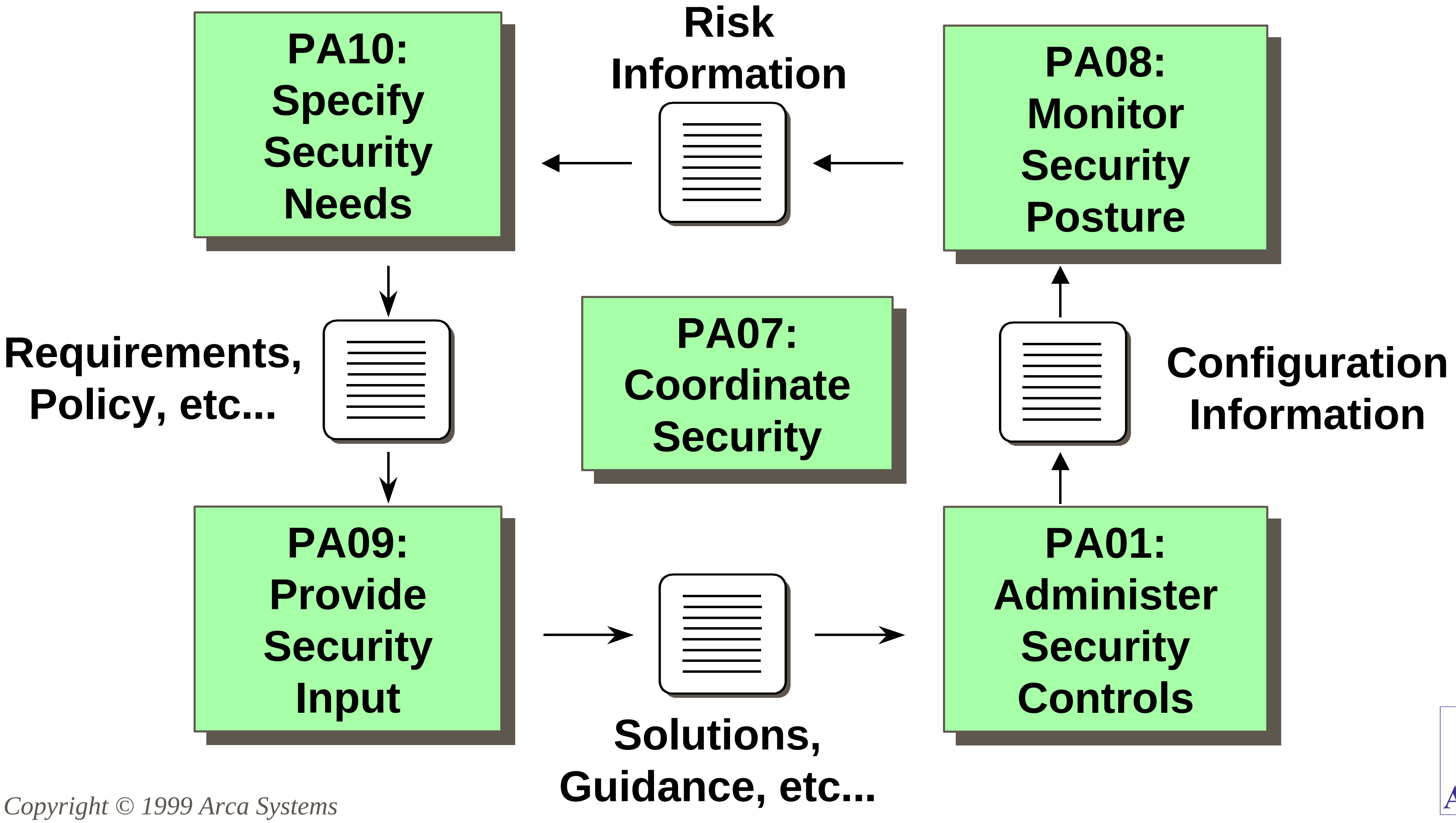
Impact Information

PA03: Assess Security Risk

Risk Information

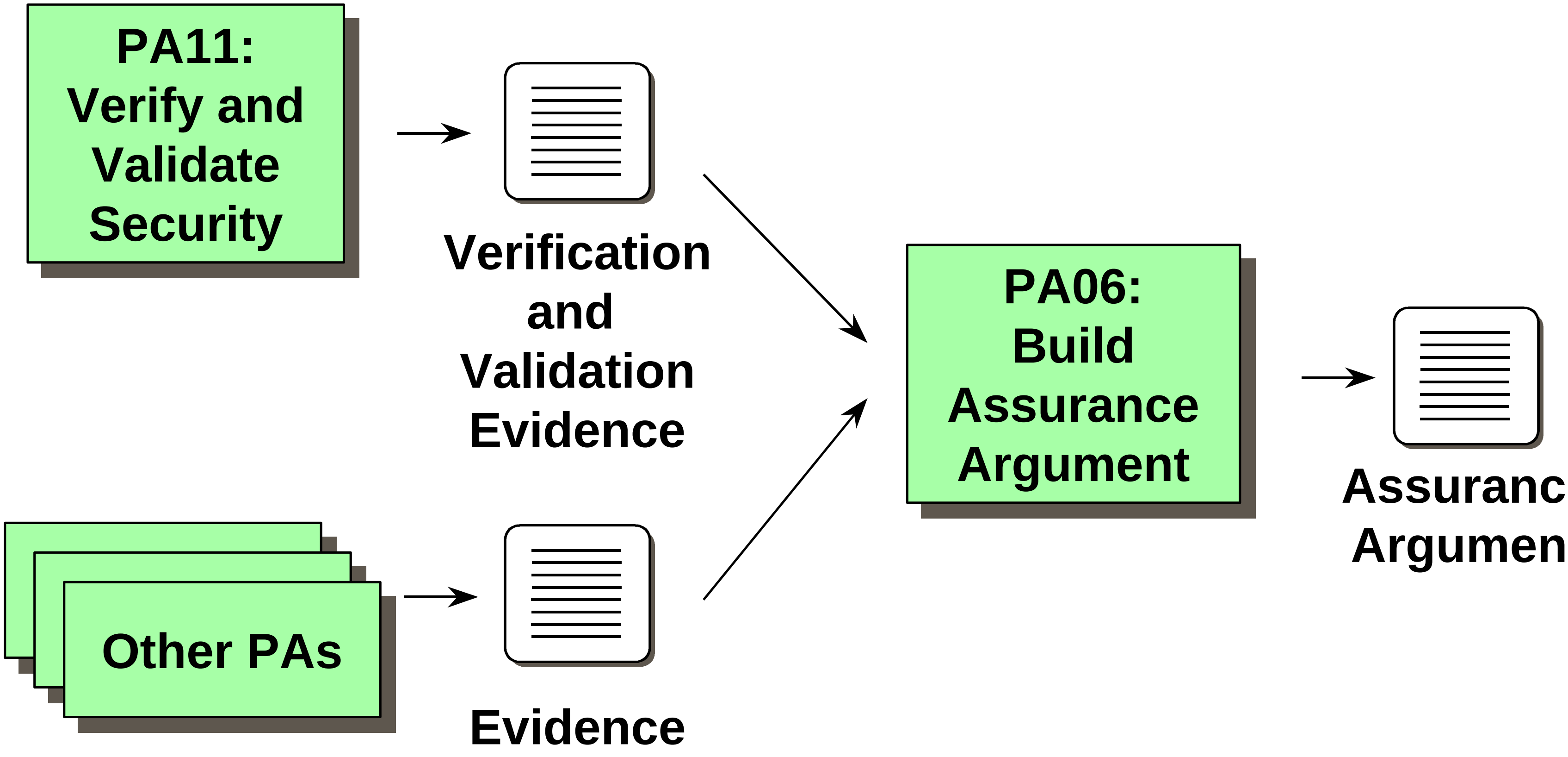
Copyright © 1999 Arca Systems
All rights reserved

Security: Part of the Systems Engineering Process


PA10: Specify Security Needs
Risk Information
PA08: Monitor Security Posture
Requirements, Policy, etc...
PA07: Coordinate Security
Configuration Information
PA09: Provide Security Input
PA01: Administer Security Controls
Solutions, Guidance, etc...

