USING SECURITY METRICS TO ASSESS RISK MANAGEMENT CAPABILITIES

Christina Kormos
National Security Agency
Phone: (410)854-6094
Fax: (410)854-4661
ckormos@radium.ncsc.mil

Lisa A. Gallagher (POC)
Arca Systems, Inc.
Phone: (410)309-1780
Fax: (410)309-1781
gallagher@arca.com

Natalie Givans
Booz·Allen & Hamilton, Inc.
Phone: (703)289-5406
Fax: (703)289-5825
givans_natalie@bah.com

Nadya Bartol
Booz·Allen & Hamilton, Inc.
Phone: (703)289-5379
Fax: (703)289-5825
bartol_nadya@bah.com

Abstract

The Systems Security Engineering Capability Maturity Model (SSE-CMM) [1] measures an organization's capability to provide security products, services, or operations. Basic activities performed in security engineering are grouped together into process areas. A common question posed by those interested in using the SSE-CMM is, How do I know if applying these processes will result in a more secure system or operational capability?

To answer this question, the SSE-CMM Project Metrics Action Committee has approached the question from two different perspectives using metrics as a basis for the answer. The first perspective looks at what information the processes provide to the user. The second perspective looks at the results of those processes and what they can tell the user about how effective the processes have been in achieving "good" security. The metrics are intended to be examples from which an organization can select to then tailor to measure its own progress against its security objectives. The metrics have been organized into "Process Metrics" and "Security Metrics."

This paper presents a brief overview of the metrics, discusses how the metrics were derived, and provides an example of categorizing them. The paper then focuses on the perspective of a systems security engineering services provider, who is applying in-house SSE-CMM metrics associated with some of the process areas. The purpose is to assess no only the provider's own risk management capability, but also the client's capability to provide good security risk management services to end-users.

USING SECURITY METRICS TO ASSESS RISK MANAGEMENT CAPABILITIES

Background

The SSE-CMM determines an organization's capability to provide security products, services, or operations. Basic activities called Base Practices (BP), performed in security engineering are grouped into Process Areas (PA). An organization's capability to perform security engineering is measured by examining the organization's performance of the BP in each of the PAs and assigning a level. These levels, shown in Figure 1, represent the maturity with which the organization performs each security engineering activity. Specifically, the levels are as follows:

- Level 1—Performed Informally
- Level 2—Planned and Tracked
- Level 3—Well Defined
- Level 4—Quantitatively Controlled
- Level 5—Continuously Improving.

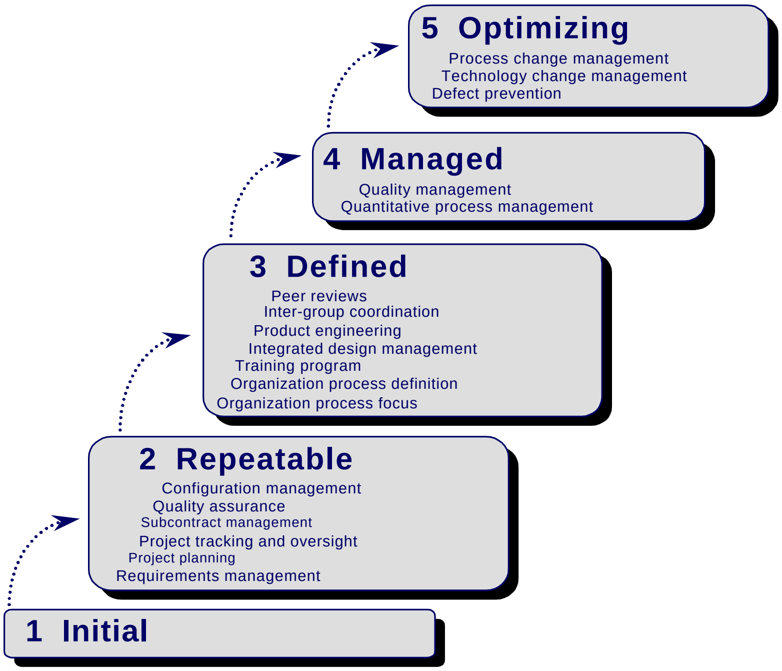


Figure 1. Continuous Capability Maturity Model

Achievement of each maturity level is indicated by performance of Generic Practices (GP), which are required for each specific maturity level.

Benefits to engineering organizations, including system integrators, application developers, product vendors, and security engineering service providers, of applying the SSE CMM are as follows:

- Savings associated with repeatable, predictable processes and practices that result in less rework
- Credit for true capability to perform, particularly in source selections
- Focus on measured organizational competency (maturity) and improvements

The SSE-CMM Appraisal Method (SSAM) [2] provides a method to conduct an appraisal of an organization's system security engineering process capability and process maturity as defined in the SSE-CMM. The SSAM is aimed primarily at appraisals conducted by third parties, but contains guidance for interpreting the method for self-assessments.

Self-assessments may be conducted for the following reasons:

- Organizational self-improvement
  - Gain an understanding of domain-related issues
  - Understand deployment of new organizational practices
  - Determine overall capability of the organization
- Process benchmarking, improvement, and institutionalization.

The SSAM provides an important tool for gaining useful insights into current processes and guidance that will lead to process improvements over time. The SSE-CMM and SSAM together provide a way to measure and improve performance in the application of security engineering principles to security engineering practice.

The SSE-CMM allows organizations to achieve different maturity levels in different PAs. It does not require the organization to achieve uniform maturity at all levels to progress to the next level, thus allowing an organization to focus on those PAs that are relevant to its specific business areas.

The model provides for increasing growth in sophistication and a number of different GPs that indicate achievement of maturity levels. Figure 2 demonstrates that the organization that achieved SSE-CMM Level 2 is performing project tracking and planning, requirements analysis, quality assurance, and configuration management. However, according to SSE-CMM maturity levels, such organization is not yet performing standard process design, process training, process measurement and management,[1] and process improvement. Similarly, the organization that has achieved Level 3 is not performing either process measurement and management or process improvement.

[1] This paper focuses on the Process Measurement portion of Process Measurement and Management activity.

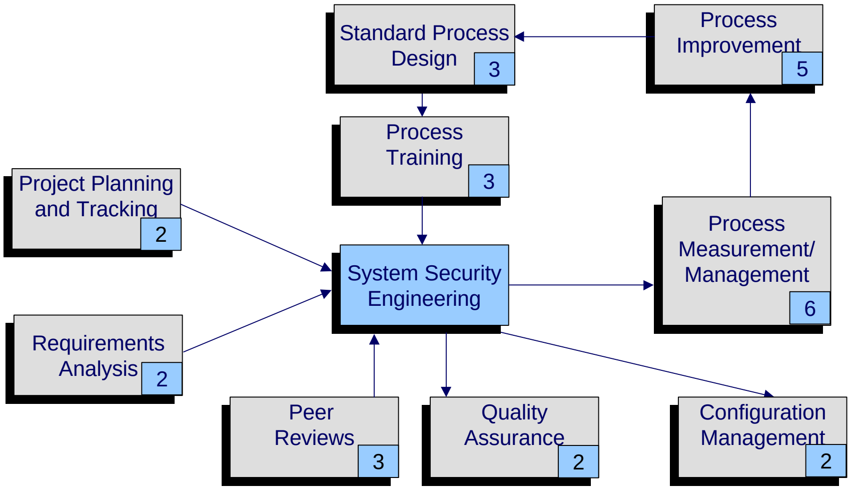


Figure 2. Implementation of Maturity Levels

With ascending maturity levels, a greater number of GPs are formalized, documented, and standardized across the organization. For example, project planning and tracking exists in some form at Levels 1 and 2, but at Level 3 it begins using organization process and project management tools. At Level 2, quality assurance involves informal reviews, whereas at Level 3 peer reviews are formalized and coordination with other system development and maintenance functions is required.

Introduction

This paper presents the SSE-CMM Project's attempts to answer a common question posed by those interested in using the model. This question is, How do I know if applying these processes will result in a more secure system or operational capability? The project has approached this question from two different perspectives using metrics as the basis for the answer. The first perspective looks at what information the processes provide to the user. The second perspective looks at the results of those processes and what they can tell the user about how effective the processes have been in achieving "good" security. The metrics discussed here are intended to be examples from which an organization can select to then tailor to measure its own progress against security objectives. The metrics have been organized into "Process Metrics" and "Security Metrics," which are defined below.

- ***Process Metrics.*** *Specific metrics that could serve as quantitative or qualitative evidence of the level of maturity for a particular process area or could serve as a binary indication of the presence or absence of a mature process.*

- ***Security Metrics.** A measurable attribute of the result of an SSE-CMM security engineering process that could serve as evidence of its effectiveness. A security metric may be objective or subjective, and quantitative or qualitative.*

The SSE-CMM Project has a subcommittee working on the development of process and security metrics. Thus far, the subcommittee has developed an initial set of metrics, discussed metrics categorization, and published an initial status report. Currently, the subcommittee is developing the Metrics Guidance document that will explore the relationship between process and security metrics and discuss various metrics validation methods. Some information from this evolving document is included in this paper.

This paper provides a brief overview of the metrics development methodology, provides examples of initial metrics and how they were derived, and presents one categorization approach. The paper then focuses on the perspective of a systems security engineering services provider, who is applying in-house SSE-CMM metrics associated with some of the PAs. The purpose is to assess not only the provider's own risk management capability, but also the client's capability to provide good security risk management services to end users.

