Security Measurement

White Paper

v2.0 12 July 2005

Prepared on behalf of the PSM Safety & Security TWG

Practical Software and Systems Measurement

Comments to:
John Murdoch
Department of Management Studies
University of York
YORK YO10 5DD UK

44 1904 43 4893
jm48@york.ac.uk

Table of Contents

List of Figures

List of Tables

Executive Summary

This paper reports on the security work that was done by the PSM Technical Working Group on Safety & Security Measurement from February 2004 to June 2005. The overall objective of the Security Measurement effort is to develop a process and set of measures to support management of future security assurance work. This paper follows the PSM process and first identifies security *Information Needs*. These information needs are developed through a review of prior security measurement efforts, and analysis of a *Security Concept Model* and *Measurable Entities Model*. The security information needs and Security Concept Model are then extrapolated to a set of *Measurable Concepts*. An outline of future efforts, development of *Security Measurement Constructs*, is also presented, but not derived, in this paper.

The development of quantitative methods in the management of security requires clear definitions of:

1. the assets to be protected and the damages that are to be avoided;
2. the system that contributes to the protection of the associated assets and that is the main subject of measurement;
3. the threat environment; the attackers, their goals and attack paths that are to be protected against;
4. the protective actions taken.

The proposed Security Concept Model identifies the following measurable aspects of security:

1. the resources deployed, in quantity and quality;
2. the compliance of current actions with plans, policies, standards and best practice models;
3. the monitoring of 'particular' security risks of the system in its threat environment and of the mitigation actions taken;
4. the performance as assessed by assurance techniques, for example, analysis, penetration testing, third-party independent testing;
5. the achieved security performance of a system in its operational environment as indicated, for example, by the prevention of or reductions in observed security-related events and losses.

A distinction is made between (1) the operation of a system to maintain security, for example information security in an organization, and (2) the engineering of security during the development of a security-critical system, for example the development of security-critical software and components. These cases differ in the scope of security actions available.

The Security Concept Model is applied to each of these cases. In the first case, measurement constructs are derived mainly from the operational security policy and the management of security risk through compliance. In the second case, measurement constructs are derived mainly from the system development lifecycle and the management of security risk through design and analysis.

PSM Safety & Security Measurement TWG

Workshop Contributors:

Dennis Ahern, *Northrop Grumman*

Frances Anderson, *Aerospace Corporation*

Matt Ashford, *SEI*

Paul Caseley, *DSTL UK MoD*

Vivian Cocca, *DoD*

Phil Flora, *Texas Guaranteed Student Loan Corp*

John Gaffney, *Lockheed Martin*

Joe Jarzombek, *National Cyber Security Division, DHS*

Cheryl Jones, PSM, *US Army ARDEC*

Greg Larsen, *Inst for Defence Analyses*

John Van Orden

Jim Moore, *Mitre Corporation*

John Murdoch, *University of York UK*

Dana Van Orman, *DCMA*

Don Reifer, *Reifer Consultants*

John Riedener, *US Army*

Rob Robason, *Wind River Systems*

Amos Rohrer, *BAE Systems*

Ioana Rus, *Fraunhofer USA, University of Maryland*

David Seaver, *PRICE Systems*

Dave Zubrow, *SEI*

Thanks also to the additional reviewers of this report, including:

Fred Hall

Ken Astley, *Loughborough University, UK*

Antony Powell, *University of York, UK*

1 Introduction

1.1 Security

Information, network, computer and software security are currently very active fields. A number of standards, recommendations, policies and practices have been developed by different communities to support the achievement of security properties in their respective domains. Although current development is rapid, measurement practices are less well established than in some other specialties. The sources used in this paper are listed in Appendix 1.

In this paper, security is taken to mean the degree of protection from attack and is a property of a system in relation to a threat environment. The term *system* is used in a very general sense: it might be a software module, computer, network or organization. In line with the main concerns of the PSM project, attention is directed mainly at the technical management of the development and operation of software-intensive systems. The definitions of terms used are given in Appendix 2.

It follows that a threat model, defining the form of attacks we are concerned about, is necessary for the concept of security to be operationally useful. The real threat environment is the operational environment of the system, and may never be known completely. However, threat models express our understanding of the threat environment and enable the development of countermeasures.

It is assumed that the target of attack is an asset associated with the system and which the system is responsible for protecting (possibly in collaboration with other systems). The required degree of protection is determined by the assets to be protected, the damage and recovery costs associated with successful attacks on them and the risk tolerance (aversion) of the parties involved. In many cases, the system will have some other primary purpose and security is a constraint that may have to be traded with other performances. In some types of system, security and safety properties are coupled; a security breach may compromise system safety.

Security is subject to the *weakest link* phenomenon; the security of a system can be compromised by single local failure event; therefore, security does not accumulate arithmetically in the manner of, for example, system mass or project costs.

Security has to be managed pro-actively; it therefore has to be treated mainly as a form of risk management, in which likely future performance has to be assessed on the basis of past and current performance. It is a time-evolving property, because it is determined in part by the evolving capabilities of attackers or potential attackers.

A wide variety of system products and services involve security-critical functions and are required to have security-related properties; also, security issues have to be managed at all aggregation levels, from networks and enterprises, network components, system architecture, computer and server platforms, to application software at code level and below. Security risks are mitigated by a wide variety of technological and organizational means.

Although applying measurement principles to security may seem daunting, there are strong reasons for developing security measurements:

1. security risk mitigations generate costs, including the opportunity costs associated with resources invested and costs associated with other system performances given up in the interests of security; we need to know what these costs are;
2. the benefits have to be argued in advance of investment and demonstrated in retrospect; measurement can provide valuable evidence to supplement qualitative assessments;
3. decisions have to be made about priorities; about which risks to address first and where security investments are likely to be most effective.

In summary, increased quantification in security management requires as clear as possible models of:

1. the system of concern;
2. the assets to be protected and their damage scenarios;
3. the threat (attack) agents of concern and their attack scenarios;
4. the risk mitigation actions/ countermeasures.

1.2 Developing PSM Measures

The PSM Project [1] is concerned with the design and implementation of measurements that meet the information needs of those responsible for managing work associated with software-intensive systems. Management tasks (and information needs) are divided into three levels in a layered management model: project management, capability (or resource) management and enterprise management. People acting in these roles typically carry responsibilities for resource allocation, planning, monitoring & control, capability development, performance management and risk management. PSM places emphasis on basing measures in technical practices, to provide as objective-as-possible indications of progress, performance etc. The specific practices of specialty work (including specialty-specific measures) are assumed as givens, as far as PSM is concerned.

PSM guidance materials capture the measurement experience of projects; types and descriptions of measures that have been found effective in the past are recorded and shared. Guidance materials comprise a measurement process model, measurement concepts and reference measurement specifications.

PSM and ISO 15939 [2] are based on the concept of *measurement constructs* (Figure 1) that link the information needs of managers with base measures of artifacts present in the managed domain. Measurement constructs embody understanding about the measured system and how measurements relate to management responsibilities. Such understanding covers:

1. *who* is involved in the domain; what are their roles, responsibilities, goals and values, leading to information needs? These questions are addressed by means of an **Information Needs Model**, based on the PSM layered management model;

2. *what* is the 'target' system, asset, service, or operation that is subject to management effort? What is it that has the security properties that are being engineered and maintained? What are the development and/or operational environment of this system? These questions are addressed by

developing a **Target System Model**. This is useful because there are significant differences between the kinds of systems of concern;

3. *what* are the security performances of concern? How is security performance manifested? How does pursuance of this property interact with the other performance attributes of an integrated system or service? These questions are addressed by means of a **Security Concept Model,** developed to be compatible with the safety concept model [3]. The objective is to provide a 'bridge' between security professionals and managers; the model provides a basis for decomposing information needs into measurable concepts in a top-down fashion;

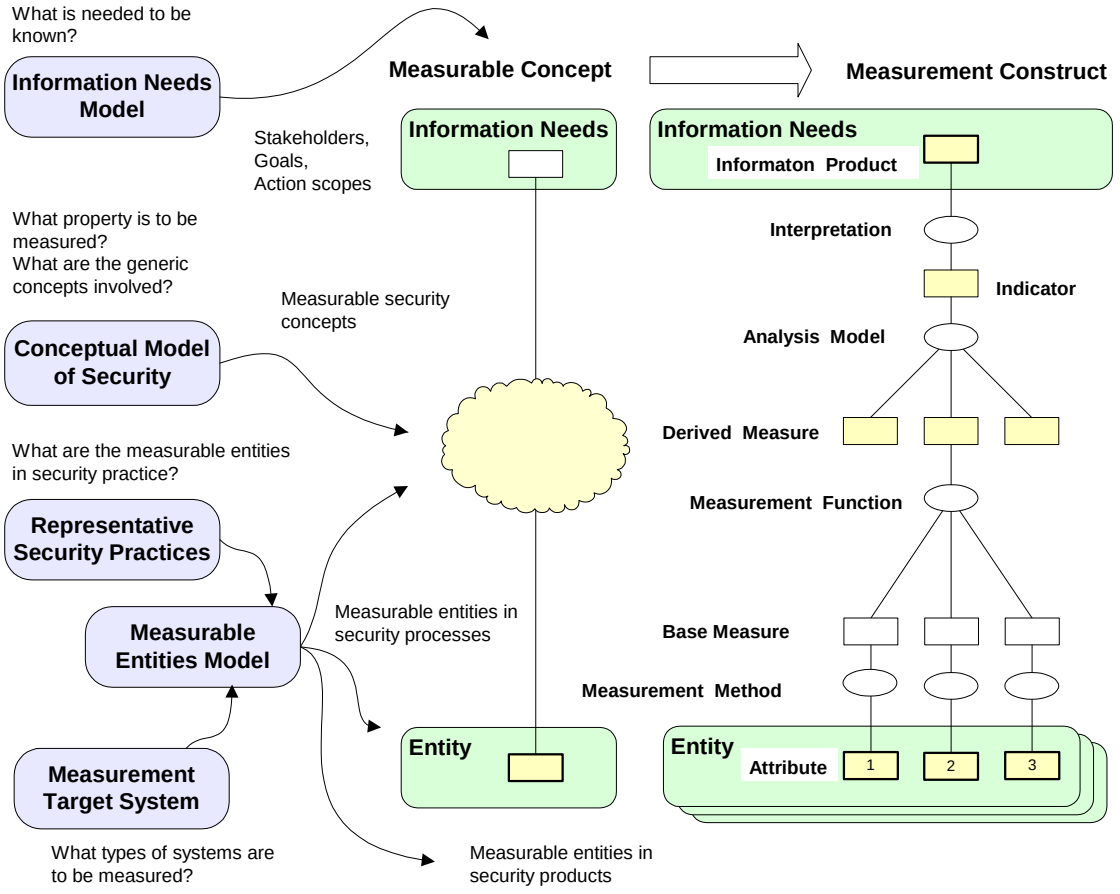


Figure 1 Illustration of the strategy used to develop security measures: top-down (based on information needs) and bottom-up (based on measurable artifacts)

4. *how* is the property achieved by the specialty engineering and operations communities? What practices and work products are involved? We address these questions by developing a **Representative Practices Model**, based on published best practice and standards in the specialty;

5. finally, a **Measurable Entities Model** is developed; work products associated with security engineering and operations management are identified and measurable attributes identified. This model provides a basis for synthesizing potential measures in a bottom-up fashion.

These five models enable the development of meaningful measurement constructs, useful in the management of security. The top-down and bottom-up analyses enable the synthesis of constructs that connect typical information needs with representative measurable artifacts Measurement constructs are augmented with measurement guidance about how to develop/ tailor measurement constructs in specific technology and organization situations. The following sections of this paper are organized around these models.

1.3 Contribution of PSM

The application of PSM principles to the security field gives the following benefits:

1. establishes common measurement principles across the diverse set of security 'sub-practices', technologies and sector-specific measurement sets;
2. integrates security measures with other (i.e. non-security) measures;
3. enables the development of indicators to inform organizational and enterprise-level management concerns; bridging technical specialty and management responsibilities.

Measurements are sought that are as simple as possible, but sufficiently detailed to enable efficient and effective management. The measurable concepts proposed in this paper have to be developed into measurement constructs and tested through practice. Involvement of the specialist communities is needed. Much of this work remains to be done; the status of the proposals made here is 'tentative'.

This work seeks to benefit technical, capability and enterprise-level managers in the following types of organization involved in security-critical systems and services:

1. system developers (at all levels of system aggregation);
2. system acquirers;
3. system operators;
4. standards and best practice/guidance model developers;
5. policy makers.

2 Information Needs Model

The PSM process addresses the development of indicators to meet the information needs arising in technical management processes. Figure 2 distinguishes between three contexts for security measurement:

1. general information security (*infosec*) required for all types of enterprise;
2. security engineering and project management capabilities required by *developers* of security-critical products;
3. security operations capability required by *users* of security-critical products (additional to general infosec).