Copyright © 1999 Arca Systems
All rights reserved

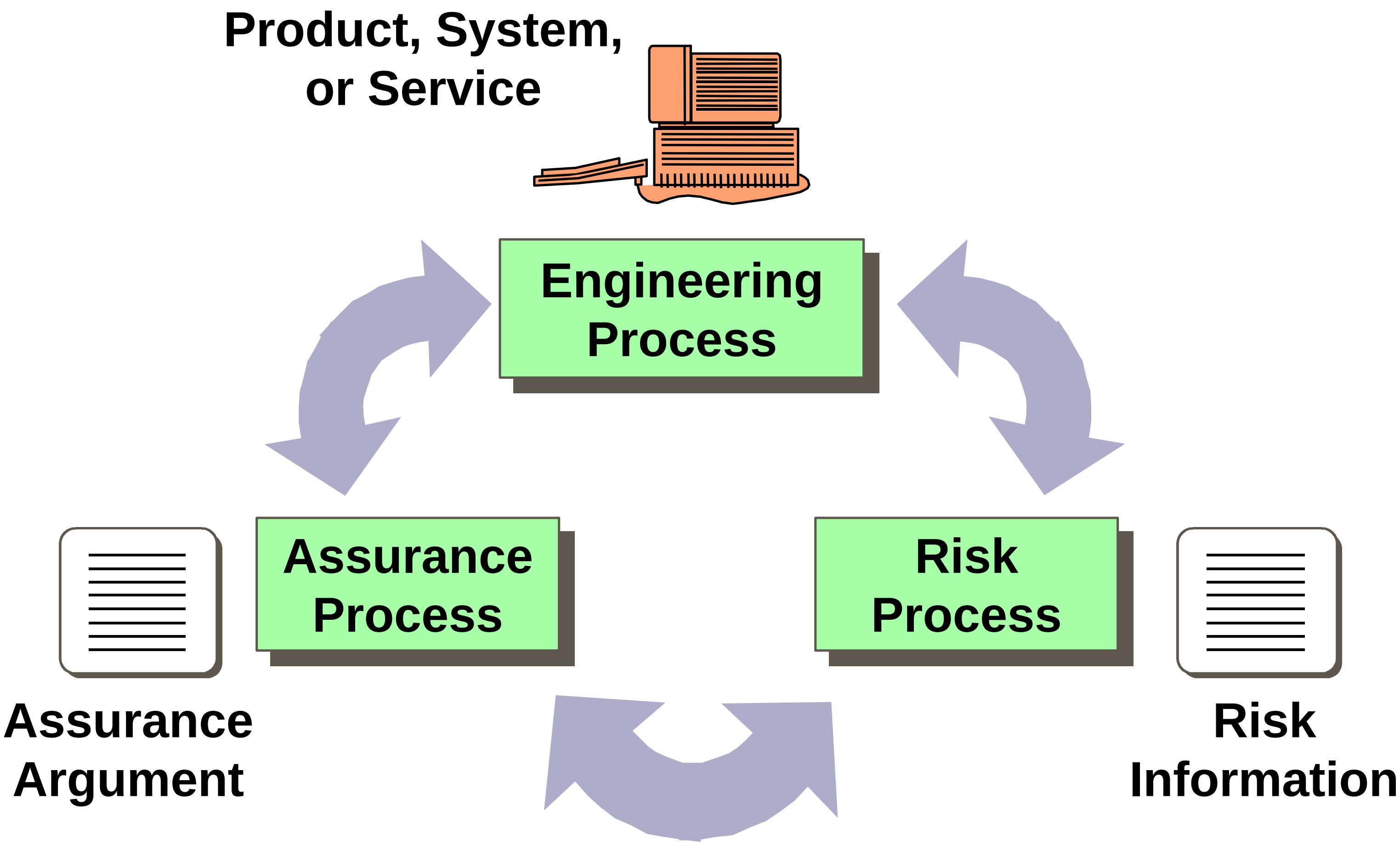
Understanding Assurance



Copyright © 1999 Arca Systems
All rights reserved

Arca
An Exodus
Communications
Company

Security Engineering Process Components



Product, System, or Service

Engineering Process

Assurance Process

Risk Process

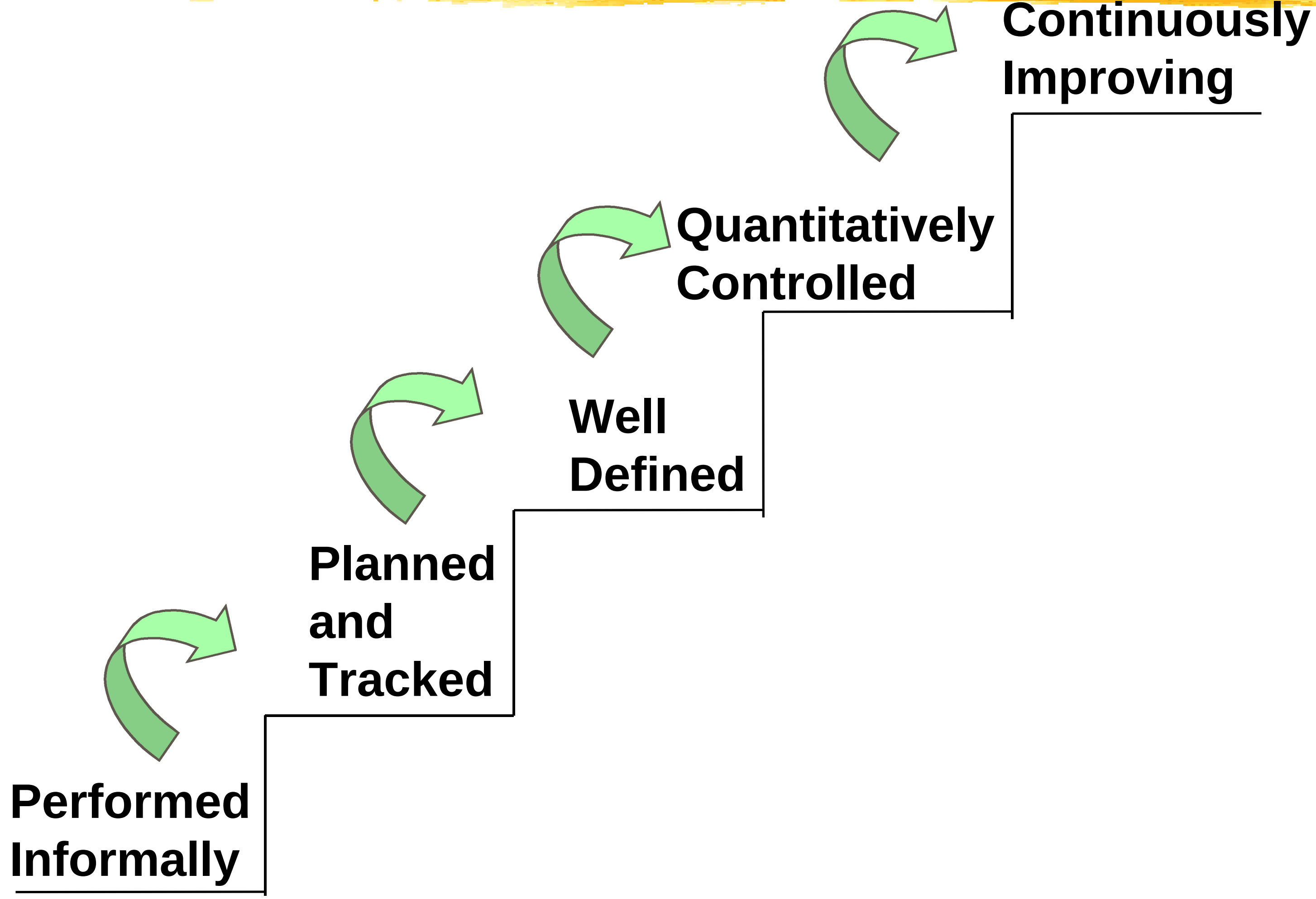
Assurance Argument

Risk Information

Copyright © 1999 Arca Systems
All rights reserved

Arca
An Exodus Communications Company

The Capability Dimension



Continuously Improving

Quantitatively Controlled

Well Defined

Planned and Tracked

Performed Informally

Copyright © 1999 Arca Systems
All rights reserved

What has application of CMMs accomplished?

- accepted way of improving process capability
- use in acquisition as indicator of capability
- ROI for software community indicates:
  - productivity gains per year: 9 - 67%
  - yearly reduction in time to market: 15 - 23%
  - yearly reduction in post-release defect reports: 10 - 94%
  - value returned on each dollar invested: 4 - 8.8%

Statistics from: "Benefits of CMM-Based Software Process Improvement: Initial Results," CMU/SEI-94-TR-13, August 1994

Copyright © 1999 Arca Systems
All rights reserved

Recommendations

- Profile developers should use the SSE-CMM as guidance
- SSE-CMM should be used in selecting profile developers
- Common Criteria team should use the SSE-CMM in developing protection profile guidance

Copyright © 1999 Arca Systems
All rights reserved