Who Are the Metric Users?

Although the metrics are being developed primarily for the SSE-CMM user (whether government or industry), they can also be used as a self-assessment tool by any organization with a security program. These metrics provide a basis for not only measuring process improvement, but also justifying security expenditures, monitoring and objectively documenting the organization's security posture, discovering areas needing correction, and establishing security goals,

These metrics will assist the SSE-CMM user in developing a metrics program and meeting the requirements for advancing through the SSE-CMM capability levels. They are intended to be examples that an organization may tailor to their business situation. These metrics, for the most part, have been developed within the boundaries of the SSE-CMM PAs – Project, Organizational, and Security Engineering. The goal is to provide an organization with the means for demonstrating improved security effectiveness associated with its offerings of security products and services. Potential user groups for these metrics have been identified and are listed below.

- Project managers and leads—for operational or development environments or process improvement
- Chain of command and funding sources— to influence budgets, priorities, and allocation of resources
- Community at large—for awareness, competition, coordination, best practices
- Procurement (e.g., Department of Defense [DoD])—looking for services or products
- Hostile entities—as a deterrent to those who either might attack or who are in competition

- Product vendors—for assessing security product effectiveness based on engineering process improvement.

The sample metrics included in this paper and in [3] should be helpful to one or more of the user groups on this list.

A Management Perspective

Management professionals are interested in maximizing return on investment and minimizing losses of assets and information. Metrics may be used as an internal control mechanism to identify areas for management attention and requirements for additional resources. If developed and applied appropriately, the metrics can demonstrate to the management chain the programmatic and operational return on investment, therefore substantially enhancing the decision-making process concerning security expenditures and projects. Metrics may also be used as a basis for reporting progress on security-related issues. Furthermore, a metrics program can justify to external entities (such as funding sources, auditors, and customers) the value of the selected projects.

A Security Perspective

Security professionals are interested in policy and technical issues. A metrics program establishes security benchmarking, pinpoints deficits, and enables improvements. It can be used to baseline and measure improvement in the daily operations of the organization. Additionally, a metrics program can provide justification for expenditures to protect the organization’s assets, such as income, intellectual capital, investments, and opportunities.

A User Perspective

Users expect their systems to be available, operational, reliable, and effective. A security metrics program can help system administrators create and maintain a reliable, secure environment for the user.

Overview of Metrics Development

The SSE-CMM Project Metrics Action Committee has used a variety of inputs to develop the metrics. The committee began by looking at existing research results and then focused on the goals and base practices of the SSE-CMM Security Engineering PAs to derive obvious metrics.

Every process has inputs, constraints, activities, and outputs. Performance, stability, capability, improvement, and investment are central to effective process management. Figure 3 shows the progression from the process inputs and constraints, to procedures, and measurable outputs.

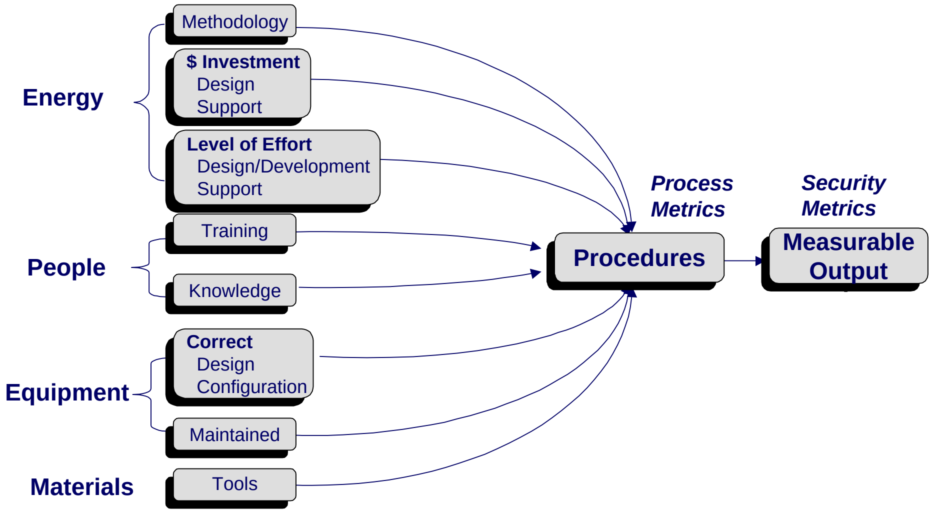


Figure 3. Metrics Development

Process performance refers to the characteristic values shown when measuring attributes of products and services that result from application of one or more processes. The existence and maturity of each process is examined first, without judging how well it is performed. Although process metrics can be obtained by measuring the entities of the process itself, security metrics can be obtained by measuring security attributes of the process results. Figure 4 illustrates the relationship between inputs into the security engineering process, the processes that are performed to accomplish security engineering, and the results of these processes.

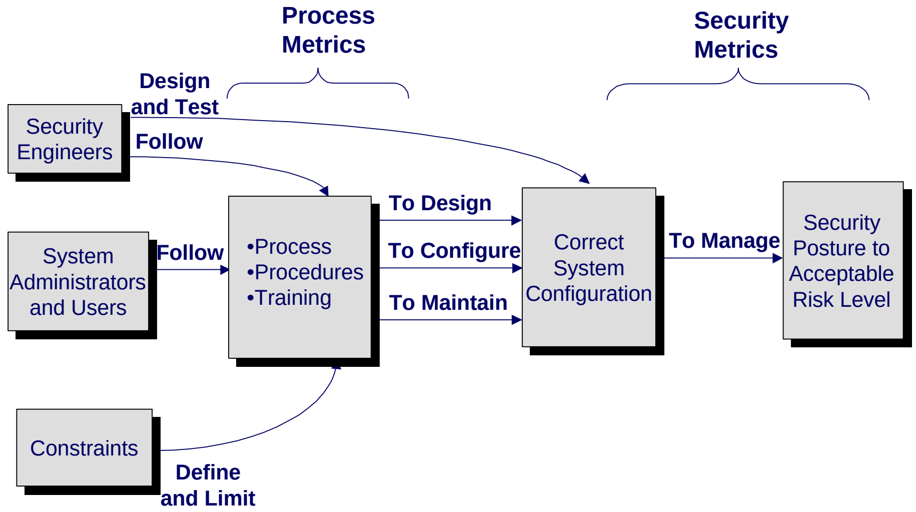


Figure 4. Process and Security Metrics Relationship

An example of specific entities that can be measured in a security engineering process and to which the process metrics can be applied is shown in Figure 5.

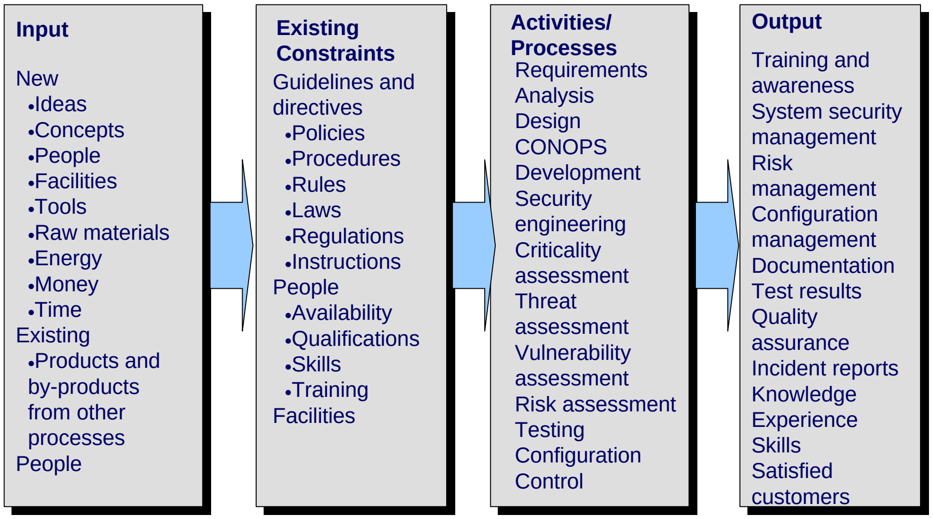


Figure 5. Measurable Process Attributes

For system security engineering, the PAs lead to either the provision of security engineering services or the development and analysis of products and systems. These are then measured by analyzing the security effectiveness of the resulting product, system, or enterprise. Examples are listed in Figure 6.