A layered management model is used to distinguish between information needs arising in enterprises. Figure 3 shows the model used in [4], suitable for a general enterprise implementing an infosec policy. The following levels are identified:

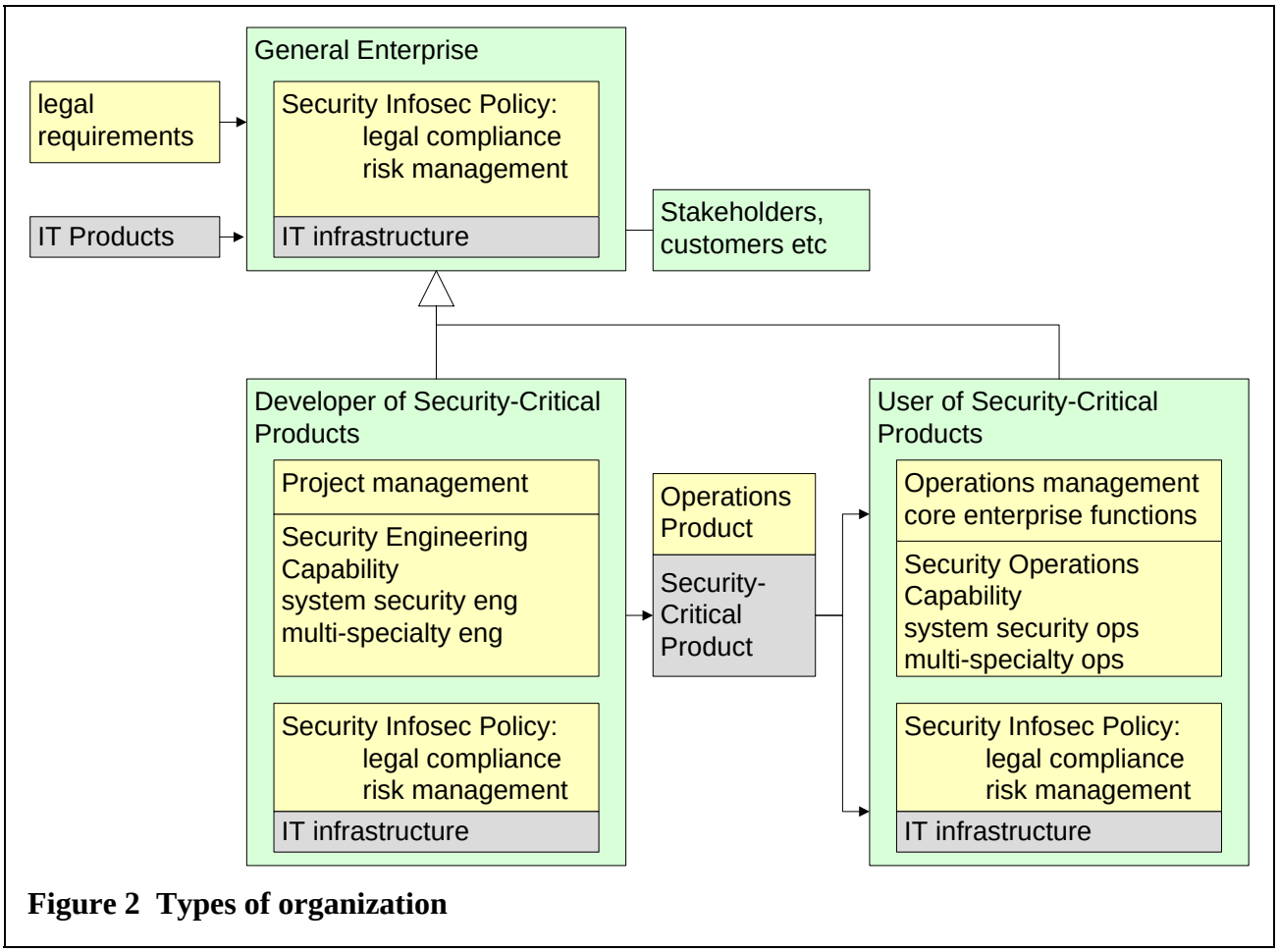


Figure 2 Types of organization

1. Enterprise management; i.e. Boards of Directors and Trustees;
2. Organization management;
3. Technical staff.

Figure 4 shows a similar model suitable for a product development organization. A project management layer has been added:

1. Enterprise management: development of the enterprise in its legal, market and financial environments; governance;
2. Organization management: development of the organization's capabilities; management of resources;
3. Project management: development of a single product or service;
4. Technical/ professional specialty work: core work involved in system development.

The allocation of roles and responsibilities varies between organizations, resulting in different groupings of information needs. However, the basic responsibilities of Figure 4 will be recognizable to most product development, project-orientated organizations.

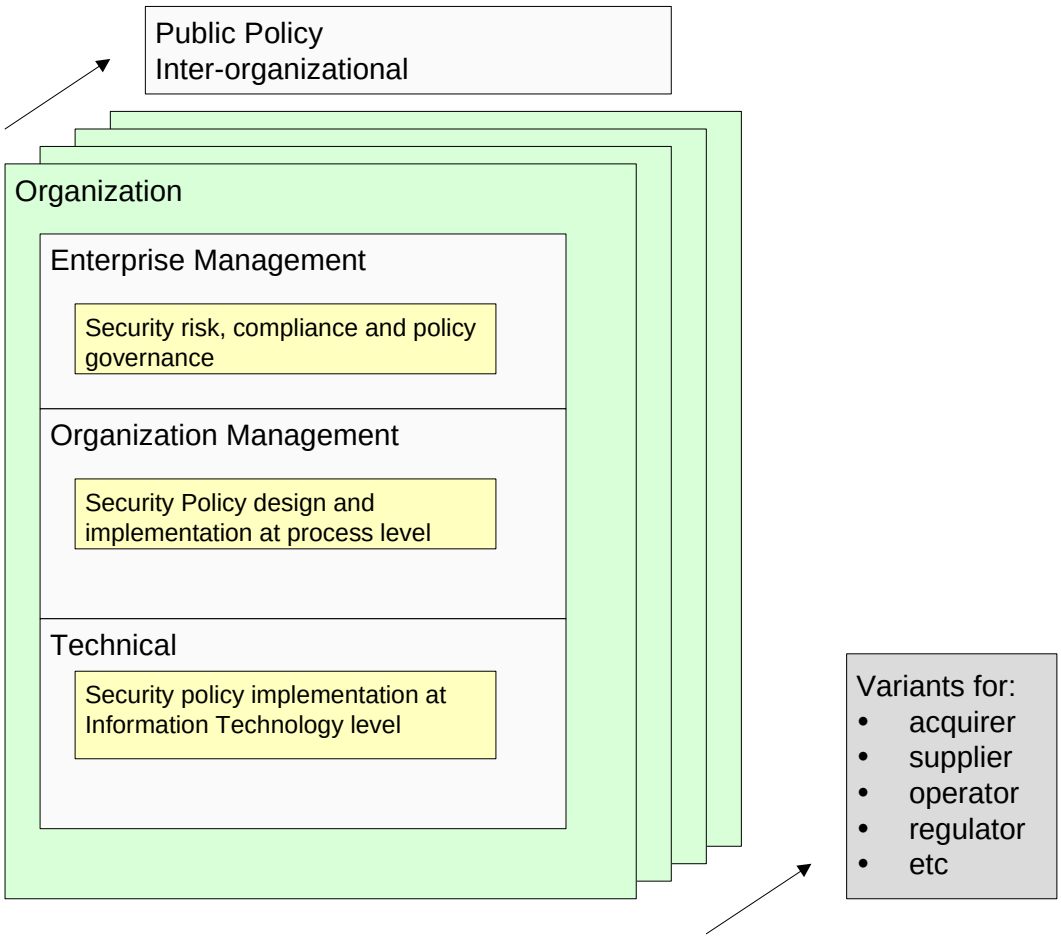


Figure 3 Information Needs Model: information security

Managers at all levels of organizations typically carry responsibility for:

1. ensuring legal and professional requirements are met;
2. judging the appropriate level of investment in security and where investment is most effectively deployed;
3. monitoring implementation;
4. validating improved performance outcomes.

The benefits arising from expenditure on security can be viewed as the *Return On Security Investment* (ROSI) [5], which relates the achieved integrated security performance to security costs incurred.

Risk management, in different forms, is present at all levels of management. The following types of risk mitigation strategy are involved in security:

1. compliance with policy, reflecting regulatory requirements, best practice models and standards;

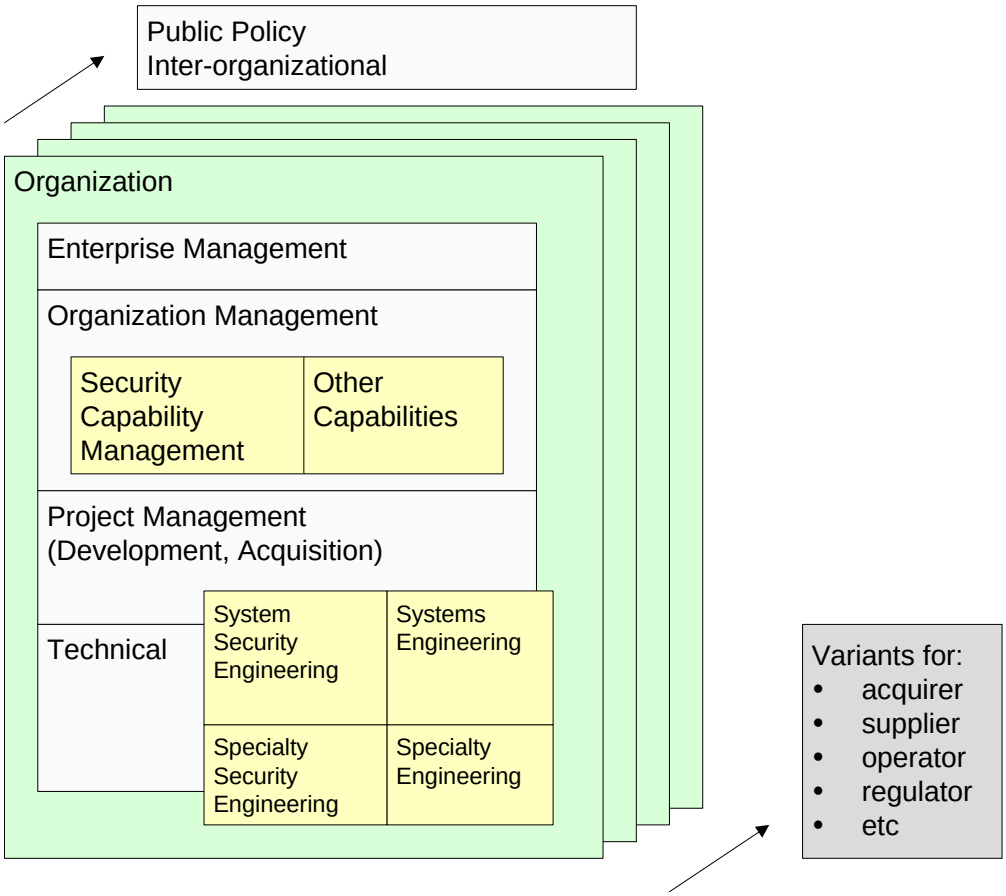


Figure 4 Information Needs Model: project organizations

2. investment in mitigations that lead to reductions in security-related losses; this appropriate where risk events are bearable but costly;
3. investment in mitigations that lead to evidence-based reductions in risk; this is appropriate where events are very costly and rare (c.f. safety risks); the ALARP principle (*As Low As Reasonably Practicable*) is invoked in the safety field to cover such risk acceptance decisions;
4. transfer of risk to partners or by insurance;
5. acceptance of risks; appropriate where events are rare and the losses acceptable.

An additional management layer *Public policy/inter-organizational management* has been included in Figures 3 and 4, in response to proposals [6] to support inter-working between user, acquirer and developer organizations. Figure 5 shows a model of the relationship between acquirer and supplier viewpoints, from [6].

More detailed information needs can be developed from role/responsibility models, matched to local organizational practices. For example, the following roles have been identified as being important in the software application security field [7]:

1. software architect;
2. developer/programmer;

3. tester;
4. manager of application development.

> Further Development
> Develop a role-based approach to developing information needs. Develop role templates that represent typical multi-role situations. Link information needs with the context and practices of roles, including type of work, worldview, process responsibilities etc. Link to DoDAF architecture aspects of roles.

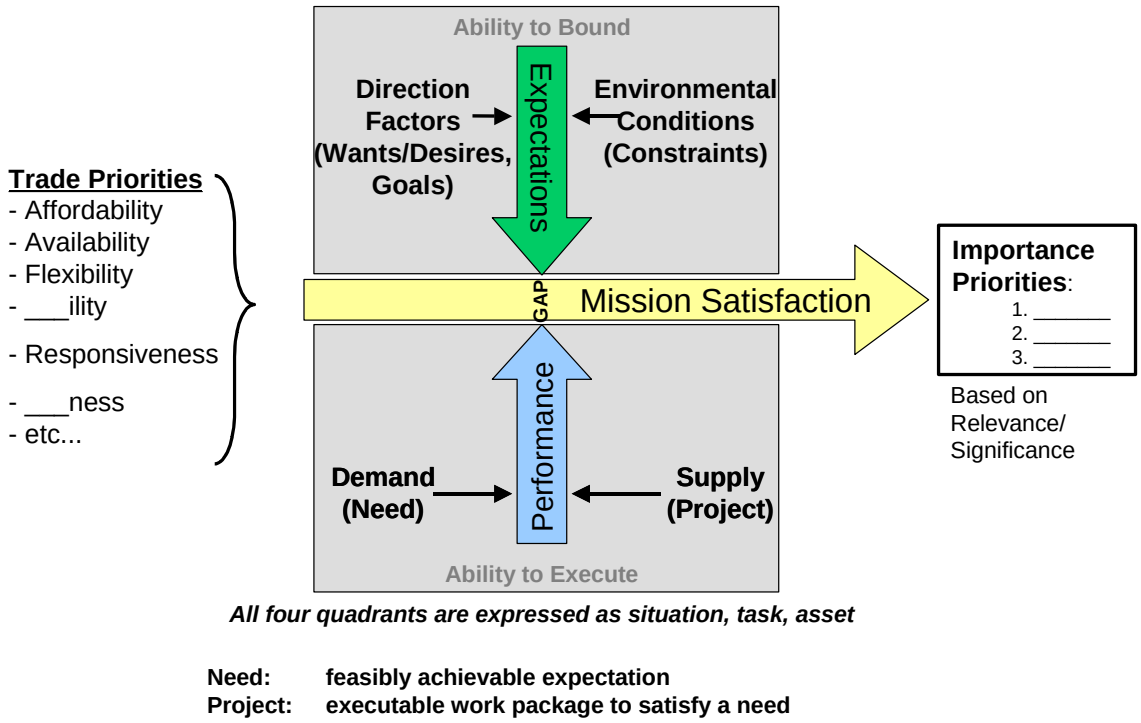


Figure 5 Inter-organizational (user/acquirer/supplier) concept, proposed by [6]

2.1 Enterprise and Board Levels

The CISWG study [4] identified the following responsibilities at Board/Trustee level for Information Security:

1. Oversee Risk Management and Compliance Programs Pertaining to Information Security (e.g. Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley);
2. Approve and Adopt Broad Information Security Program Principles and Approve Assignment of Key Managers Responsible for Information Security;
3. Strive to Protect the Interests of all Stakeholders Dependent on Information Security;
4. Review Information Security Policies Regarding Strategic Partners and Other Third-parties;
5. Strive to Ensure Business Continuity;
6. Review Provisions for Internal and External Audits of the Information Security Program;
7. Collaborate with Management to Specify the Information Security Metrics to be Reported to the Board.

The top-level metrics recommended under these headings are given in Appendix 5. Similar responsibilities would be expected for developer organizations, at this level, with the oversight of infosec policy being supplemented with that of security policy and practices associated with product development.

In addition to the above, senior executives will be concerned with the costs involved in meeting security objectives and the effectiveness of investments made:

1. for developers of secure products, integrated performance of security efforts and the ROSI, as evidenced in security properties of developed products and services for client organizations;
2. for general infosec, integrated performance and ROSI of security processes.

Traditional ROI calculations can be applied to security investments (Appendix 5). The inputs to ROI calculations are subject to considerable uncertainty in many cases. However, ROI captures a fundamental truth – we should judge the value of a particular security investment in terms of its assessed effectiveness in avoiding losses.