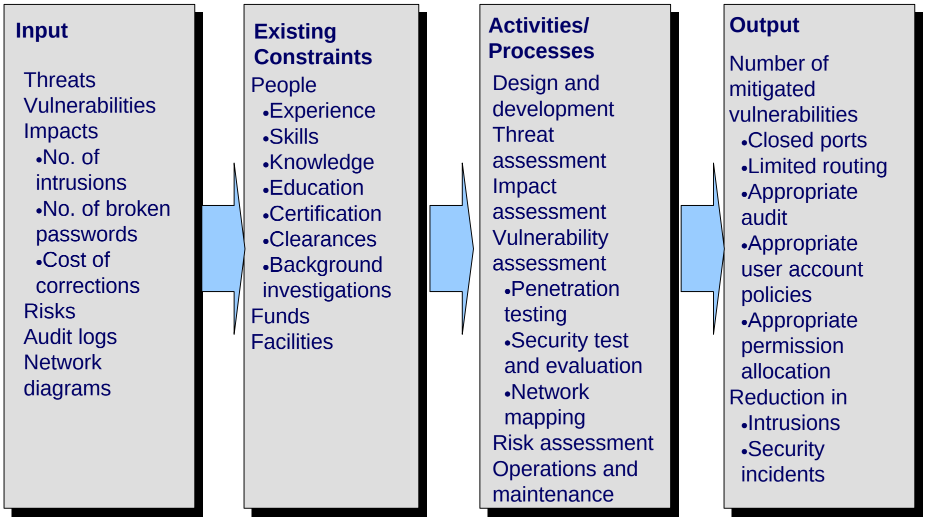


Figure 6. Measurable Security Attributes

Measuring security effectiveness is a challenging enterprise. None of the metrics can be used productively without understanding the relative importance of system security for the organization’s mission. The selected metrics should be relevant to the organization’s business areas. An organization may not require the application of Level 5 SSE-CMM capabilities relative to the cost of achieving it, and the business requirement for achieving a specific maturity level may apply to a subset of the system engineering PAs.

Another challenge of measuring security effectiveness in networks is that it can only be done relative to the known threat environment, attacks, and vulnerabilities. Until security engineers can anticipate future attacks, any security engineering effort will be performed without assurance that the applied measures provide protection from known and unknown attacks.

Finally, the metrics may not be used as an absolute measurement of the organization’s performance if the importance and the state of system security before the effort are unknown. Knowledge of the baseline security posture and its improvement goals is required to obtain any meaningful measurement of the organization’s process and security performance. To identify whether the security engineering effort is effective in appropriately protecting the organizations systems and networks as it relates to the known threat environment, it is essential to be able to measure the “before” and “after” states of these systems and networks. Figure 7 demonstrates this concept.

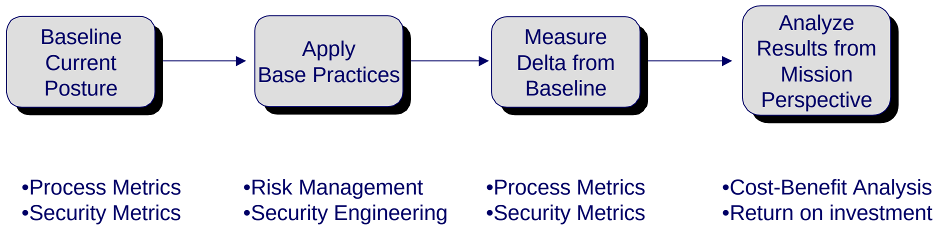


Figure 7. Applying Process and Security Metrics

As illustrated in the figure, the first step is to apply metrics to capture the baseline security posture of the system by applying both process and security metrics. SSE-CMM BPs are then performed to identify countermeasures that would result in improvements in the organization’s security posture and to implement them. Performing another assessment after the recommended countermeasures have been applied would provide a means to measure the difference between “before” and “after” security posture and identify relative improvement in it. This result could then be analyzed against the organization’s mission (e.g., cost-benefit analysis or return on investment) to interpret the meaning of the results for the organization.

Grouping of Metrics

In the process of developing the metrics, numerous methods were used for grouping them, which also resulted in developing additional metrics. One such method for discovering and categorizing metrics, the top-down approach, is discussed here.

The top-down approach, illustrated in Figure 8, considers the guidance and policy and the user, security professional, auditor, and management perspectives. Security professionals and auditors often focus on reducing threats and vulnerabilities to increase security, whereas users and managers focus on operational capability, low cost, and user friendliness. Managers are seeking a return on investment and therefore tend to focus on metrics that reduce negative effect on their mission, total costs, and human life.

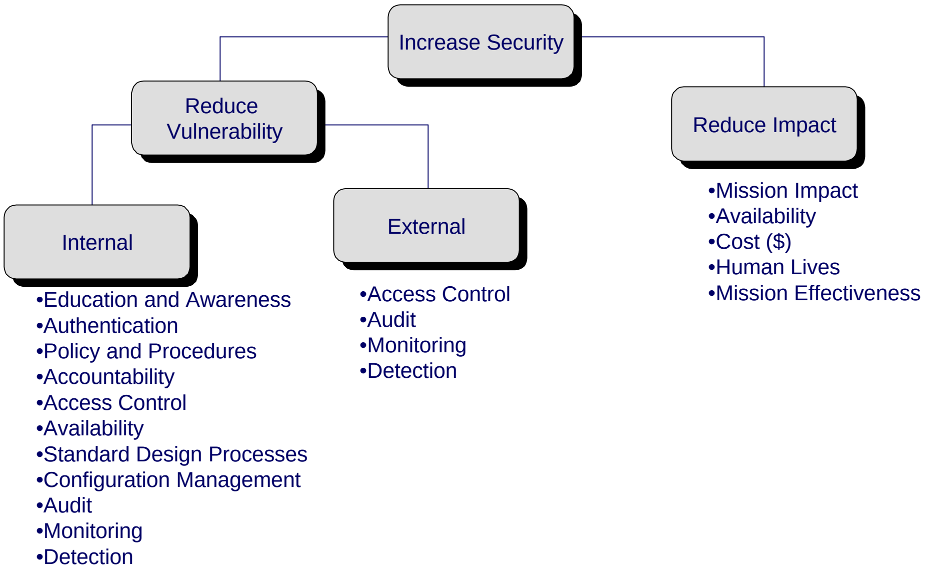
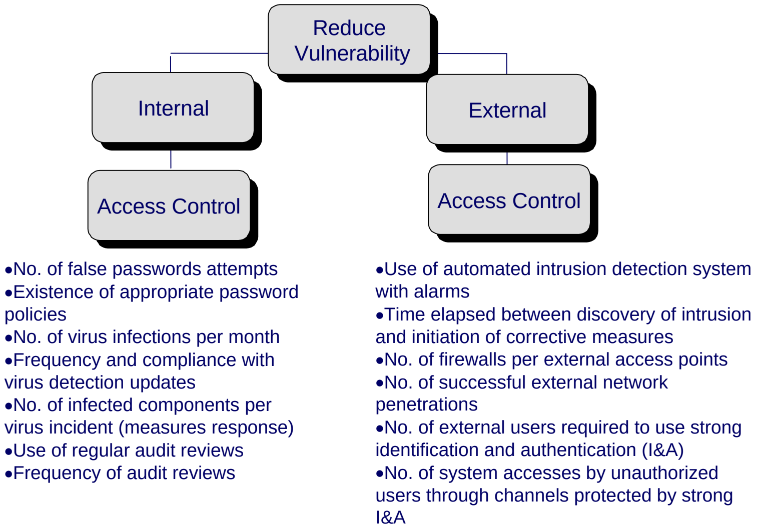


Figure 8. Top-Down Tree Diagram

Figure 9 illustrates how the tree diagram can be broken down into a set of example security and process metrics. (Detailed decompositions can be found in [3].) In the figure, the “use of automated intrusion detection system with alarms” and “use of regular audit reviews” are process metrics, whereas “time elapsed between discovery of intrusion and initiation of corrective measures” and “frequency of audit reviews” are security metrics.



- No. of false passwords attempts
- Existence of appropriate password policies
- No. of virus infections per month
- Frequency and compliance with virus detection updates
- No. of infected components per virus incident (measures response)
- Use of regular audit reviews
- Frequency of audit reviews

- Use of automated intrusion detection system with alarms
- Time elapsed between discovery of intrusion and initiation of corrective measures
- No. of firewalls per external access points
- No. of successful external network penetrations
- No. of external users required to use strong identification and authentication (I&A)
- No. of system accesses by unauthorized users through channels protected by strong I&A

Figure 9. Possible Metrics–Access Control

Using Metrics in the Real World

Many of the contributing organizations to the SSE-CMM Project have been applying the SSE-CMM to their own organizations as a self-assessment tool. This section describes not only one organization’s view of the application of the Risk Management PAs to its service offerings but also the role metrics have played, or will play, in that effort. This organization is a system security engineering service provider.

At the time of this paper, Booz·Allen & Hamilton was preparing for a self-assessment against Level 3 of the SSE-CMM Risk Management PAs. As shown in Figure 10, the SSE-CMM PAs, are separated into two groups: Risk Management and the remainder of System Security Engineering. Multiple links exist between the processes that belong to both areas. Booz·Allen began the self-assessment against the Risk Management PAs.