In uncertain situations in which we are concerned about evolving threats, decision-making based on simple ROI assessments may be unwise. Choosing not to invest in a security action may lock us out of learning about evolving threats. An alternative decision model may be to use 'real options' theory – which has been successfully applied to R&D management [8].

> Further Development
> Explore the *real options* approach to managing security risk, by analogy with R&D management. An investment in a security appliance many not be justifiable in NPV terms, but would be if an option is created that can be exercised (e.g. implement a defensive measure) at some time in the future.

2.2 Organization Level

The CISWG study [4] identifies the following responsibilities in the management of general information security:

1. Establish Information Security Management Policies and Controls and Monitor Compliance;
2. Assign Information Security Roles, Responsibilities, Required Skills, and Enforce Role-based Information Access Privileges;
3. Assess Information Risks, Establish Risk Thresholds and Actively Manage Risk Mitigation;
4. Ensure Implementation of Information Security Requirements for Strategic Partners and Other Third-parties;
5. Identify and Classify Information Assets;
6. Implement and Test Business Continuity Plans;
7. Approve Information Systems Architecture during Acquisition, Development, Operations, and Maintenance;
8. Protect the Physical Environment;
9. Ensure Internal and External Audits of the Information Security Program with Timely Follow-up;
10. Collaborate with Security Staff to Specify the Information Security Metrics to be Reported to Management.

Various information needs are implied by these responsibilities. Some 39 metrics are recommended under these headings in [4], mainly monitoring compliance with the security policy (Appendix 5 includes some examples).

Organizations that develop security-critical products have additional responsibilities associated with the security engineering capability required for development purposes. Two kinds of responsibility are involved:

1. the development of security engineering capability, as required by development projects;
2. the management of those resources across projects.

The following information needs arise:

1. the current security capability/ competence of the resources available to be deployed on projects;
2. level of compliance with applicable standards and best practice models;
3. costs and efficiency of security engineering capability;
4. effectiveness and ROI of security engineering capability, as evidenced in performance of product development projects;
5. effectiveness and ROI of security engineering capability, as evidenced in performance of delivered products and services;
6. estimation of resource, cost and schedule needs of new projects;
7. monitoring of project progress and evolving security resource needs.

The safety and security extensions [9] to the iCMM and CMMI models provide a reference set of 16 practices (Appendix 5). Information needs arise in terms of establishing continuous improvement in these processes. A distinction is drawn in this paper between (a) the measurement of cost, performance and risk in a vertically integrated way (through the organizational hierarchy/ responsibility chain) and (b) the measurement of end-to-end process performance in a horizontally integrated way (the process view). Both views are important. The first is directed more at assessing the effectiveness of security investments and risk management (with less attention on how the work is structured); the second more towards assessing the efficiency of end-to-end security processes (to support process improvement). 'Vertical' measurement of performance and risk does not itself require work areas to be structured as processes, but is compatible with a process approach. However work is organized, it seems important to ground measurement as much as possible in the technical/ operational practice level i.e. at the level where risks are detected and where inventiveness and creativity are deployed in their mitigation. This orientation may help to tailor/anchor best practice models based on process maturity to specific project and operational situations [10].

The estimation of likely future costs of security is being addressed by the parametric cost modeling community [11]. Much of this paper is about the complementary issue of assessment of future security performance.

2.3 Project Level

The management of a project to develop a security-critical product gives rise to a set of information needs that are focused on the progress of development of the particular product. This is the main concern of the PSM / ISO 15939 measurement approach.

Typical information needs include:

1. Tracking security requirements and compliance;
2. Tracking identified security risks (identified threats and vulnerabilities);
3. Progress and costs of mitigation actions, against plans and risk tracking; keyed with product development life-cycle;
4. Tracking integrated security performance, balancing investment between identified risks;
5. Supporting trades between security and other system performances;
6. Assessing integrated past performance of security activity;
7. Tracking security assurance activities, progress, costs;
8. Assessing compliance with applicable standards and use of best practice knowledge;
9. Assessing readiness/ awareness (readiness to respond to events not foreseen in plans and risk assessments).

The measurable concepts proposed in Section 7 include the counting of tracked threats and vulnerabilities and the mitigation actions adopted.

2.4 Technical/Professional Specialty Level

The CISWG study [4] lists the following elements of an information security program, at technical level:

1. User Identification and Authentication
2. User Account Management
3. User Privileges
4. Configuration Management
5. Event and Activity Logging and Monitoring
6. Communications, Email, and Remote Access Security
7. Malicious Code Protection
8. Software Change Management, including Patching
9. Firewalls
10. Data Encryption
11. Backup and Recovery
12. Incident and Vulnerability Detection and Response
13. Collaborate with Management to Specify the Technical Metrics to be Reported to Management

These responsibilities are mainly concerned with the appropriate exploitation of technical features existing in commercially available IT systems and COTS components. The security policy is implemented as a set of decisions on how to deploy these security controls (e.g. automatic logging off of users after a selected idle time.) The recommended metrics generally reflect this orientation. This approach can be characterized as the decomposition of the security policy into sets of organizational procedures and actions on the IT infrastructure of the organization.

In the case of product development organizations, the scope of technical specialization involved will depend on the product type and technologies involved. The concept of *system security engineering*, included in Figure 4, may be useful [12]. By analogy with *system safety engineering*, system security addresses the integrated security of aggregated systems comprising different technologies. It also provides a platform for trade-offs that span different security threats, vulnerabilities and safety issues. Both are supportive of the more general *systems engineering* effort, that carries responsibility for trade-offs with other system qualities and functions.

The concern of this work is the development of software-intensive systems; the following specialist fields are involved, among others:

1. Network security;
2. Computer security;
3. Specialist security components and technologies;
4. Software security;
5. Associated hardware security (e.g. tamper-proofing).

These specialties have their own practices and are deployed on projects so as to integrate with the product development life cycle.

Information needs at technical development levels are mainly concerned with assessing the performance of designed, implemented and deployed products. Measurement is conducted with reference to requirements and specifications and in the context of a system development life-cycle. Product measurement blends into the quality assurance field (e.g. [13] for software) at this level.

It is not possible, in the general case, to drive security engineering exclusively from requirements. Instead, a dual approach is needed, typical of engineering:

1. Requirements-driven – assessment of security requirements, decomposition and application to the system structure;
2. Design-driven – identification of the scope of the secure assets and deployment of appropriate development/operation practices. Appropriateness is developed within specialist practices and embodied in standards.

The proposed measurement of security work balances these aspects i.e. (a) tracking responses to particular requirements, threats, vulnerabilities and events and (b) monitoring compliance with generally-recognised security engineering and operations practices.

The functions and components of security-critical systems are typically subjected to various inspections and tests, to provide security assurance. The Common Criteria approach [14] has evolved in the IS domain, in which internationally recognized assurance criteria have been agreed for common security functional components and systems. Standardization enables the development of a market in security-assessed products. Whether or not standardized testing is applied, the assurance techniques available provide a measurement approach, based on objective testing and assessment of security components and functions. Testing of prototype units by way of experimentation is included in this type.

Practices particular to the security field are sketched in Section 6 and Appendix 5.

2.5 Public Policy, Inter-Organizational Level

An information security strategy developed for legal compliance and operational risk management purposes does not necessarily address longer-term improvements within the industry. The model of Figure 5 [6] has been proposed to help close the gap between the desires and expectations of users and the security performance deliverable by suppliers using current technologies. Information needs arising in this concept will involve the development of actionable security requirements from user expressions of need, threat modeling and assessment of achievable security performances.

> Further Development
> Define information needs arising from the inter-organizational model, supporting negotiation between acquirer and supplier organizations and the development of actionable requirements.

2.6 Time-Orientation View

Underlying most information needs is a *decision situation* in which a desired future state is sought and a choice has to be made based on assessed past performance and current opportunities and constraints. All these assessments are subject to uncertainty, giving rise to:

1. information needs about the past, recent or distant - past performance assessment (achieved performance, customer satisfaction); aggregated assurance:

    2.1. How secure has the system been?
    2.2. What is the progress (and cost) of security assurance?
    2.3. How efficient/effective have the security processes been, as enacted?
    2.4. What was the achieved performance compared with policy/objectives?
    2.5. What was the achieved performance in customer (other stakeholder) terms?

2. information needs about the present - current performance management (monitoring, control, progress assessment; design and operations decisions, response, recovery):

    2.1. How secure is the system?
    2.2. What is the current performance of the system/ organization, compared with the security objectives?
    2.3 What are the achieved performance outcomes of the actions taken?
    2.4 What resources are actually being deployed?
    2.5 To what degree are policies, standards etc being complied with?
    2.6 What is the progress / status of security work?

3. information needs about the future - estimating and planning (costs, resources, schedule, processes, organization, performance); risk assessment; awareness, readiness:

    3.1 How secure will the system be (or what are the residual security risks), for different sources of risk?
    3.2 How much is it worth spending to reduce security risks?
    3.3 What are the most cost-effective actions to reduce security risks?
    3.4 What are the opportunity costs of chosen actions and of security expenditure?

3.5 How ready is the developer/operator organization to undertake security-critical work?
3.6 How will the threat environment evolve in the future?
3.7 What resources should be committed to the security work (money, time, capability)? And over what timescales (current project, medium term development)?

4. information needs about constraints - compliance (standards, regulatory certification, best practice, legal).

4.1 Are 'best practices' being followed (are our practices taking account of industry-known risks)?
4.2 Are we meeting legal obligations?

The following table gives examples of information needs along this dimension, and at the levels of the layered model of Figure 4.

2.7 Plan, Risk, Awareness View

A feature of security is that many of the threats of concern are *learning* agents, resulting in a greater emphasis on real time maintenance of security properties, as compared with pre-analysis and designed-in protection. Security engineering shares many of these characteristics but has the additional feature of a 'battle of learning curves', implying a more dynamic, through-life approach. Three kinds of *readiness* can be identified

1. Conventional planning (project development or operational plan) in which tasks are designed, resources deployed and progress monitored against plans (the 'knowns');
2. Risk management, in which possible unwanted scenarios are identified and provisions and contingencies set aside to cope with them (the 'known unknowns');
3. Awareness/readiness, in which resources are deployed to cope with unforeseen events (the 'unknown unknowns').

The best mix of these approaches depends on the flexibility available and the levels of uncertainty and risk involved. An example of an awareness approach is CISCO's monitoring of unusual patterns of network use [15].

3 Security Concept Model

This section develops a Security Concept Model - a model of the security domain that supports the identification of measurable concepts. The Concept Model captures the essential aspects of measuring security and is adaptable to all security management situations. General measurable concepts are implied. Development of measurement constructs will then follow from an application of this model to particular situations.

The following concepts are implied by the definitions of Appendix 2:

1. A *system* that is providing some useful function or service in an operational environment;
2. A set of *assets*, abstract or concrete resources associated with the system, that are to be protected from misuse;
3. A threat agent or attacker in the operational environment, seeking to exploit the assets;
4. A desirable property, quality or state of the *system* in relation to the *threat environment*, called *security*, associated with protection from attack;

	Information Needs about:			
	Achieved Past Performance	**Current Performance**	**Likely Future Performance**	**Compliance**
Enterprise/ Public Accountability	Costs of security, Delivered security performance Effects on profitability & productivity Opportunity costs ROSI Learning curves	Current security performance Current Enterprise risk Public risk exposure Current expenditure Current resource allocations	Enterprise risk Public (externalized) risk Threat environment	Legal Policy Governance
Organization	Delivered security performance Effectiveness and efficiency of security processes, security management system, policy Actual costs Achieved Process maturity	Current security capability Maturity Benchmarking Current investment in development – product and process Current outcomes Responsiveness, flexibility, awareness Competence	Future process risk Predicted security performance & risk Future threats	Compliance Legal Best practice State-of-the-art
Project/ Operations	Actual delivered security effectiveness of integrated product or service Assurance Integrated efficiency and effectiveness at project/ operations level	Progress of security work against plan Progress of risk mitigations Progress of contingency actions Costs Outcomes of tasks in terms of risk and performance Event response	Estimation and costs of security development and operation Project Risk Planning	Regulatory Awareness Adherence to policy
Technical	Integrated costs of security work Integrated effectiveness and efficiency at technical level Achieved security performance Security-related damages Assurance	Current residual security risks Progress of risk mitigations Current performance – response, recovery Current costs Relative merit of different risk mitigation options	Predicted technical security risks Estimates Planning Required security performance Anticipation	Regulatory Interface Best practices

Table 1 Typical information needs of managers of security-related work

5. A set of defined occurrences and costly consequences, associated with a successful attack on the assets;
6. the concept of a *security risk* arising from a combination of the presence of an attacker, an attack goal, a vulnerability in the system and the damage costs caused by a successful attack.

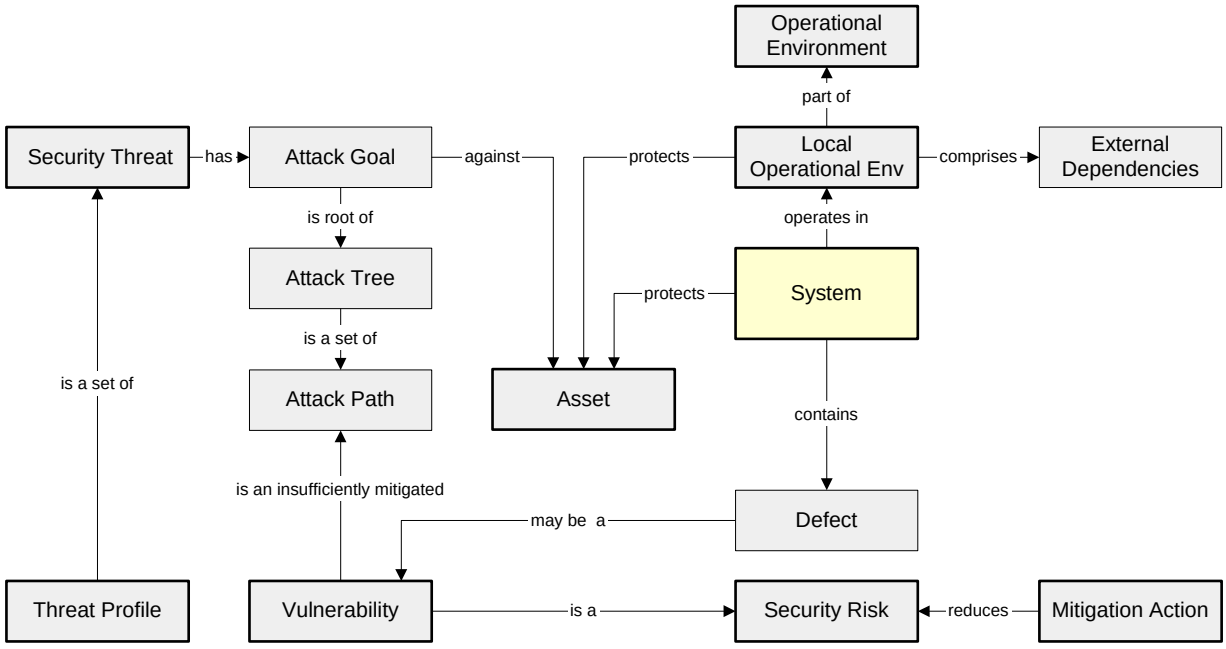


Figure 6 Information model representing security concepts

It is assumed that. the *system* has the responsibility of maintaining an acceptable level of *security*, within the *threat environment,* with the possible assistance of *external dependencies*.

The following concepts are used in the following discussion and are based on a *systems approach* to security (Figures 6 and 7 illustrate some of these):

1. an *environment* with which the system interacts and over which it has no direct control;
2. a *local environment* that lies outside the functional boundary of the system (and therefore is not under its direct control) but which contains external dependencies, i.e. other systems on which the system depends to achieve security;
3. a *boundary*, or *perimeter*, that separates the system from its environment;
4. intended *users* of the system, benefiting from the core functions or services provided by it;
5. *threat agents*, *attackers* or adversaries;
6. *ports* (points of *entry* and *exit*) that are required for the system to deliver its services and functions, but which may be used by attackers;

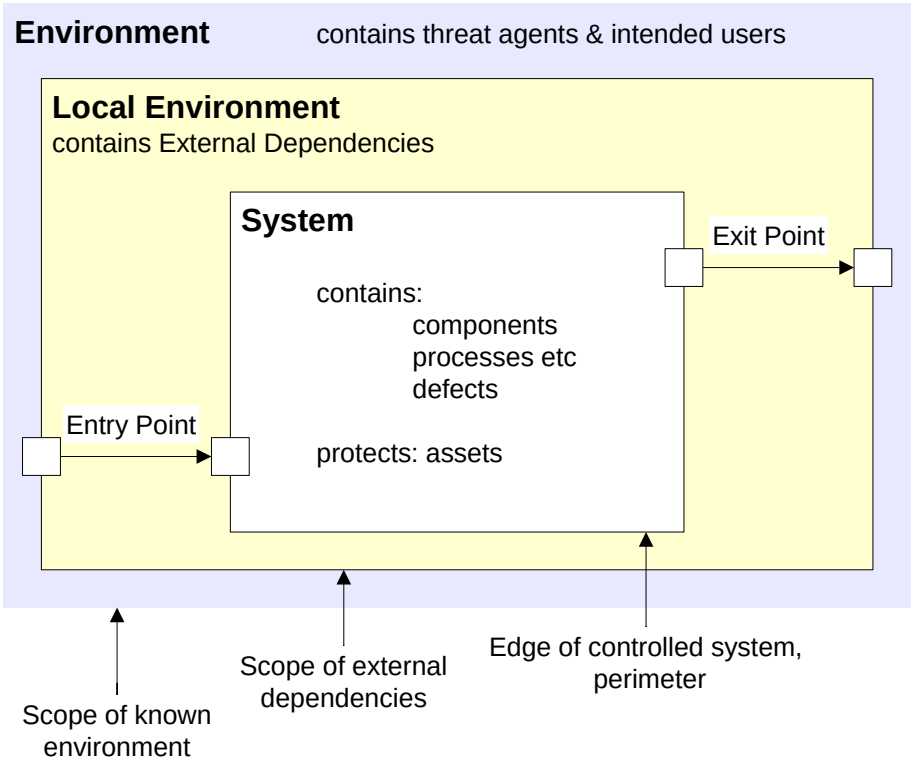


Figure 7 A security-critical system and its environment

7. *threats*; viewed as the goals of attackers and their potential means of attack on the system;
8. top-level goals are decomposed into sub-goals in AND/OR relationships in the form of *attack trees*; an attack tree comprises a set of *attack paths*, that link system vulnerabilities to an attack goal;
9. *defects* in the system that may or may not be security-related;
10. *vulnerabilities*, *security flaws* or *weaknesses* in a system that may allow a threat to eventuate;
11. *security events*, viewed as actual security-related occurrences arising from combinations of threats and vulnerabilities;
12. an *operator* of the system, striving to maintain a secure state (for systems with human components).

Further information models illustrating these concepts are included in Appendix 3.

The form of security engineering involved in a particular application will vary, depending largely on the type of system and asset involved:

1. type of technology and scale; software or hardware component, subsystem, networked information system, organization;.

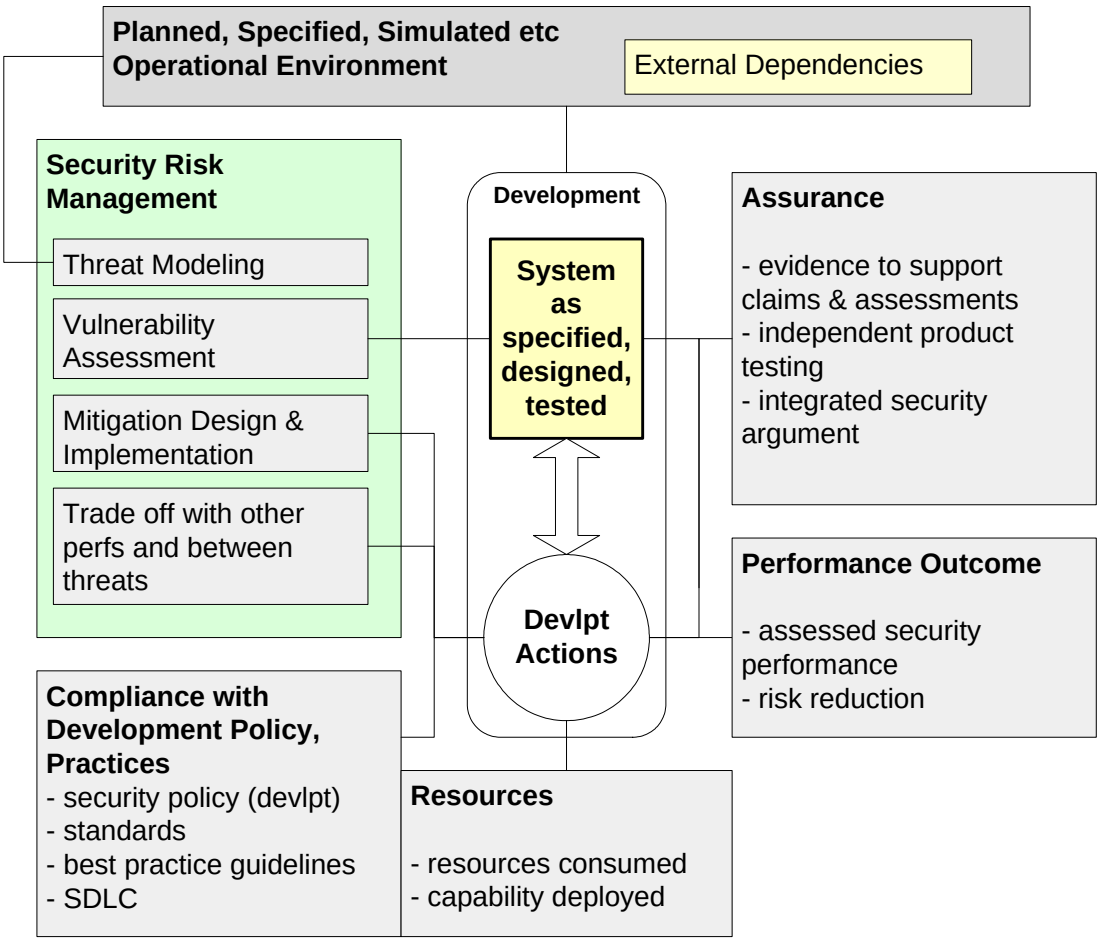


Figure 8 Security Concept Model - system development

2. developmental status (under development, designed, implemented, deployed, operated, maintained);
3. primary function; to provide other (non-security) functionality or services, but with security as an additional requirement/ constraint; or to provide security functionality only (i.e. would not be required if security was of no concern).

The target system will be determined by the responsibilities of those whose information needs are being served. The Target System Model is discussed further in Section 4.

Security is also defined in terms of the work involved (Appendix 2), expressing *how* the property of security is achieved in a system. A wide range of different kinds of security action exist, depending on the type of system and environments involved. The term *security action* is used in this paper to cover all kinds of security work. Typically, security will be achieved by security specialists working collaboratively with others, e.g. engineers, managers and operators. Security actions are allocated to security specialists (e.g. development of encryption components) as well as other specialists and professionals (e.g. software engineers).

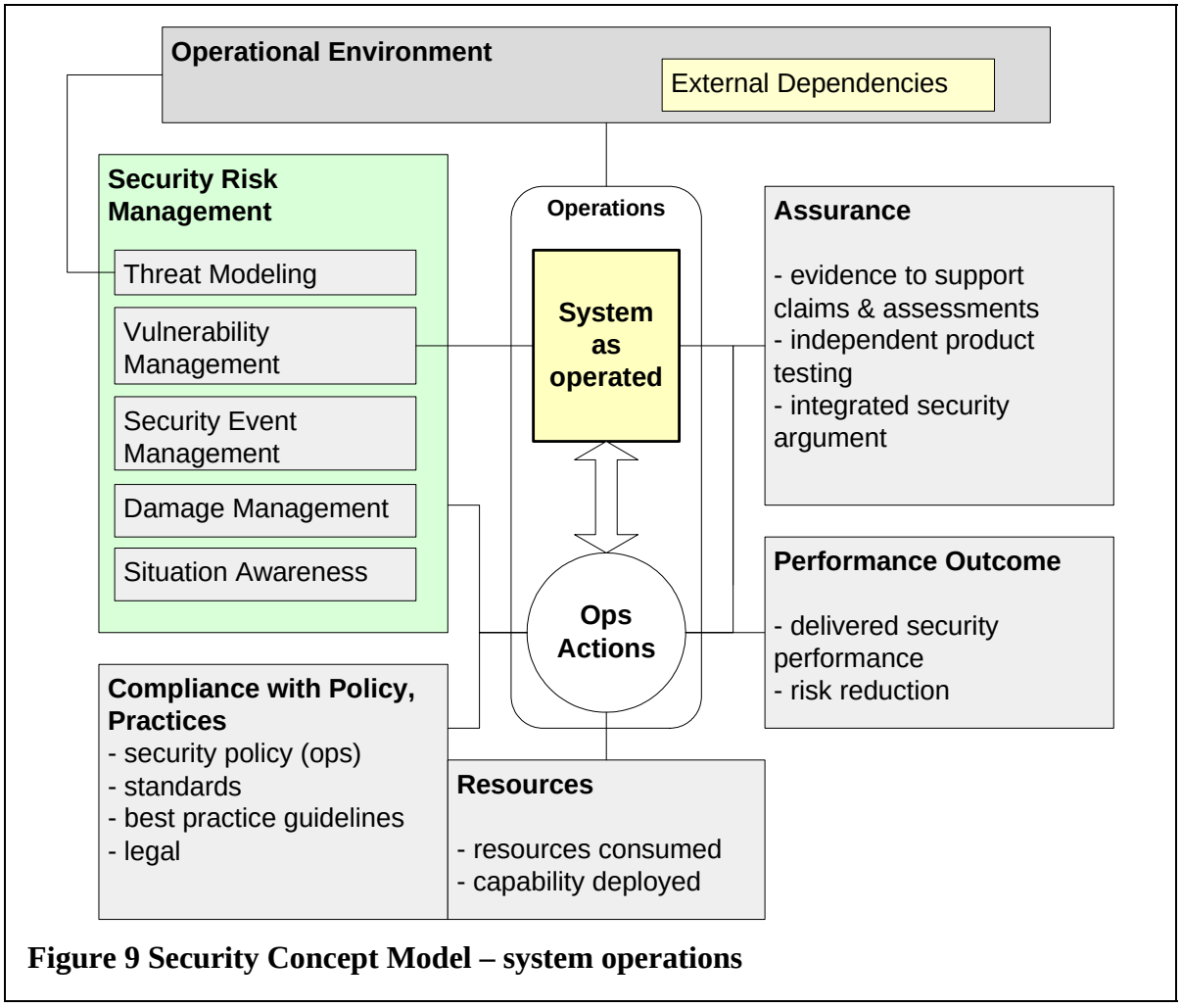


Figure 9 Security Concept Model – system operations

Security is achieved in a system by a variety of means. The following are the fundamental strategies:

1. consideration of security properties throughout the system development lifecycle, influencing requirements specification, design at architecture and component levels, implementation, deployment and operation;
2. design and deployment of security-specific functional components (encryption, access control, firewalls etc.);
3. security-specific testing and assurance;
4. compliance with security policies and implied operational functions (monitoring, event response etc);
5. improvements in general security engineering and operational capabilities and management of resources.

The first of these strives to apply security engineering to all phases of a system's development lifecycle and to reduce vulnerabilities introduced by shortfalls in basic system development processes. The second strategy strives to exploit technology-based concepts to provide protection. The third strategy strives to strengthen testing and assurance practices to focus on security properties of the system. The fourth strategy seeks to improve the organizational

aspects of security, and the fifth to improve the capability and resources available to organizations that carry security-related responsibilities.

Security engineering at tactical and detailed levels depends on the type of system and assets involved. However, this general description enables an approach to be developed to security measurement.

Due to the uncertainties involved in security engineering and operation, a risk-based approach is generally used to manage the prioritization of security requirements and the deployment of resources.

These considerations are brought together in the Security Concept Models of Figures 8 and 9, applicable to development and operational contexts, respectively.