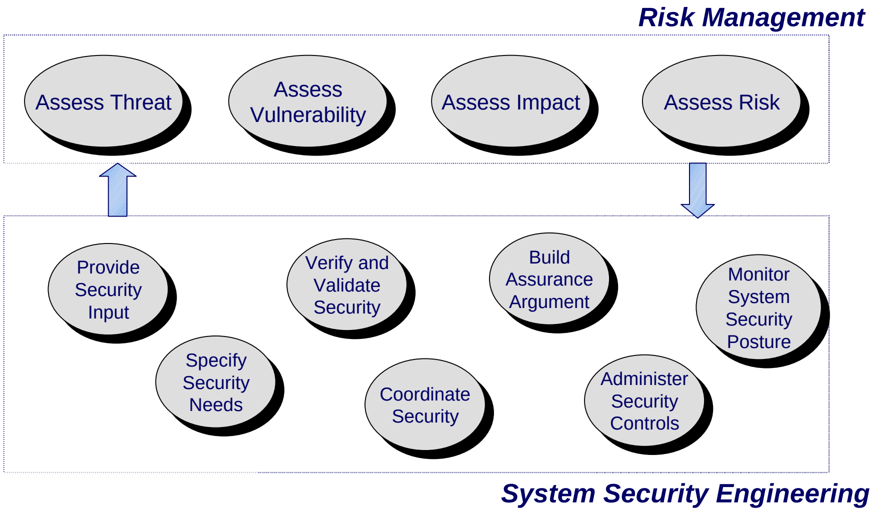


Figure 10. SSE-CMM Process Areas

SSE-CMM Level 3 requires that the following capabilities be met:

- Base practices are met
- Performance is planned
- Performance is disciplined
- Performance is verified
- Performance is tracked
- A standard process is defined
- A standard process is performed
- A standard process is coordinated.

Process metrics against these areas are straightforward. In the first analysis area, the capability metrics for GPs are basically yes/no binary measurements; the organization either does or does not meet the capability criteria. The status of the binary condition can be assessed through the course of the weeklong assessment on either a corporate basis, or a group or project basis. In setting up a security engineering program that meets the Level 3 maturity criteria in each of the Risk Management PAs, the above list of capabilities enabled Booz·Allen to determine how we will measure our success in the process performance against the GPs.

The next area of analysis was the specific BPs within each of the PAs. We performed further decomposition of the BPs by taking the BPs of each of the Risk Management PAs and determining how their existence within the Booz·Allen service offerings would be measured. Rather than repeat the BP descriptions for each of the PAs in this paper, we will focus on what we learned about the use of metrics for process measurement and security engineering output measurement.

The first step of our self-assessment was to identify the existing system risk management methodologies currently used within the company, compare them, determine if they were meaningfully different, develop a standard process, and require their use for all risk assessment efforts. Although the collected processes, tailored to different client groups, looked somewhat different on the surface and were documented in different formats, fundamentally they were very similar. The Booz·Allen risk management staff, working for different clients at different locations, used the same basic methodology as was collected for the self-assessment. It has been relatively straightforward for us to harmonize the various methods applied to DoD, Civil, Intelligence, and commercial customers and then arrive at a single, standardized process at a higher level.

After standardizing, documenting, and communicating the Booz·Allen Risk Management methodology in a single format, the self-assessment team assessed the methodology against the PAs. It appeared that a security engineering services provider should be able to measure success of its services the same way as the Business Process Reengineering (BPR) services providers do by determining the difference in performance before and after the services were performed. Therefore, just like the BPR organization claiming a processing time reduction of 150 percent, the system security engineering organization should be able to claim, for example, an 80-percent reduction in network intrusions as a result of implementation of their recommended countermeasures. However, that is not the case.

It quickly became evident that for a security engineering service provider it is significantly easier to conduct a meaningful self-assessment using process metrics (i.e., is our risk assessment process mature enough to achieve SSE-CMM Level 3?), than using security metrics (i.e., implementation of our risk assessment approach resulted in 50-percent reduction in intrusions for a specific client). The reason has more to do with the nature of measuring security effectiveness in networks than with whether a service provider has the “best” process.

The processes used by Booz·Allen include metrics, such as assigning high, medium, and low probabilities to various assessed parameters, or assigning monetary values to specific impacts, such as loss of information, corruption of information, or lack of availability of information or system resources. Examples of quantified gains from applying repetitive processes include security testing and evaluation (ST&E) of identical network components at different sites and a set of full risk assessments performed at several practically identical sites. In the first case, the cost of the initial effort was 8 times greater than the cost after the processes were established and applied. In the second case, the Phase 1 risk assessments took three people 5 days, whereas Phase 2 and 3 risk assessments took two people 2 to 3 days. The savings to the client were obvious.

Using SSE-CMM security metrics that measure the result of performing the security engineering processes is not as straightforward. Traditionally, when a security engineering service provider performs analyses in the risk management area, a common project is to perform a risk assessment and recommend countermeasures. Under this scenario, the security engineering service provider does not often implement the recommended countermeasures or get an opportunity to measure their effectiveness. On rare occasions, the specific security engineering service provider is allowed to establish a long-term relationship with a client organization. Such relationship might make it possible to conduct a measurement study that would quantify the benefits of implementing recommended security countermeasures. However, the security engineering service provider is usually left with no means of assessing success, other than qualitative measures, such as client satisfaction, use of best industry practices, and other similar measures.

An interesting paradox was discovered for applying of the SSE CMM to service providers. This issue of success measurement does not come up during the SSE-CMM assessment against Level 3 capabilities because this level does not require measuring the success or failure of system security in a customer's system as a result of applying specific security engineering processes. The primary measure of success determined by Level 3 is whether processes exist, are communicated, and are performed in a standard manner. Therefore, this level of self-assessment alone is not sufficient to determine the ultimate success or failure of the effectiveness of the provided security engineering services beyond the binary (yes/no) level. The issue of whether the applied processes are relevant to the problem to be solved is never considered because security effectiveness of these processes is not measured.

Booz·Allen believes that it is essential for security engineering service providers to begin finding ways and means of quantifying the benefits that they bring to their customer organizations. Although it is clearly of value to have and perform well defined, proven processes, their outcome must be measured, if at all possible. Without that, it is impossible to determine whether the processes will lead to better security in customer systems.

Conclusion

The SSE-CMM Project's Metrics Subcommittee began its work with the intuitive sense that the more mature the engineering process applied to a problem, the better the outcome. As a first step, implementing the BPs of the SSE-CMM and assessing ourselves against the model can determine if our processes are mature across the organization. Those subcommittee members who perform these processes as services to clients everyday believe that we owe it to our clients and our own organizations to go further in assessing the effectiveness of the services that we provide. Higher levels of maturity require measurements tied to the business goals of the organization and the needs of its clients.

The Metrics Subcommittee is in the beginning stages of its work. However, it is clearly apparent from the early development and application of these metrics that community and client participation in validating the metrics and the relationships between them is needed. The SSE-CMM Metrics Subcommittee is committed to being the catalyst for this community endeavor.

Acknowledgments

Partial funding, guidance, and support for the SSE-CMM Project have been provided by the National Security Agency (NSA) and Canadian Security Establishment (CSE). Many of the organizations participating in the SSE-CMM Project have also contributed their own time and funding to this work. The following list gratefully acknowledges the effort and support of those organizations participating in the SSE-CMM Project Metrics Action Committee: Arca Systems, Inc.; AverStar, Inc.; Booz, Allen & Hamilton; Defense Information Systems Agency (DISA); EDS; EWA-Canada; and G-J Consulting, Inc.

References

[1] Systems Security Engineering Capability Maturity Model Project*, Model Description, Version 2.0 Beta*, *October 1998.*

[2] Systems Security Engineering Capability Maturity Model Project*, Appraisal Method, Version 2.0 Draft, January 1999.*

[3] Systems Security Engineering Capability Maturity Model Project, *Security Metrics Action Committee Progress Report, Draft, February 1999.*

Using Security Metrics to Assess Risk Management Capabilities

Christina Kormos, National Security Agency

Lisa A. Gallagher, Arca Systems, Inc.

Natalie Givans, Booz-Allen & Hamilton, Inc.

Nadya Bartol, Booz-Allen & Hamilton, Inc.

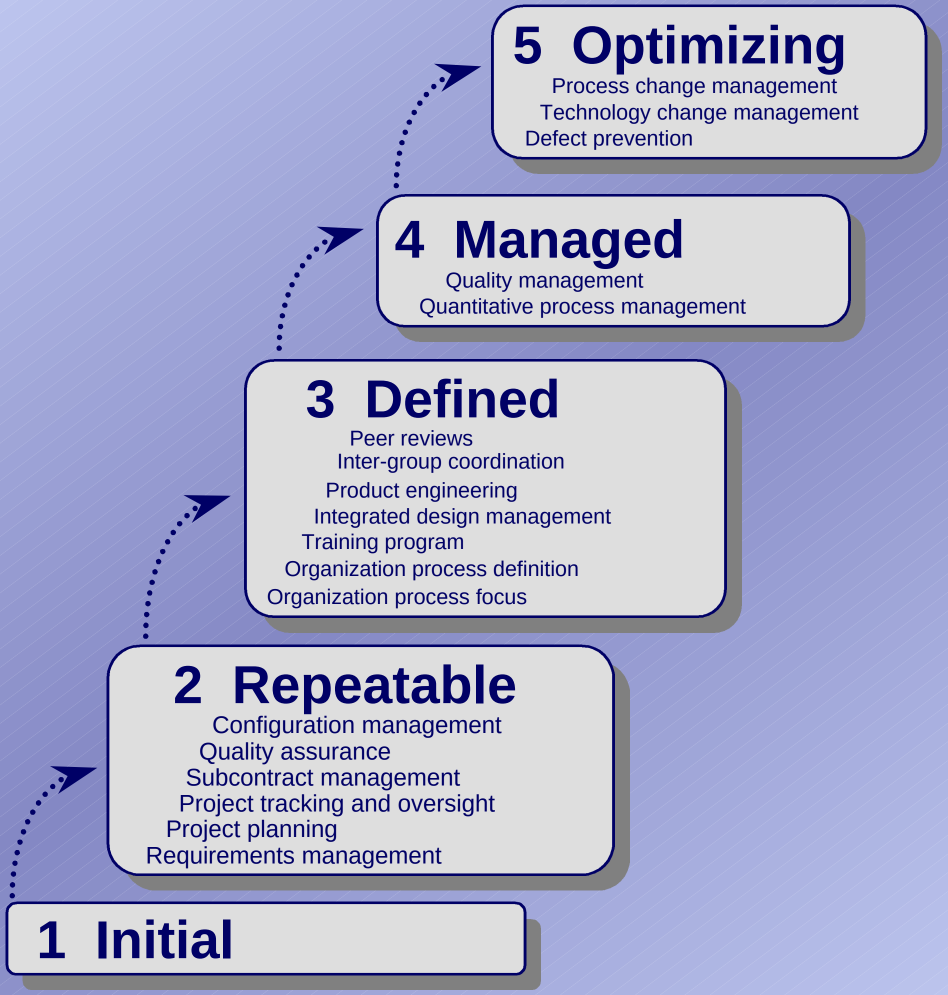
Presented by

Natalie Givans

Booz•Allen & Hamilton, Inc.