At the centre of Figure 8 is a representation of security actions applied to a product system during a development phase of the system lifecycle. Measurements may be of properties of the product system (e.g. number of vulnerabilities identified by a scanner) and/or of the activities involved (e.g. level of compliance with a defined procedure or check list). The product and activity measures are closely inter-related. Five classes of measurement are identified in Figures 8 and 9:

1. security risk management;
2. assurance;

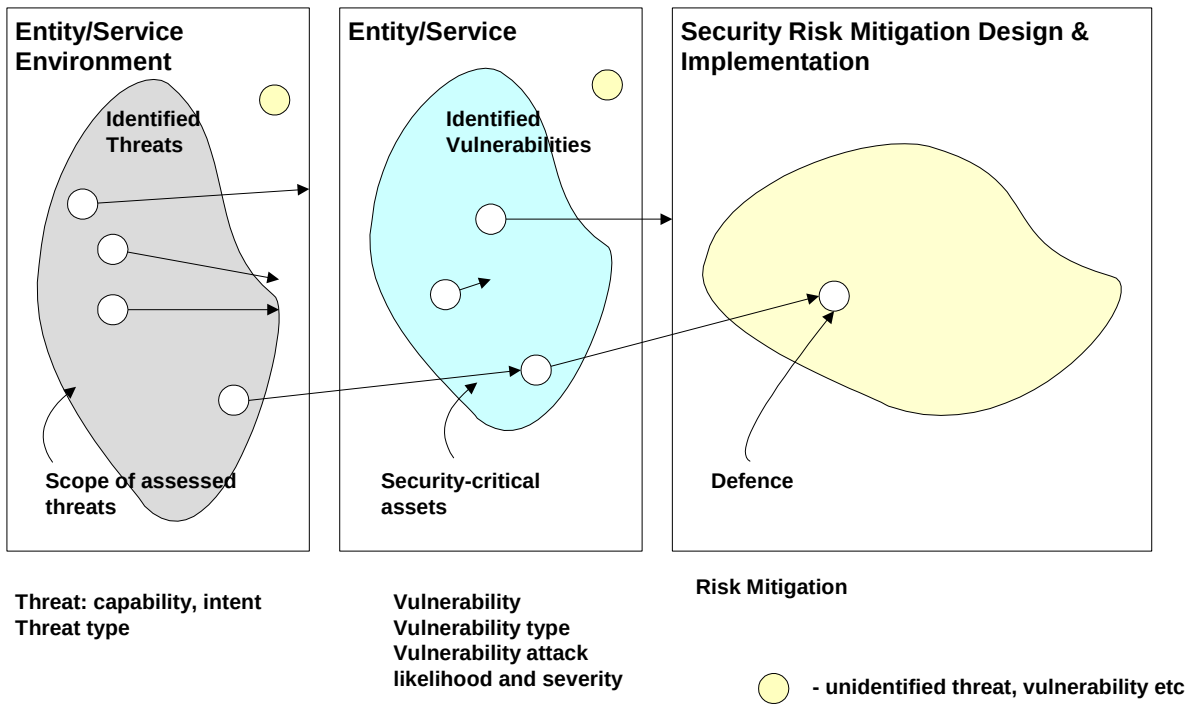


Figure 10 Three inter-dependent strategies to manage security risk (development)

3. compliance with policy, standards, guidelines;
4. security resource management and capability development;
5. delivered security performance of the system in operation.

The last of these is a vital concern because it represents the end benefit arising from all security actions. Security risk management during operation is extended to include operational mitigations (security event response and damage management).

Security engineering practice is based on threat modeling. During development, possible threat agents, their objectives and likely attack paths are assessed. The potential vulnerabilities in the system design and implementation are also assessed. The system is designed to resist the identified attack paths by means of various types of mitigation. During operations, each of the aspects of threats, vulnerabilities, events and damages can be viewed as distinguishable but inter-dependent *managed domains*.

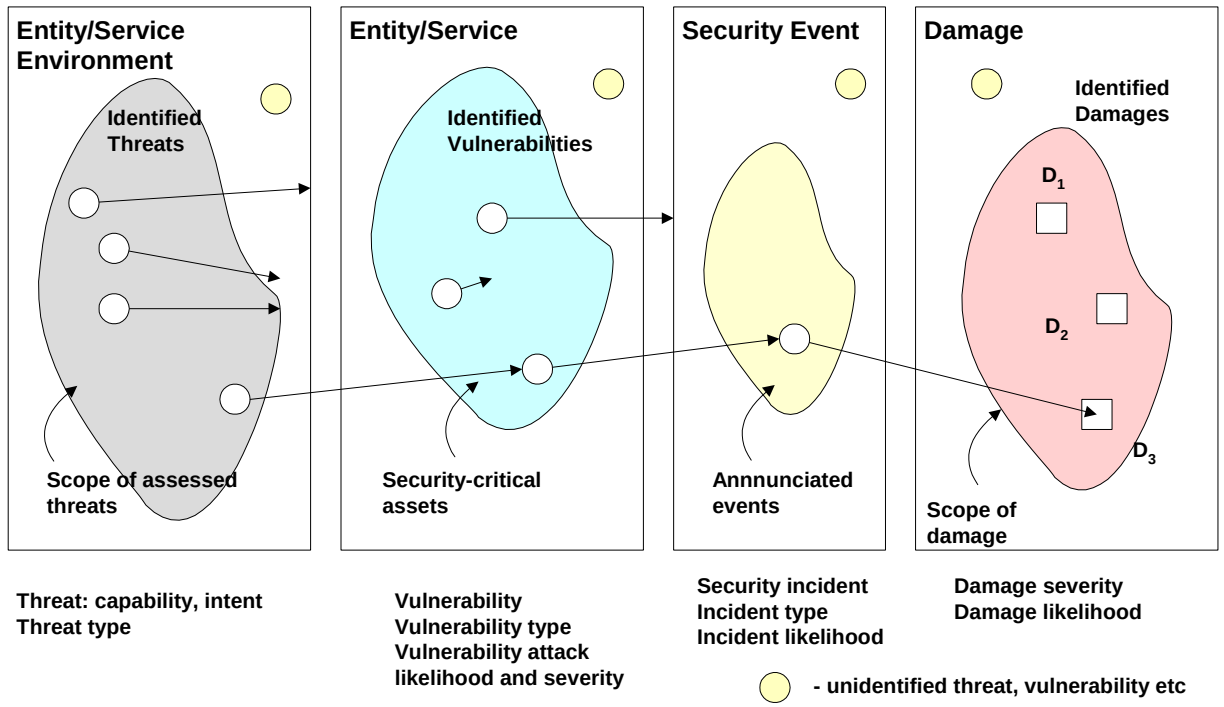


Figure 11 Four inter-dependent strategies to manage security risk (operations)

Security risk management during development and operations is illustrated in Figures 10 and 11 respectively.

4 Target Systems Model

Security concerns arise in systems and assets of many types and over an enormous range of scale. Examples include:

1. Software at code level, bit/register level;
2. Software module, object
3. Software application
4. Software system, architecture;
5. Hardware component, particular technology/ physical principles;
6. System, an aggregation of software and hardware components (single, monolithic entity);
7. Networked system, where communication links and nodes lie within protected environments;
8. Systems of systems, i.e. systems that are developed to independent goals, but are required to inter-operate;
9. Systems with specific prime function; information processing, command & control, embedded real-time control etc;
10. System or component with a prime function to mitigate security risk;
11. Internet technology component or system, where communication links and nodes are provided by many other parties;
12. Grid systems;
13. Mobile/ ubiquitous systems;
14. System in which safety and security properties are inter-dependent;
15. Organization with infosec policies;
16. Development system (infrastructure used to design, develop, manufacture and operate security-critical components and systems).

Figure 12 shows one categorization of systems that might be useful for developing security measures. Typical risks and mitigation actions are indicated.

The identification of base measures depends on the identification of entities involved in system development. These will vary across the different types and scales of entity. It is useful to develop a set of representative component/ system types, such as those sketched in Figure 13. Such templates help specifying measurement constructs, the assumptions made in their development and the tailoring of them to particular situations.

Notations vary between areas of security practice. The system architecture notation recommended in the DoDAF standard [16] might be appropriate for defense systems. Network security could make use of the notations of the CISCO SAFE methodology [15], for example. Software security could make use of standard software architecture and design notations. The threat modeling approach to software application development reported in [7] makes use of classic data flow diagrams.

The concept of a *local* operational (threat) environment seems to be important, because it represents a distribution of risk mitigation between the system of concern and other, external systems. This enables modeling of the distribution of risk acceptance over complete systems. Defense-in-depth involves *as-designed* distributions of risk reduction, complemented with maintenance and adaptation during operations.

From a measurement perspective, the target system will be determined in part by the information needs being served, i.e. the scope of the actions available to the users of indicators. A useful concept here is the *level of intervention* available to decision-makers; for example, the management of an infosec policy will usually work at the level of COTS components. These can be configured, integrated and operated in definable ways, but the functionality and flaws in the components are accepted as-delivered. A developer of secure software can intervene at a more detailed level, for example, tracking individual defects and vulnerabilities at code level.

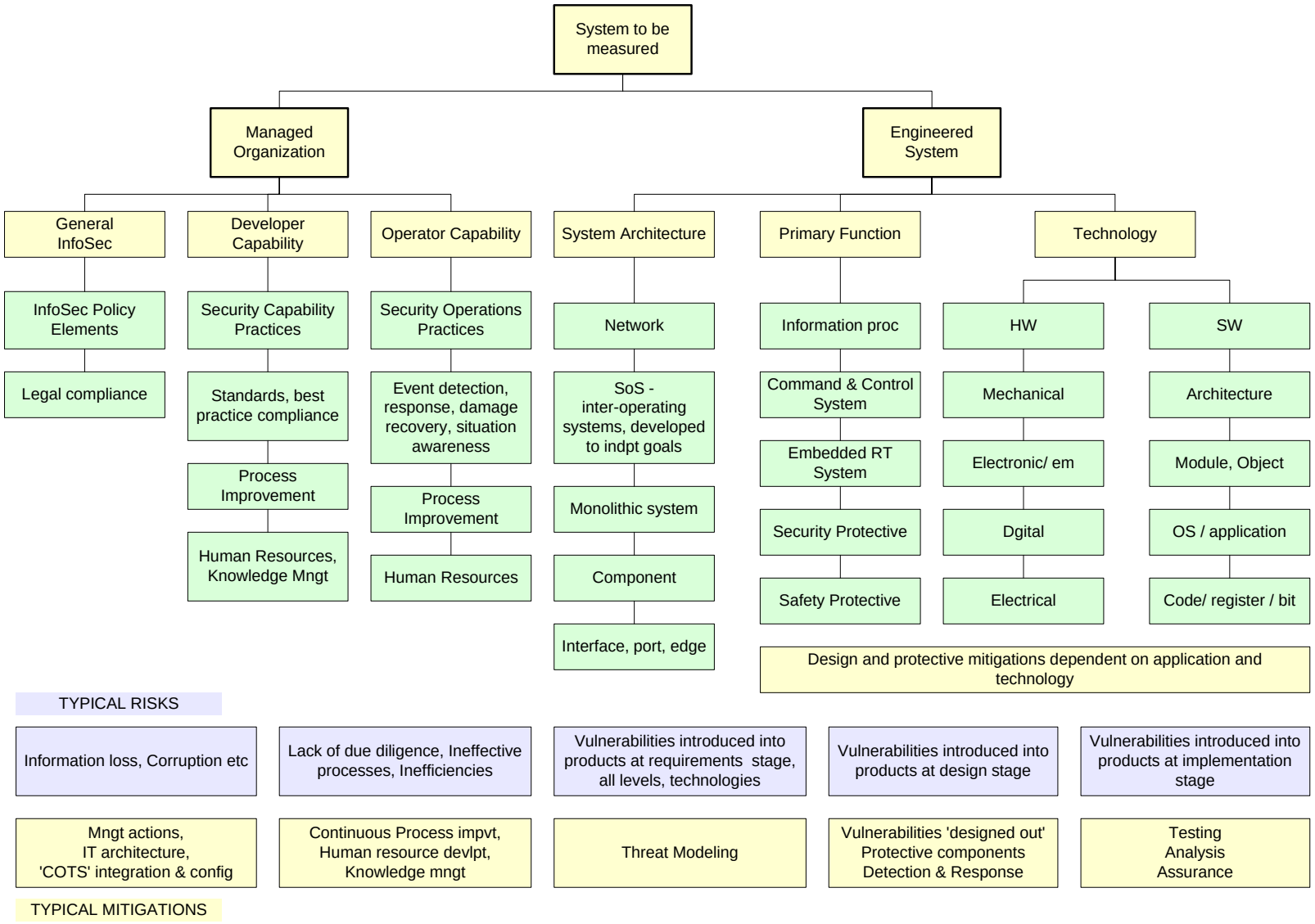
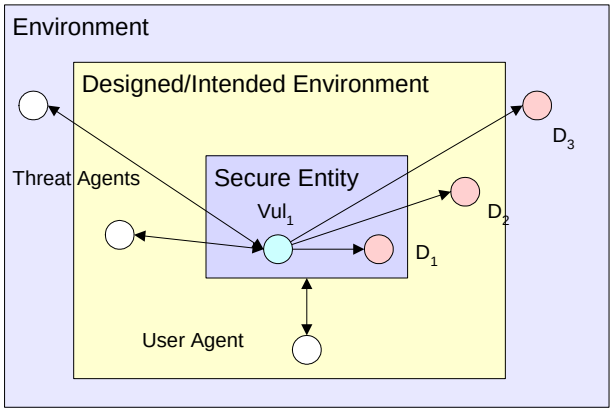
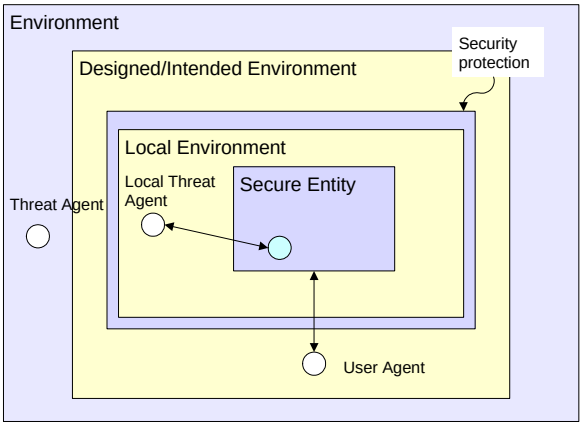


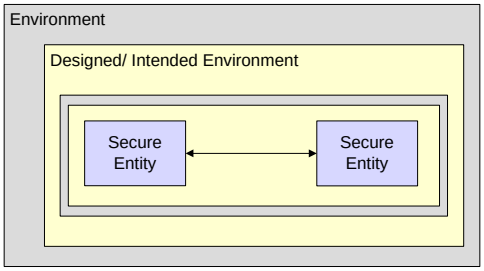
Figure 12 Typology of systems



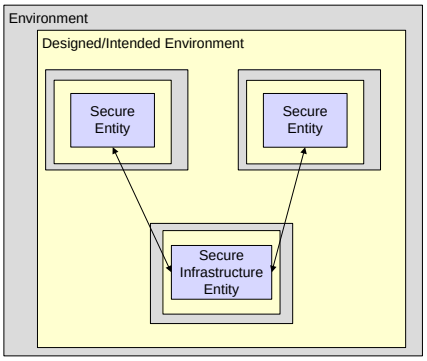
Single entity, sw, hw, mixed



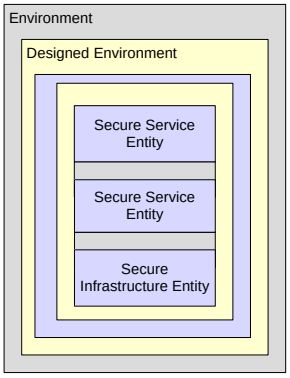
Secure entity with protection



Networked entities within a protected environment; trusted paths, integrity



Networked entities with access from unprotected environment



Layered entities e.g. ports

e.g. NIST models [17]
DoDAF models [16]
SW models [7]
Network models [15]

Architecture models

Figure 13 Template system architectures to support security management (sketches only)

5 Representative Security Practices Model

The development of measurement constructs within the PSM approach involves the mapping of information needs to identified base measures (Figure 1). These will be attributes of artifacts that are present in the relevant practices. Measurement guidance assumes typical practices and work products by developing representative models for these.