October 1999

Continuous Capability Maturity Model



5 Optimizing

Process change management
Technology change management
Defect prevention

4 Managed

Quality management
Quantitative process management

3 Defined

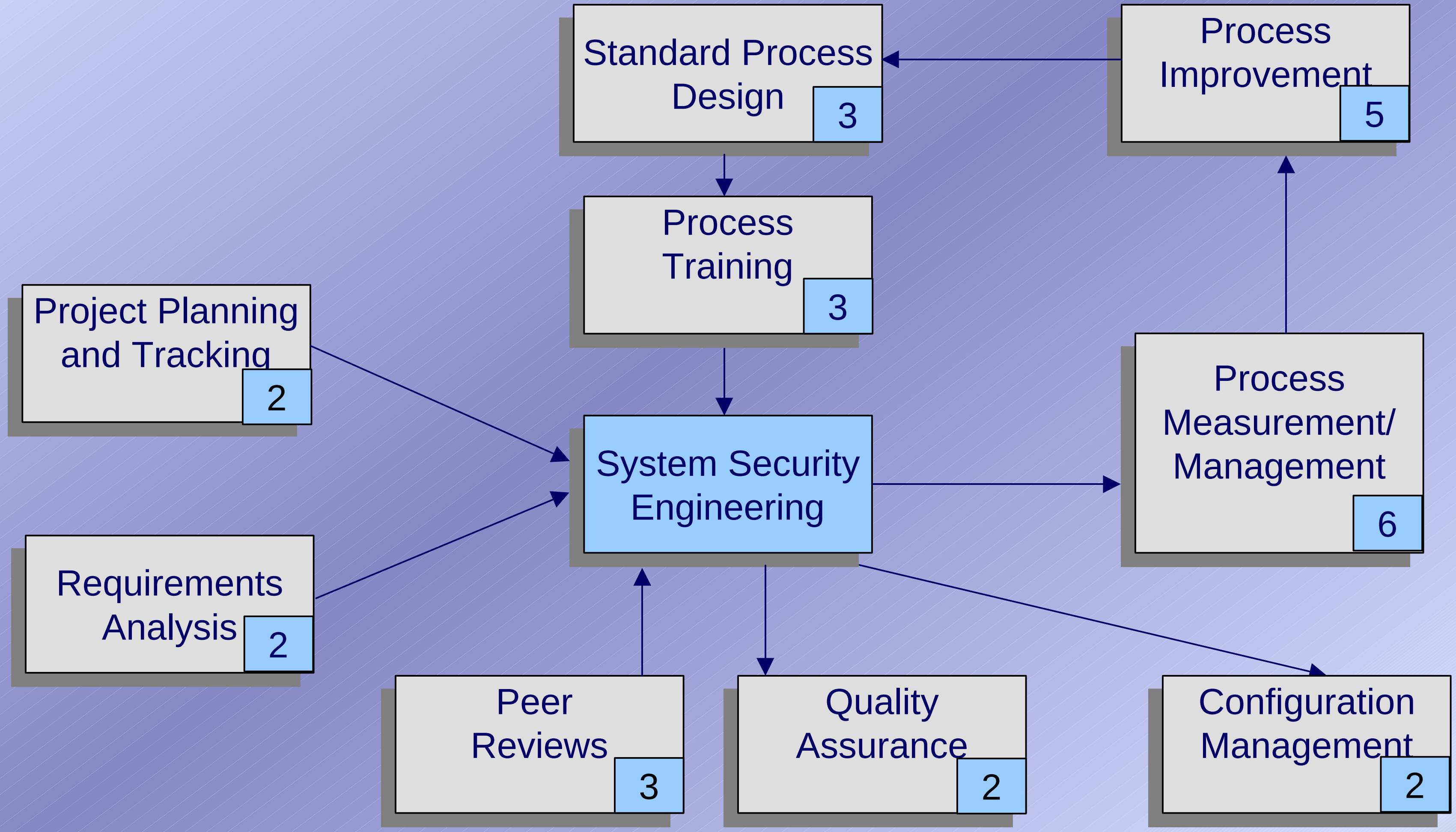
Peer reviews
Inter-group coordination
Product engineering
Integrated design management
Training program
Organization process definition
Organization process focus

2 Repeatable

Configuration management
Quality assurance
Subcontract management
Project tracking and oversight
Project planning
Requirements management

1 Initial

Relationship of Activities and Maturity Levels



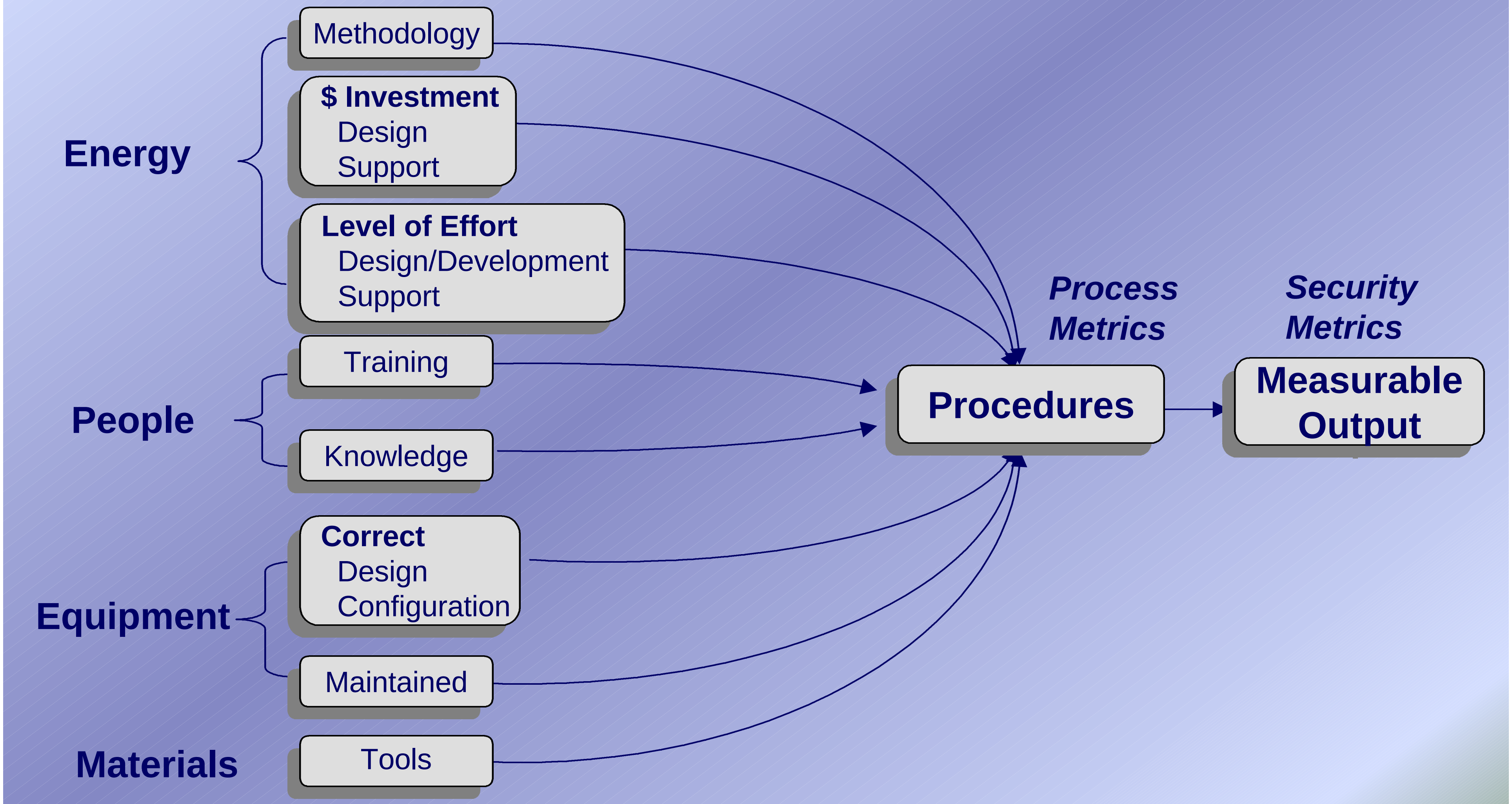
Metrics Overview

- A process is the logical organization of people, material, energy, equipment, and procedures into work activities designed to produce a specified end result
- Performance, stability, capability, and improvement and investment are central to effective process management
- SSE CMM uses two types of metrics: process metrics and security metrics

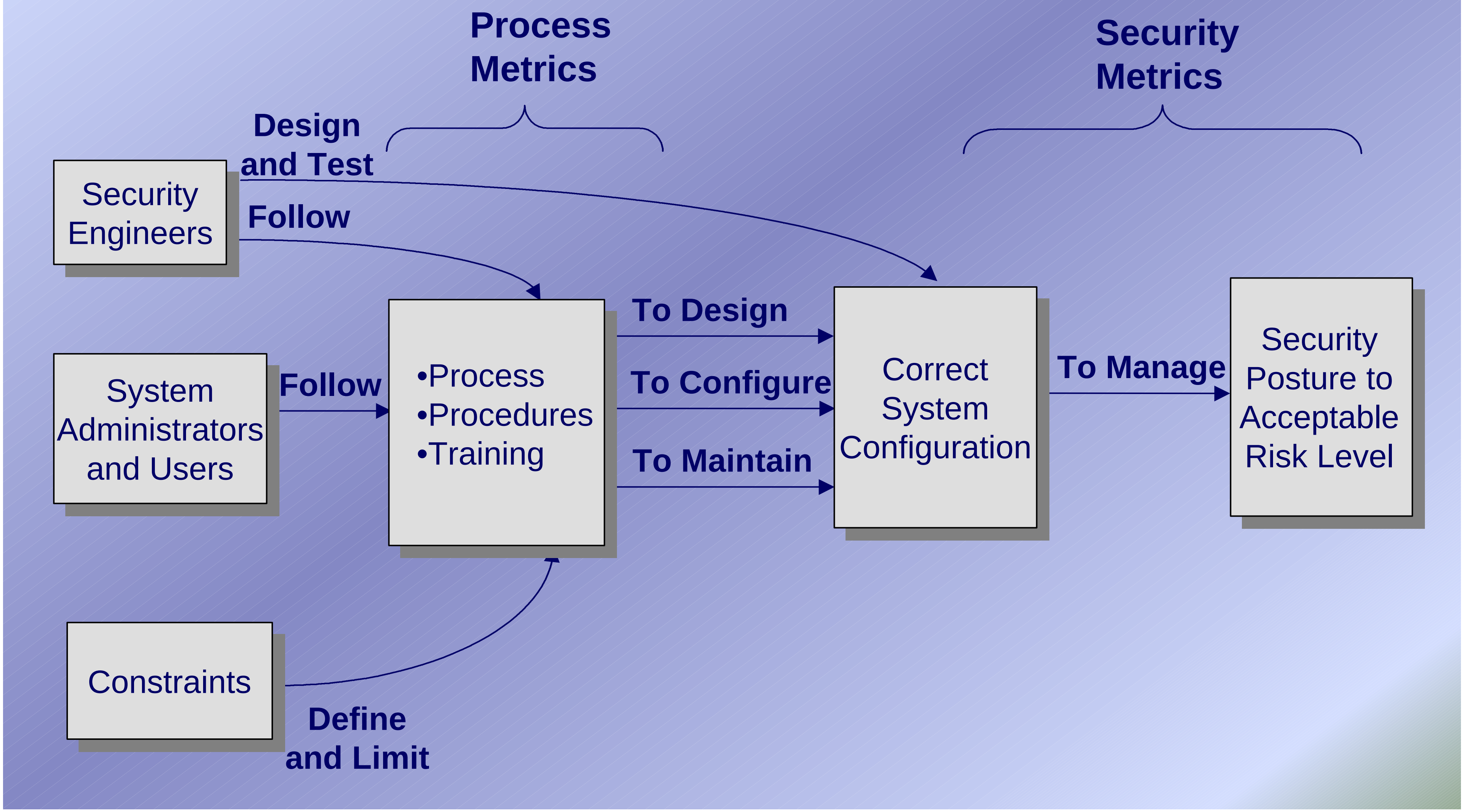
Metrics Users

- Project managers and leads—for operational or development environments or process improvement
- Chain of command and funding sources— to influence budgets, priorities, and allocation of resources
- Community at large—for awareness, competition, coordination, best practices
- Procurement (e.g., Department of Defense [DoD])—looking for services or products
- Hostile entities—as a deterrent to those who either might attack or who are in competition
- Product vendors—for assessing security product effectiveness based on engineering process improvement.

Metrics Development



Relationship between Security and Process Metrics



Process Metrics

Security Metrics

Security Engineers

Design and Test

Follow

System Administrators and Users

Follow

- Process
- Procedures
- Training

To Design

To Configure

To Maintain

Correct System Configuration

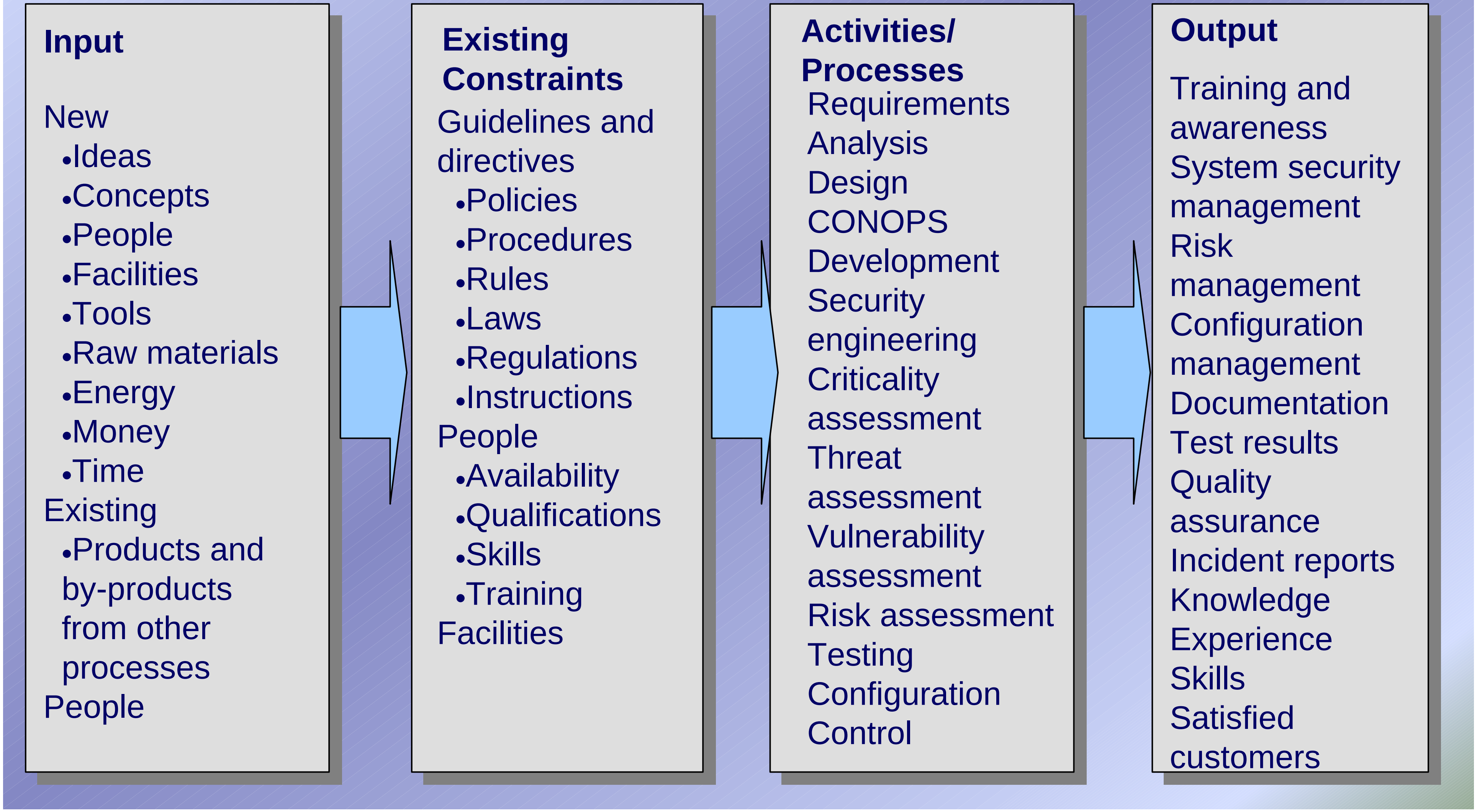
To Manage

Security Posture to Acceptable Risk Level

Constraints

Define and Limit

Process Metrics



Input

New

- Ideas
- Concepts
- People
- Facilities
- Tools
- Raw materials
- Energy
- Money
- Time