In the security domain, practices will vary widely, depending on the type and scale of entity of concern and its environment. Security standards and published good practice guidelines provide source materials. Example practices include:

1. software engineering for secure code (development process models, vulnerability scanning tools, formal analysis techniques etc);
2. systems engineering for secure systems (e.g. maturity models SSE CMM, safety & security extensions to the iCMM / CMMI models);
3. Common Criteria – development of security functional components and systems in the IT field;
4. development of security-specific functional components (e.g. encryption, A&I);
5. information security management (ISO/IEC 17799, CISWG study) and policy compliance;
6. network security;
7. damage recovery.

Each of these areas (and many others) has extensive and rapidly developing practices. Appendix 5 provides some review material and references, including the goals and practices of the safety & security extensions of the iCMM/CMMI models [9].

Security practices have the general objectives of achieving reductions in security risks and compliance with applicable regulations and standards. Identifying security practices, together with the systems they are applied to, enables the identification of potential measurements.

During development, security engineering practices are enacted to achieve security goals expressed as requirements placed on products. During operations, security operations practices are enacted to achieve security goals expressed as performance goals.

The following paragraphs provide a summary model of security practices, sufficient to develop useful measurable concepts.

5.1 Security Risk Management

Improving the general quality of product development contributes to security. Recent work on the measurement of software security has treated security in product quality terms [18]. This provides a valuable underlying approach, since every defect introduced during development is a potential vulnerability.

There are likely to be benefits from also implementing formal risk management processes, because this enables prioritization of defects from a system security perspective and the accumulation of experience tailored to security issues. In software development, for example, a combination of strategies can be adopted:

1. improve general product quality; reduction of defects;

2. check for defects that are typically implicated in security vulnerabilities, based on accumulated experience in the type of product being developed;
3. check for defects against particular attack goals and trees, using security risk assessment conducted for the particular product and threat environment.

The basic methodology of risk management is as follows (adapted from [15] and [19]):

1. identify the assets and functions that are critical to the success of the organization, product, service;
2. assess threats to the assets; modeled often as attackers with attack goals etc;
3. assess vulnerabilities of the system; modeled often as paths in an attack tree;
4. on the basis of 2 and 3, assess the security risks to which the assets are potentially exposed for example, in terms of confidentiality, integrity, availability and privacy in the case of information security;
5. establish acceptable thresholds for those risks;
6. mitigate known risks and maintain to acceptable levels by;
    a. for infosec policy implementation: identifying and implementing security strategies, policies, and controls involving people, process, and technology;
    b. for developers: detecting, removing, reducing vulnerabilities introduced during the SDLC (Figure 14); introducing protective systems, developing operational protections, increasing confidence by test and assurance;
7. maintain 'situation awareness' to detect new risks.

Security development practices can be decomposed and related to the systems they are applied to, in a manner similar to security policy decomposition. For example, a representative lifecycle for application software security comprises the following steps [7]:

1. Gather security requirements;
2. Secure design (architecture, components);
3. Model threats;
4. Perform implementation-level analyses (code reviews);
5. Perform Penetration tests;
6. Secure deployment;
7. Integrate feedback.

The actions involved in mitigating security risks vary enormously over the types of system, threat and vulnerability involved. Mitigation actions may be categorized as follows:

1. reduce the likelihood of an attack attempt, for example by seeking to modify the components of Figure 15;
2. remove (design out) the vulnerability;
3. reduce likelihood of a successful attack by operational means (detection and response);
4. reduce effects of a successful attack, through design and/or operational means;
5. improve damage recovery following a successful attack.

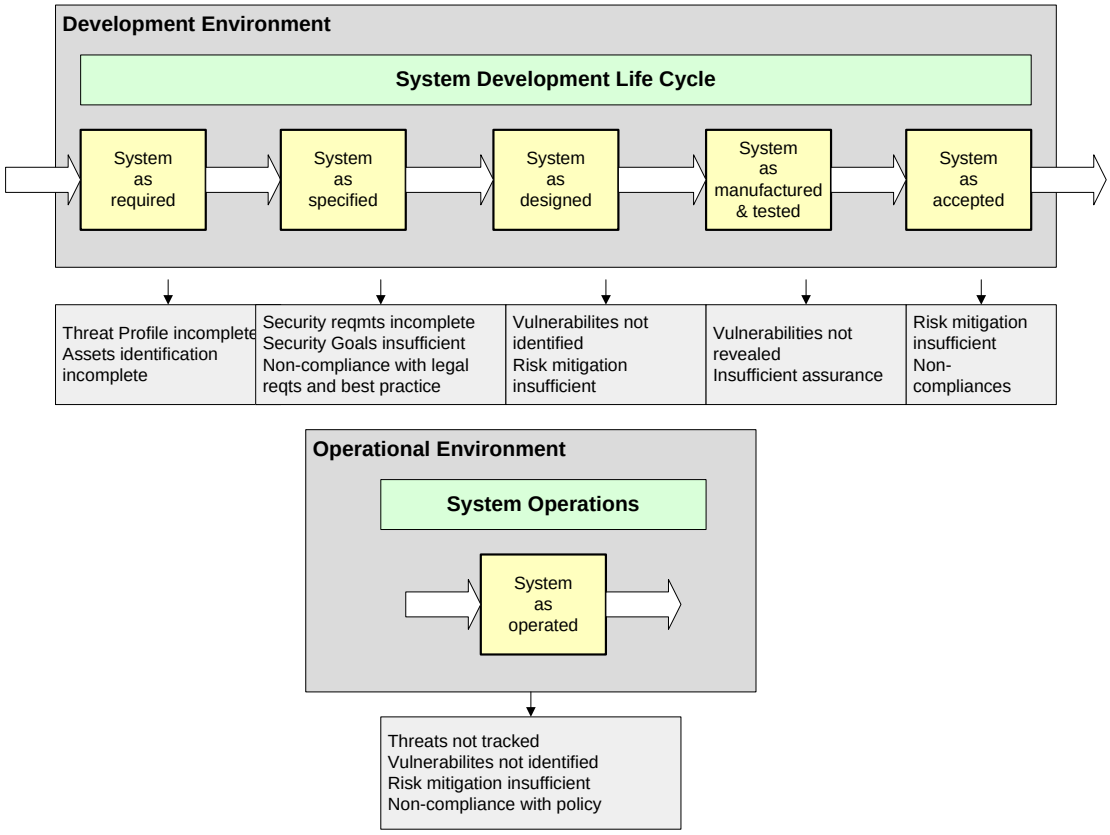


Figure 14 Linear view of development and operations processes illustrating sources of security risks

From a practical point of view, a given situation will present a decision-maker with a constrained scope for action, implying an information need and measurement construct that is restricted to the responsibility involved.

The set of implemented mitigation actions (as part of a security policy or development process) can be tracked and monitored as for any other tasks. Time, cost and progress measures can be developed.

A claim about a risk often represents a mix of objective measurement and professional judgment. The confidence that can be placed in it is increased by the provision of supporting evidence. This leads to the development of security cases (by analogy with safety cases); structured arguments that integrate the evidence supporting a claim.

5.2 Policy Compliance

As discussed above, an infosec security policy is decomposed into a set of policies applicable to different appliances and aspects of information security. For example, a top-level security policy may be decomposed into the following elements [15].

1. physical security policies;

2. access control policies;
    a. password properties, change properties etc

3. dialup and analog policies;
    a. modem response
    b. one-time passwords
    c. traffic monitoring
    d. fax line use
    e. password storing
    f. strong authentication

4. remote access policies;
    a. T1
    b. Frame relay
    c. VPN access

5. remote configuration policies;
    a. secure sockets layer
    b. secure shell

6. VPN and encryption policies;
    a. User management
    b. Time length control
    c. Encryption standard

7. network policies;
    a. router policy
    b. firewall policy
    c. DMZ policy
    d. Extranet policy
    e. www policy
    f. wireless policy
    g. server policy

8. data sensitivity, retention and ethics policies;

9. software policies;
    a. operating system policy
    b. virus protection policy
    c. user software policy
        i. installation policy
        ii. database policy
        iii. e-mail policy.

The measurements recommended in the CISWG study [4] are mainly monitoring compliance with a policy.

5.3 Threat Modeling

Threats may be viewed as the attack goals of threat agents. The factors involved in assessing the security risk posed by a particular agent have been modeled by [19], as shown in Figure 15. These factors can be assessed on the basis of qualitative scales, enabling risks to be prioritized. For example, the threat capability of a group of terrorist threat agents is assessed on the basis of [19]:

1. Group size;
2. Level of education;
3. Cultural factors;
4. Access to communications and the Internet;
5. Technical expertise;
6. History of activity;
7. Sponsoring countries;
8. Funding.

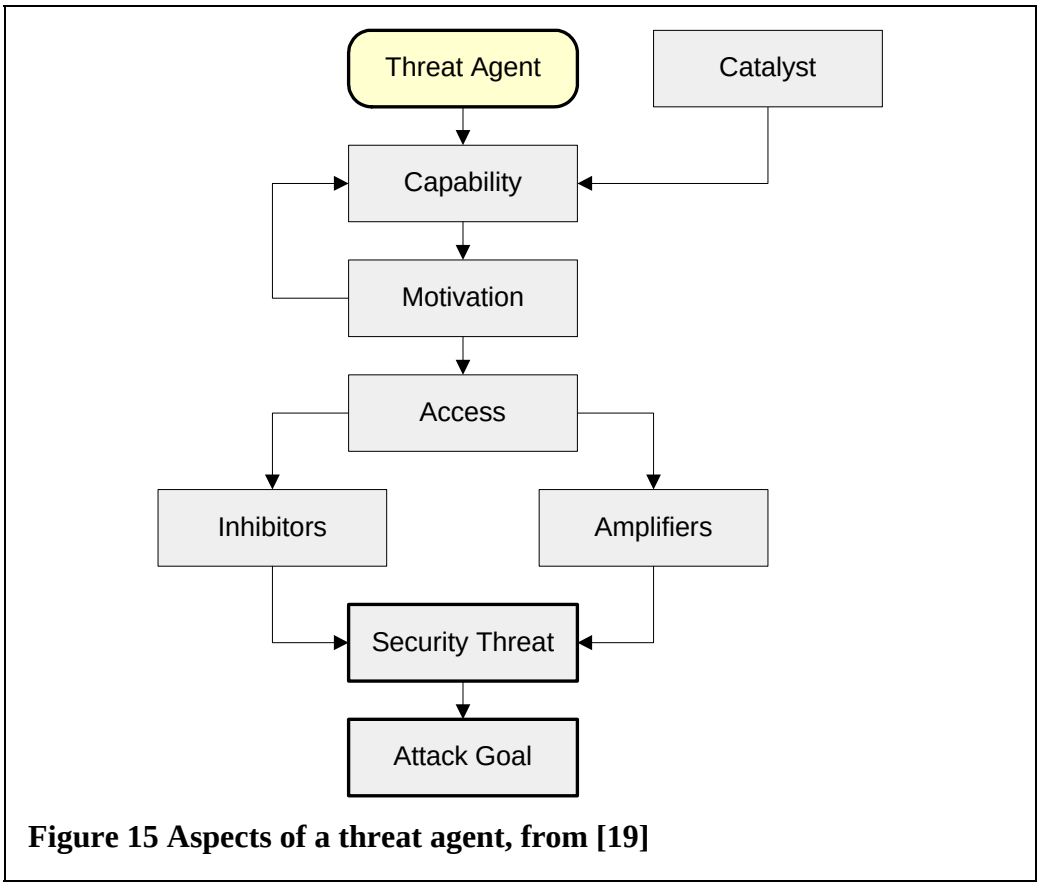


Figure 15 Aspects of a threat agent, from [19]

The particular attack goals and the options for achieving them in relation to the target system, are modeled by *attack trees*. A top-level goal (Figure 16) is decomposed into sub-goals in an AND/OR tree. The path from a leaf node to the top-level root is an *attack path*. The set of all identified threats to a system from a particular threat agent, is the agent's *threat profile*.

Attack trees may be used to integrate quantified assessments of the costs to the attacker in achieving the goal at each node. Alternatively, a probability of success may be associated with each node, making the threat tree similar to Fault Trees, as used in safety engineering.

The likelihood of a successful attack can be assessed by from the probabilities along the complete attack path. The security risk associated with the attack is assessed from the costs associated with the effects of the successful attack.

Mitigation actions may then be developed if the assessed risk exceeds an acceptable threshold. For security events that carry high damage (and for which we are highly averse), trade-offs between mitigation costs and damage costs may be considered under the ALARP Principle, as for safety.

Alternatively, for security events that can be accepted as an operational cost, mitigation investment can be compared with annual expected losses.

The attack paths of an attack tree that have not been mitigated sufficiently represent vulnerabilities in the target system

In addition to the probability and cost aspects, measurements can also be based on tracking identified threats and attack paths (as in a project risk register); the number of threats (top level goals) and attack paths, under selected categories, can be tracked over time. Time and costs associated with mitigation actions can be tracked.

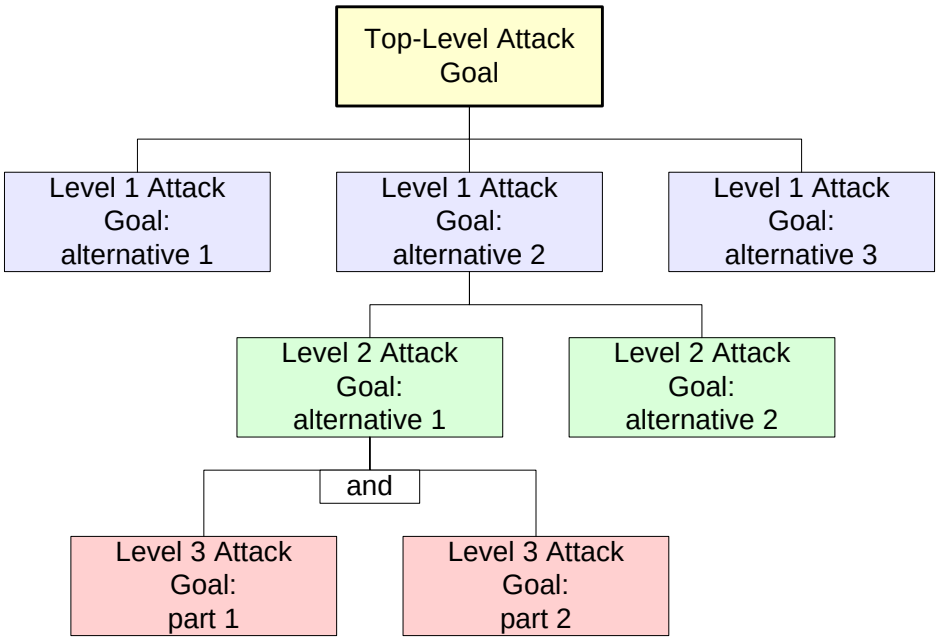


Figure 16 Attack Tree

The particular form of attack goals and sub-goal strategies will depend on the target system and assets. For example, threat effects have been classified as follows in the development of secure application software [20]:

STRIDE

1. Spoofing;
2. Tampering;
3. Repudiation;
4. Information disclosure;
5. Denial of service;
6. Elevation of privilege.

5.4 Vulnerability Assessment

While threat modeling is an important top-down approach to developing secure systems, it is also necessary to take a bottom-up approach, in which defects are sought that might lead to vulnerabilities.

Defects can be introduced at all phases in a development lifecycle; requirements, design and implementation. For example, at software level, a defect tracking system may be used to improve general software quality. However, a defect will have variable security implications, depending on whether it is exploitable by attackers and the consequences of a successful attack..

The following classification has been reported [20] for types of security vulnerability in software:

DREAD

1. Damage potential;
2. Reproducibility;
3. Exploitability;
4. Affected user;
5. Discoverability.

For software, vulnerability scanning tools (e.g. from Ounce Labs) are available today to assist with the detection of defects commonly associated with security events. Similar principles can be applied to systems, more generally, making use of libraries of known types of defect.

The tracking of potentially exploitable defects and vulnerabilities enables the measurement of numbers of these over time, in different type and status categories.

5.5 Evaluation, Testing

The Common Criteria (CC), now established as an international standard ISO/IEC 15408 [14], provide a framework for the independent evaluation of the security performance of IT products. The evaluation process involves:

1. the identification of security objectives and requirements, constituting a *Security Target* (ST);
2. the optional use of a standard *Protection Profile* (PP), representing typical sets of security functions;
3. the identification of a *Target of Evaluation (*TOE);
4. the evaluation of the TOE against the PP and security requirements;
5. several evaluation levels (EAL 1 through EAL 7), providing different levels of evaluation rigor, and therefore confidence in the performance.

The Common Criteria provide assurance to a system developer that an acquired security product meets specified security performance standards. Security risk is reduced by assessment against internationally agreed performance standards. The CC framework is built around catalogs of PPs and evaluated products. Additional requirements and evaluation criteria, not in the standard models, can be included.

Evaluation of the resistance of products to attacks provides important supporting evidence of the effectiveness of risk mitigation actions. The security of a system is assessed against a defined threat model.

The security concept model includes all test and evaluation-based measures under the *Assurance* heading.

6 Measurable Entities

Measurable entities are the work products and events that are involved in system operations and development. The measurable entities in operations are implied by the decomposition of a security policy into sub-policies for various aspects of security. In development, entities will be derived from the SDLC and the formalized security risk management process, as mapped onto the components and subsystems involved.

Table 2 identifies a selection of measurable entities, for illustrative purposes. A particular project will present a particular set of such entities.

Phase	Measurable Entity	Attributes	Notes
Context: Capability	Reference Process Model and Practices	Strengths and Weaknesses Practice Characterizations Goal Ratings PA ratings Capability Profiles	iCMM/ CMMI measures relating to the institutionalization of processes.
Start Up	Security Policy/ Plan	Security Process Definition Tasks Schedule Resources Work Products	Planning and deployment of security process assets on a particular project.
		Roles, responsibilities	Including independent security checks
		Staff Competencies Skills and Experience Matrix	
		Reporting Arrangements	
		Contractual Agreements	
		Dispute Resolution Provision	
Product Development; Pre-manufacture	Security Requirements / Objectives Log or database	Requirement Count Requirement Scope Requirement Source Status	Summary record of security requirements, including customer sourced, derived (developed by the security process) and requirements placed on suppliers
	Security Asset Log	Product Components Product Functions Product Modes Mission Phases Process Resources	
	Threat Tracking System	Threat Agent Count Threat Agent Status Threat Attack Tree Threat Risk	.
	Vulnerability Tracking System	Vulnerability Count Vulnerability Status Vulnerability Scope	
	Security Action/ Mitigation Log	Action Count Action Status	Summary record of all actions generated by the security process, including mitigations.

Post Manufacture: assembly, integration and test	Verification Test Log	Verification Count Verification Status Action Status Action Scope	Summary records of the tests and other data that demonstrate security requirements have been met.
	Acceptance Test Log	Validation Count Validation Status Action Status Action Scope	Summary record of the validation tests and other data that are agreed as acceptance criteria across customer/supplier interfaces.
Operations	Event Tracking System	Count Type/ severity Action Status Scope	Threat and vulnerability tracking systems remain to support operations
	Damage Tracking System	Count Type/ severity Action Status Scope	
	Security Policy Compliance	Check list Count Type Action Status	
Security Assurance	Security Assurance Case	% completion against planned argument structure	Replaced or augmented with Common Criteria approach, if applied.

Table 2: Measurable entities involved in tracking particular risks

7 Measurable Concepts

The following measurable concepts are proposed, based on the preceding models. The structure of the PSM I-C-M Table is followed.

Information Category	Measurable Concept	Examples	Measurement Reference
Schedule and Progress	Work Unit Status	Mitigation Status	Security Risk Tracker
		Status of planned security process tasks	Project Plan
Resources and Cost	Security Capability Deployed	Competency of teams	Professional Society models
	Capability Maturity	Maturity of security practices	Audit against CMMI/ iCMM extensions
	Resources Consumed in Operations and development	Costs	Project Plan
		Schedule	Project Plan
Product Size, Stability and Scope	Scope - Security (secure system)	Security Requirements	Requirements Tracker
		Security-Critical Functions	System design and threat environment. Scope provides basis for estimating and monitoring progress
		Security-Critical Components	
		Security-Critical Interfaces	
		Security-Critical Modes	
		Security Enclaves	
		Security Change Workload	Project Plan
	Scope - Security-critical Assets	Value	Priority; level of protection required

		Damage Costs	Damage scenarios
		Security Risk Tolerance	Assurance required
Environment Properties	Security Risk: Threat Agents	Threat Level [19]	Standard models
		ROI for Attacker	Attacker perceived Gain & Attack Cost
	External Dependency	Externalized Risk	Security risk borne by external agencies
	Insurance	Insured Risk	Financial risk transferred to insurer, at cost
Product Quality	Defects	Defects potentially security-related Latent defects	Categorized by SDLC phase
	Security: Attack Trees	Count of trees and status Count of Attack Paths in each tree and status	
	Security Risk: Vulnerabilities	Likelihood of attack/ exploit	Assessment Penetration Testing
		Likelihood of successful attack	
	Security Risk: Damages/ Impacts	Impact Cost	Damage Assessments
	Security Risk: Security Events	Count of, categorized Undetected events	Monitoring Systems (e.g. IDSs)
	Security Risk: Responses	Response success rate	Monitoring Systems
	Assurance - Security: Test/ Analysis/ Inspections	CC EALs	Common Criteria independent tests
		SW scanning tools e.g. OUNCE Labs Vulnerability density	Checks implicit in tools
		Integrated Security Assurance Case	
Process Performance	Compliance: Legal	Regulatory certification	Legal requirements
	Compliance: Industry/ standards	Secure SW development – checklists of common vulnerabilities	Industry recommendations (e.g. CERT)
	Compliance: Best practice	Checklists (see Appendix 5)	DISA Checklists, Security Engineering
	Compliance: Security Policy	CISWG [4]	Adopted Security Policy
	Situation Awareness	Detected potential threats	Identified threats
	Performance Outcome: Events/ Incidents	Number of intrusions, incidents by category, 'near misses'	Historical performance
	Performance Outcome: Damages	Damage costs, to operator and other parties	Recovery cost monitoring systems
	Performance Outcome: Residual Risk	Residual security risk	Difficult to directly measure, but as assessed
	Performance Outcome: Effectiveness	Return on investment ROSI Response Time	

	Performance Outcome: Security Options	Security options	
	Custome r Trust	Trust in organization / system as expressed by customers, users	User perception relative to the past

Table 3 Measurable Concepts for security, derived from the Security Concept Model

Security performance is viewed as a combination of directly measurable security events (e.g. number of successful intrusions, costs incurred) and reductions in the risks of future events. A risk perspective is necessary to support decisions about the allocation of resources and the taking of preventative actions. Direct measurement of security outcomes (e.g. in terms of the penetration of attack scenarios) is also necessary to ground assessments and provide objective evidence. Events that are very high risk (c.f. safety accidents) may be intolerable, in which case the risk approach is dominant. Near-miss events and successfully repulsed attacks will provide measurement data under these circumstances.

8 Measurement Guidance

The following steps are proposed (outline only):

Context of security measurement

1. identify security assets, surfaces, objectives, policy, environment;
2. identify context in terms of type of asset, and whether development project or operations management;
3. identify interfaces with other responsibility areas, performances;
4. identify standards, procedures being applied;

Information Needs

5. identify roles/responsibilities of those requiring management information about security;
6. identify information needs of those roles/responsibilities;
7. categorize needs with reference to proposed information needs model (risk, cost, progress, performance, readiness, compliance) at the three management levels (project/operations, organization, enterprise);

Measurement Systems

8. survey measurable entities, with reference to proposed security measurement concept (threat environment, system vulnerabilities, events, damage);
9. depending on local resources and context, develop risk and performance tracking systems and measurements based on them;
10. map tracking systems to artifacts in the managed sub-domain (field of action);

Measurement Constructs

11. develop indicators to serve information needs, based on identified base measures;

12. depending on local contexts, tailor the security measurement constructs proposed in the security measurement model;
13. adapt measures in response to evolving threats and vulnerabilities.

> Further Development
> Develop a security measurement process model, for each of the development and operations cases. Align with a risk management process, operational security policy and the SDLC.

9 Conclusion

An integrated approach to security measurement has been proposed. The security field is diverse and evolving rapidly to meet the dual challenges of net-centric systems and increasingly capable threat agents. Several topics of further development have been identified in this report. More generally, effort is required in the following areas:

1. Develop example measurement specifications based on particular security practices/ standards, and particular technologies (e.g. software development, CC security functional components);
2. Provide practical guidance on how to develop security measures;
3. Develop wider engagement with security specialists, to test proposals etc;
4. Test measurement proposals and improve by means of project trials.

10 References

1. PSM 2003 www.psmsc.com
2. ISO/IEC, **ISO/IEC 15939:2002(E),** *International Standard Software engineering - Software measurement process*, 2002-07-15, ISO/IEC.
3. Murdoch, J., **v 2.0,** *Safety and Security Measurement*, February 2004, PSM.
4. CS1/05-0005, *Corporate Information Security Working Group: report of the best practices and metrics teams*, 10 January 2005, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Government Reform Committee, US House of Representatives.
5. Berinato, S., *Finally, a Real Return on Security Spending*, in *CIO Magazine*. 2002
6. Larsen, G. *Strategic Observations and Thoughts on a System Model for Security Metrics/Measurements: Why can't we get traction?* in PSM TWG. 23 March 2005. Herndon VA. 2005.
7. Swiderski, F. and W. Snyder, *Threat Modeling*. 2004, Redmond, Washington: Microsoft. 259.
8. Rouse, W.B. and K.R. Boff, *Value-Centered R&D Organizations: ten principles for characterizing, assessing and managing value.* Systems Engineering, 2004. **7**(2): p. 167-185.
9. Ibrahim, L., *et al.*, *Safety and Security Extensions for Integrated Capability Maturity Models*, September 2004, US FAA & DoD.
10. Charette, R., L.M. Dwinnell, and J. McGarry, *Understanding the Roots of Process Performance Failure.* CrossTalk, 2004. **August 2004**: p. 18-22.
11. Colbert, E. et al, *Costing Secure Systems: 5th Workshop*, 21 March 2004, USC-CSE.
12. **ISO/IEC 21827 v3.0,** *Systems Security Engineering Capability Maturity Model (SSE-CMM)*, ISO/IEC.

13. **ISO/IEC 9126** *Information technology - Software Product Evaluation - Quality characteristics and guidelines for their use*.
14. **ISO/IEC 15408 v2.1,** *Common Criteria for Information Technology Security Evaluation*, Common Criteria Project Sponsoring Organizations.
15. Paquet, C. and W. Saxe, *The Business Case for Network Security: advocacy, governance and ROI*. 2005, Indianapolis: Cisco Press. 381.
16. DoDAF, *DoD Architecture Framework Version 1.0*, 9th February 2004, US Department of Defense, Architecture Framework Working Group.
17. Stoneburner, G., **NIST SP 800-33,** *Underlying Technical Models for Information Technology Security*, December 2001, NIST.
18. Zubrow, D., J. McCurley, and C. Dekkers, *Measures and Measurement for Secure Software Development, DHS BSI web site*. 2005, US Department of Homeland Security
19. Jones, A. and D. Ashenden, *Risk Management for Computer Security: protecting your network and information assets*. 2005, Oxford: Elsevier. 274.
20. Howard, M. and D. LeBlanc, *Writing Secure Code*. 2003: Microsoft Press International. 800.
21. **ISO/IEC 15408-1:1999(E),** *Information technology — Security techniques — Evaluation criteria for IT security*, 1 December 1999.
22. **BS ISO/IEC 17799:2000,** *Information technology - Code of practice for information security management*, 15 February 2001, ISO/IEC.
23. Firesmith, D.G., **CMU/SEI-2003-TN-033,** *Common Concepts Underlying Safety, Security and Survivability Engineering*, December 2003, Carnegie Mellon University.
24. PMI, *A Guide to the Project Management Body of Knowledge: PMBOK 2000*, Project Management Institute.
25. APM, *PRAM Project Risk Analysis and Management Guide*, Association for Project Management.
26. Chapman, C. and S. Ward, *Project Risk Management: processes, techniques and insights*. 2nd ed. 2003, Chichester: John Wiley. 389.
27. MIL STD-882B, *System Safety Program Requirements*, . 1984, US Department of Defense: Washington DC
28. **IEC 1508** *Functional Safety: Safety-Related System (Draft)*, International Electro-technical Commission.
29. Williams, J.R. and G.F. Gelen, **ATR 97043,** *A Framework for Reasoning about Assurance*, 23 April 1998, Arca systems Inc.
30. Weick, K. and K. Sutcliffe, *Managing the Unexpected: Assuring High Performance in an Age of Complexity*. 2001: John Wiley. 224.
31. Henning, R. *Workshop on Information Security System Scoring and Ranking*. May 21-23, 2001. Williamsburg, VA: Applied Computer Security Associates & MITRE. 2001.
32. **BS 7799-2:2002,** *Information security management systems - Specification with guidance for use*, 5 September 2002, British Standards Institute.
33. Deming, W.E., *The New Economics: for industry, government, education*. 2nd ed. 2000, Cambridge, Mass.: The MIT Press. 247.
34. Swanson, M., *et al.*, **NIST Special Publication 800-55,** *Security Metrics Guide for Information Technology Systems*, July 2003, NIST.
35. **DoD Directive 8500.1,** *Information Assurance*, 24 October 2002, US Department of Defense.
36. Alberts, C.J. and A.J. Dorofee, **CMU/SEI-2001-TR-016,** *OCTAVE Criteria, Version 2.0*, December 2001, SEI CMU.