Existing

- Products and by-products from other processes

People

Existing Constraints

Guidelines and directives

- Policies
- Procedures
- Rules
- Laws
- Regulations
- Instructions

People

- Availability
- Qualifications
- Skills
- Training

Facilities

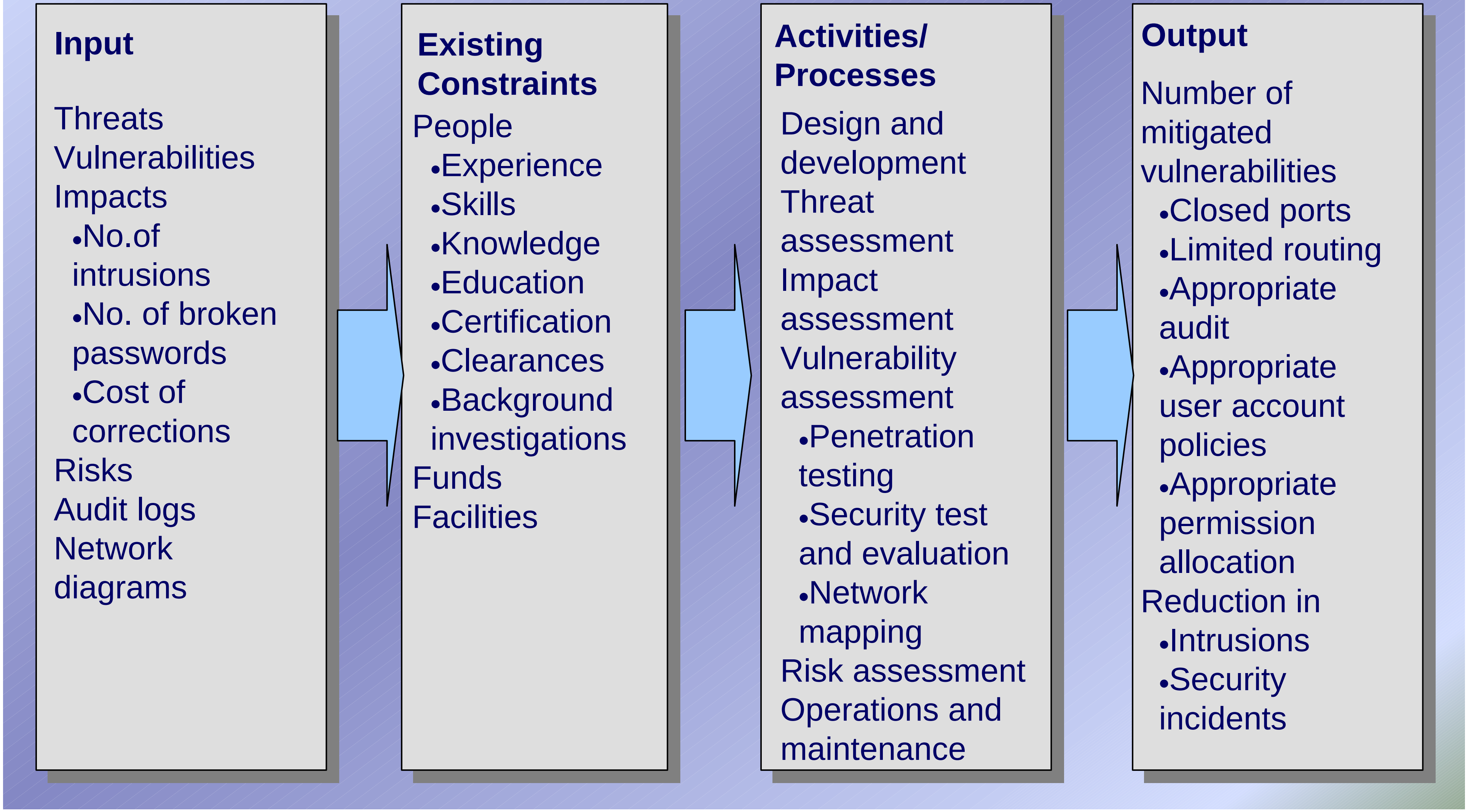
Activities/ Processes

Requirements Analysis
Design
CONOPS
Development
Security engineering
Criticality assessment
Threat assessment
Vulnerability assessment
Risk assessment
Testing
Configuration Control

Output

Training and awareness
System security management
Risk management
Configuration management
Documentation
Test results
Quality assurance
Incident reports
Knowledge
Experience
Skills
Satisfied customers

Security Metrics



Input

Threats
Vulnerabilities
Impacts
- No.of intrusions
- No. of broken passwords
- Cost of corrections

Risks
Audit logs
Network diagrams

Existing Constraints

People
- Experience
- Skills
- Knowledge
- Education
- Certification
- Clearances
- Background investigations

Funds
Facilities

Activities/ Processes

Design and development
Threat assessment
Impact assessment
Vulnerability assessment
- Penetration testing
- Security test and evaluation
- Network mapping

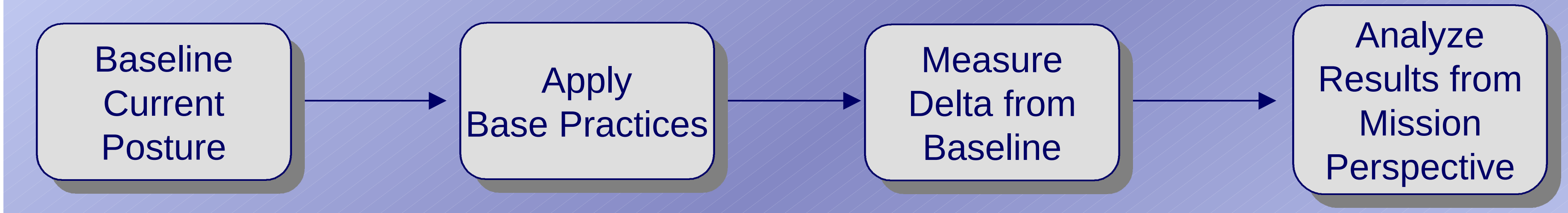
Risk assessment
Operations and maintenance

Output

Number of mitigated vulnerabilities
- Closed ports
- Limited routing
- Appropriate audit
- Appropriate user account policies
- Appropriate permission allocation

Reduction in
- Intrusions
- Security incidents

What is Measured



Baseline Current Posture

Apply Base Practices

Measure Delta from Baseline

Analyze Results from Mission Perspective

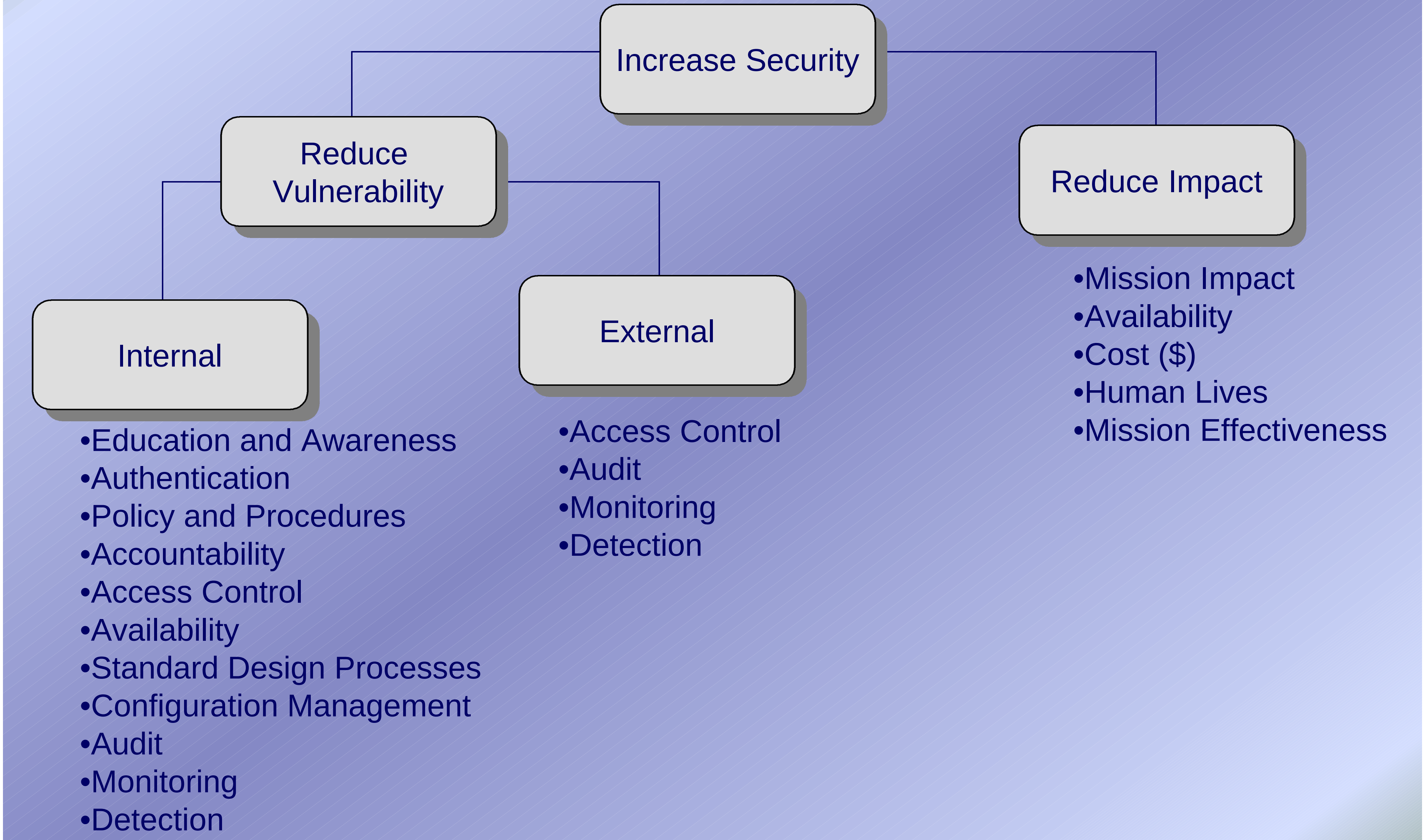
- Process Metrics
- Security Metrics

- Risk Management
- Security Engineering

- Process Metrics
- Security Metrics

- Cost-Benefit Analysis
- Return on investment

Top-Down Tree Diagram



Increase Security

Reduce Vulnerability

Internal

- Education and Awareness
- Authentication
- Policy and Procedures
- Accountability
- Access Control
- Availability
- Standard Design Processes
- Configuration Management
- Audit
- Monitoring
- Detection

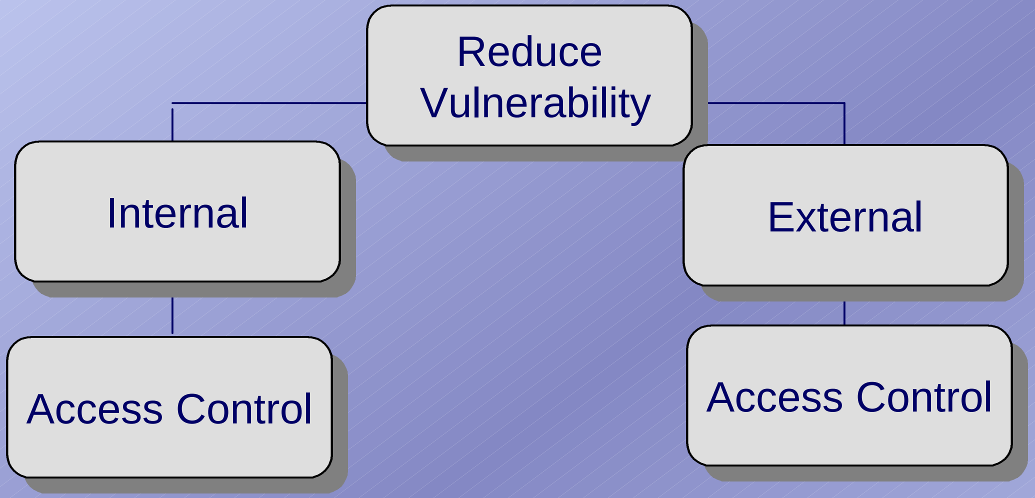
External

- Access Control
- Audit
- Monitoring
- Detection

Reduce Impact

- Mission Impact
- Availability
- Cost ($)
- Human Lives
- Mission Effectiveness

Possible Metrics



Reduce Vulnerability

Internal

Access Control

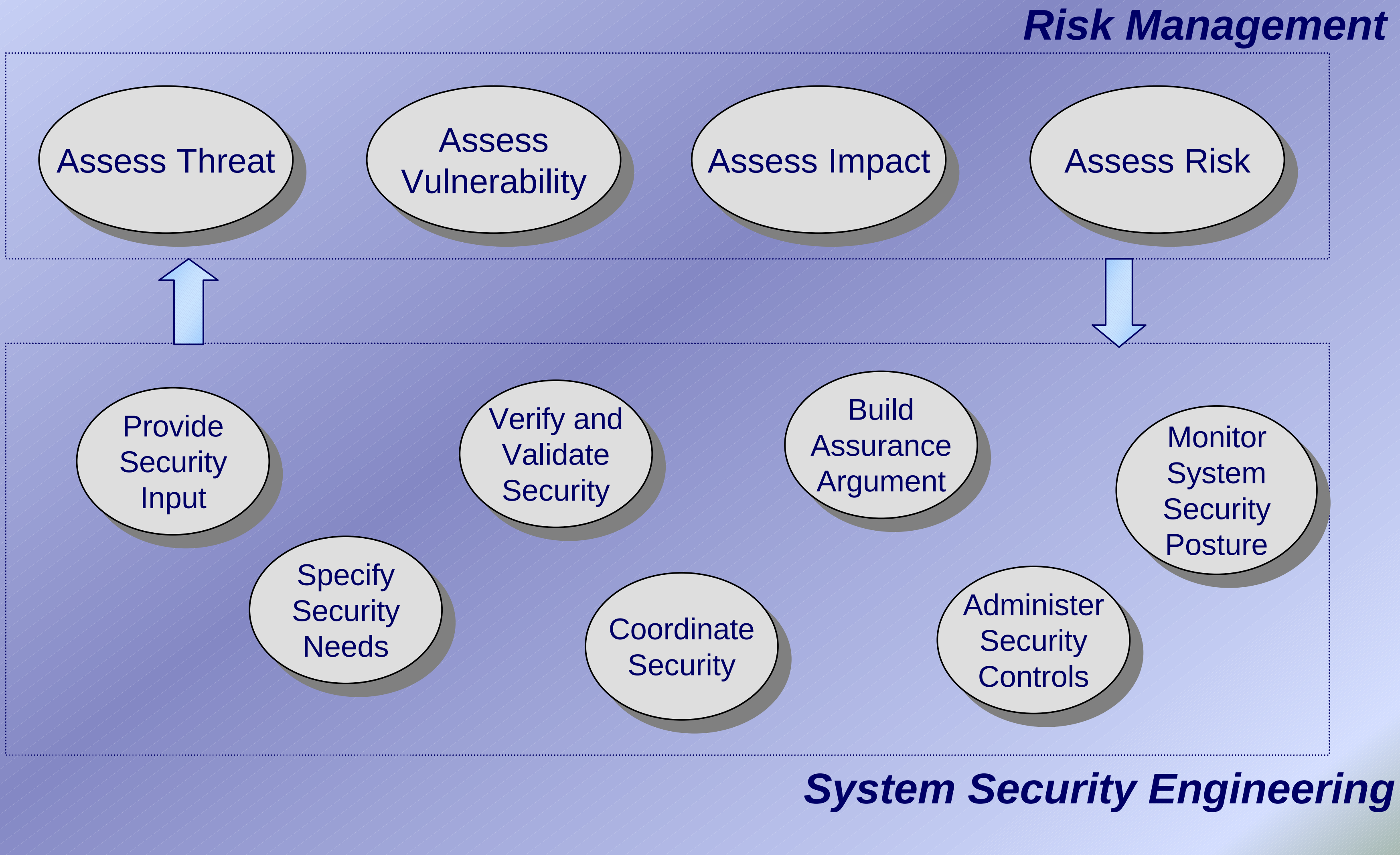
External

Access Control

- No. of false passwords attempts
- Existence of appropriate password policies
- No. of virus infections per month
- Frequency and compliance with virus detection updates
- No. of infected components per virus incident (measures response)
- Use of regular audit reviews
- Frequency of audit reviews

- Use of automated intrusion detection system with alarms
- Time elapsed between discovery of intrusion and initiation of corrective measures
- No. of firewalls per external access points
- No. of successful external network penetrations
- No. of external users required to use strong identification and authentication (I&A)
- No. of system accesses by unauthorized users through channels protected by strong I&A

System Security Engineering Process Areas



Specific Examples

- For security test and evaluation of identical network components at different sites the difference between the first effort and subsequent efforts was 8-fold. By repeating the processes and using the same generic documentation, we were able to assess and evaluate discovered vulnerabilities quickly and efficiently.
- For a phased risk assessment effort for a military client we were able to reduce the number of days spent on a site survey from 5 to 2-3, and the number of required people from 3 to 2.

Discoveries

- Measuring process effectiveness is easy
- Measuring security effectiveness is difficult
  - Unknown future attacks
  - Difficult to capture security posture after countermeasures have been applied
- Level 3 is insufficient because it does not address measuring process output

Conclusion

Higher levels of maturity require measurements tied to the business goals of the organization and the needs of its clients.

Acknowledgements

Partial funding, guidance, and support for the SSE-CMM Project have been provided by the National Security Agency (NSA) and Canadian Security Establishment (CSE). Many of the organizations participating in the SSE-CMM Project have also contributed their own time and funding to this work. The following list gratefully acknowledges the effort and support of those organizations participating in the SSE-CMM Project Metrics Action Committee: Arca Systems, Inc.; AverStar, Inc.; Booz, Allen & Hamilton; Defense Information Systems Agency (DISA); EDS; EWA-Canada; and G-J Consulting, Inc.

Authors

- **Christina Kormos, National Security Agency,** 410-854-6094(Ph), 410-854-4661(F), ckormos@radium.ncsc.mil
- **Lisa A. Gallagher (POC), Arca Systems, Inc.,** 410-309-1780 (Ph), 410-309-1781 (F), gallagher@arca.com
- **Natalie Givans, Booz-Allen & Hamilton, Inc.,** 703-289-5406 (Ph), 703-289-5825 (F), givans_natalie@bah.com
- **Nadya Bartol, Booz-Allen & Hamilton, Inc.,** 703-289-5379 (Ph), 703-289-5825 (F), bartol_nadya@bah.com