Appendix 1 Sources

Report/ Standard/ Practice	Source	Status/ Application
DoD Directives e.g. DoDD 8500.1	DoD	Various PKI systems KMI
ISO/IEC 17799:2000	ISO/IEC	Information Systems - includes organizational issues
ISO/IEC 13335	ISO/IEC	Security Management
ISO/IEC 15408 Common Criteria	Now established as an ISO standard	IT systems and products – excludes organizational issues etc. Establishes third-party independent evaluation of security properties.
ISO/IEC 21827 SSE-CMM	ISO/IEC Consortium, with SEI	Systems Security Engineering Capability Maturity Model (SSE-CMM)
OCTAVE	SEI, CMU	Security risk assessment method
Costing Secure Systems – COCOMO	USC-CSE	Parametric cost modeling/ estimation – extensions to include security costs
NIST Handbook SP 800-30	NIST	Risk Management Guide for Information Technology Systems
NIST Handbook SP 800-55	NIST	Security Metrics Guide for Information Technology Systems
iCMM/ CMMI Safety & Security extensions	FAA/ DoD	Safety and security extensions to the CMMI maturity model. Defines 22 practices under five headings
Security Management views and practices	CSO	Chief Security Officer issues
Security Technical Implementation Guides (STIGS) and Checklists	NIST CSRC, DISA	Computer and IT security
Federal Agency Security Practices	NIST Computer Security Resource Center	Security Practices (computer, network, physical etc.)
Threat Trees, Attack Trees	Security Literature	Systematic method that links attack goals with system vulnerabilities
SANS Checklists	SANS Institute	Internet security
CERT Guides	SEI CMU	Internet security
DISA Checklists	DISA	Security practices
IS* Concept	Security Metrics Workshop	ACSA, Mitre
CISWG Report CS/05-0005	Corporate Information Security Working Group, Govt Reform Committee, US House of Representatives	Security metrics for information security
ISG Assessment Tool, Report	Information Security Governance Task Force, Cyber-Partnership	
ISO/IEC 9126	Software Quality attributes	Being revised
DHS BSI Website	Security Measurement: quality attribute approach	Draft advisory material for software security

Table 4 Sources used in this report

Appendix 2 Glossary

Asset

Information or resources to be protected by the countermeasures of a system (a Target Of Evaluation in Common Criteria evaluation terms).
Adapted from ISO/IEC 15408-1 [21]

Attack Goal

The objective of an attacker.

Attack Tree or Threat Tree

The means by which the goal of an attacker can be achieved, decomposed recursively as sub-goals in AND/OR relations.
Set of alternative attack paths by which a top-level attack goal can be achieved.

Defect

A flaw in a system that results in it not performing as wished. In this paper, a defect may or may not have security implications.

Information Security

Information security is characterized as the preservation of:

1. confidentiality: ensuring that information is accessible only to those authorized to have access;
2. integrity: safeguarding the accuracy and completeness of information and processing methods;
3. availability: ensuring that authorized users have access to information and associated assets when required.

ISO/IEC 17799 Information technology — Code of practice for information security management [22]

Mitigation

Reduction in risk achieved by some action. Security risks during development can be reduced by better requirements, design, improved manufacture and test and countermeasures. During operation, security risks can be reduced by improved policies, better enactment and countermeasures.

Return on (Security) Investment; ROI, ROSI

Benefit achieved, usually expressed in money terms, arising from expenditure on security

Risk Assessment

Assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence.
ISO/IEC 17799 Information technology — Code of practice for information

security management [22]

Risk Management

Process of identifying, controlling and minimizing or eliminating security risks that may affect information systems, for an acceptable cost.
ISO/IEC 17799 Information technology — Code of practice for information security management [22]

Security

The security of a system is the extent of protection against some unwanted occurrence such as the invasion of privacy, theft, and the corruption of information or physical damage.
[onlineethics.org/glossary.html]

The quality or state of being protected from unauthorized access or uncontrolled losses or effects. Absolute security is impossible to achieve in practice and the quality of a given security system is relative. Within a state-model security system, security is a specific 'state' to be preserved under various operations.
[www.nrc.gov/site-help/eie/terms_id.html]

Work that involves ensuring the confidentiality, integrity, and availability of systems, networks, and data through the planning, analysis, development, implementation, maintenance, and enhancement of information systems security programs, policies, procedures, and tools.
[www.opm.gov/fedclass/text/GS-2200.htm]

System

A specific IT installation, with a particular purpose and operational environment. – ISO/IEC 15408.

As used in this report, a general term indicating an entity that provides some useful functionality and has to be developed and operated. Also has assets that are to be protected from attack.

Threat Agent or Attacker

An individual, group or agency that has (security) attack goals against some asset.

Target of Evaluation (TOE)

An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.
ISO/IEC 15408-1 [21]]

Threat Profile

The set of threats (attack goals) presented to a system.

Threat

The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security.
www.ee.oulu.fi/research/ouspg/sage/glossary/

Vulnerability

A defect in a system that enables an attacker to exploit some asset.
An attack path in an attack tree that is insufficiently mitigated.

Appendix 3 Data Models

The following charts show information models of the concepts involved in security.

'Roundtangles' represent *roles* – sources of information need and instigators of actions. Rectangles represent entities relevant to security engineering and operations.

Figure	Caption
17	Threat Agent (or attacker) role as the source of Attack Goals
18	Developer role as the source of mitigation actions during development. SDLC = System Development Life Cycle
19	Operator role as the source of mitigation actions during system operations
20	Security Manager (operations) role as a monitor of security performance, compliance and residual risk
21	Board Member/Trustee role as a monitor of security performance, governance and residual risk
22	Security Manager (Development) role as a monitor of assessed security and resource usage
23	System physical and organizational decomposition; also as represented in different development phases
24	Interaction between Threat Agent and Operator roles

Further Development
Review the information models and representative roles of Figures 6 and 17-24; check consistency between them and check implied definitions with security standards etc. Also check with [23].
Ensure measurable concepts are consistent with these in concept and terminology.
Consider these models as starting points for tailoring to particular applications.

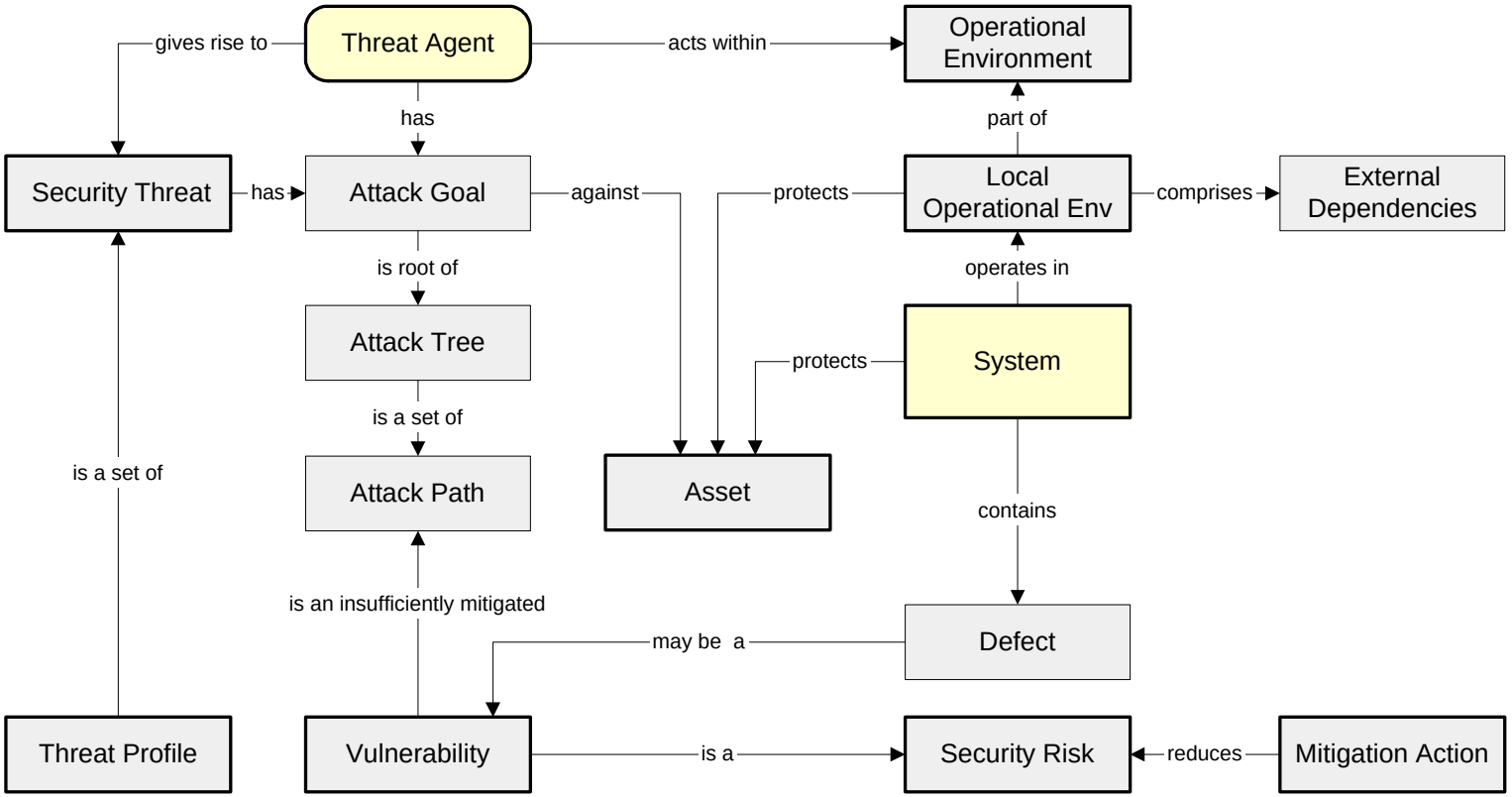


Figure 17 Threat Agent (or attacker) role as the source of Attack Goals

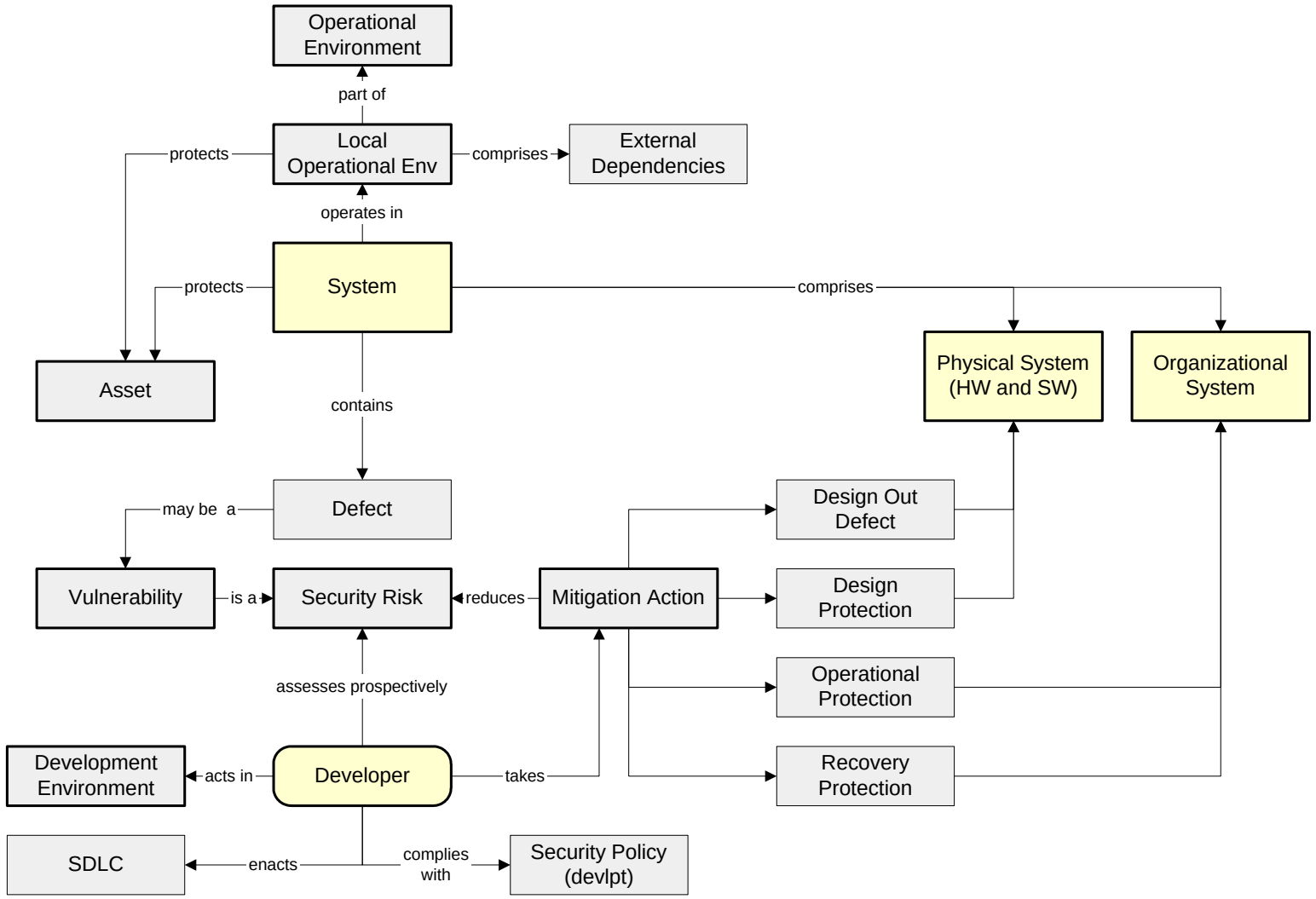


Figure 18 Developer role as the source of mitigation actions during development. SDLC = System Development Life Cycle

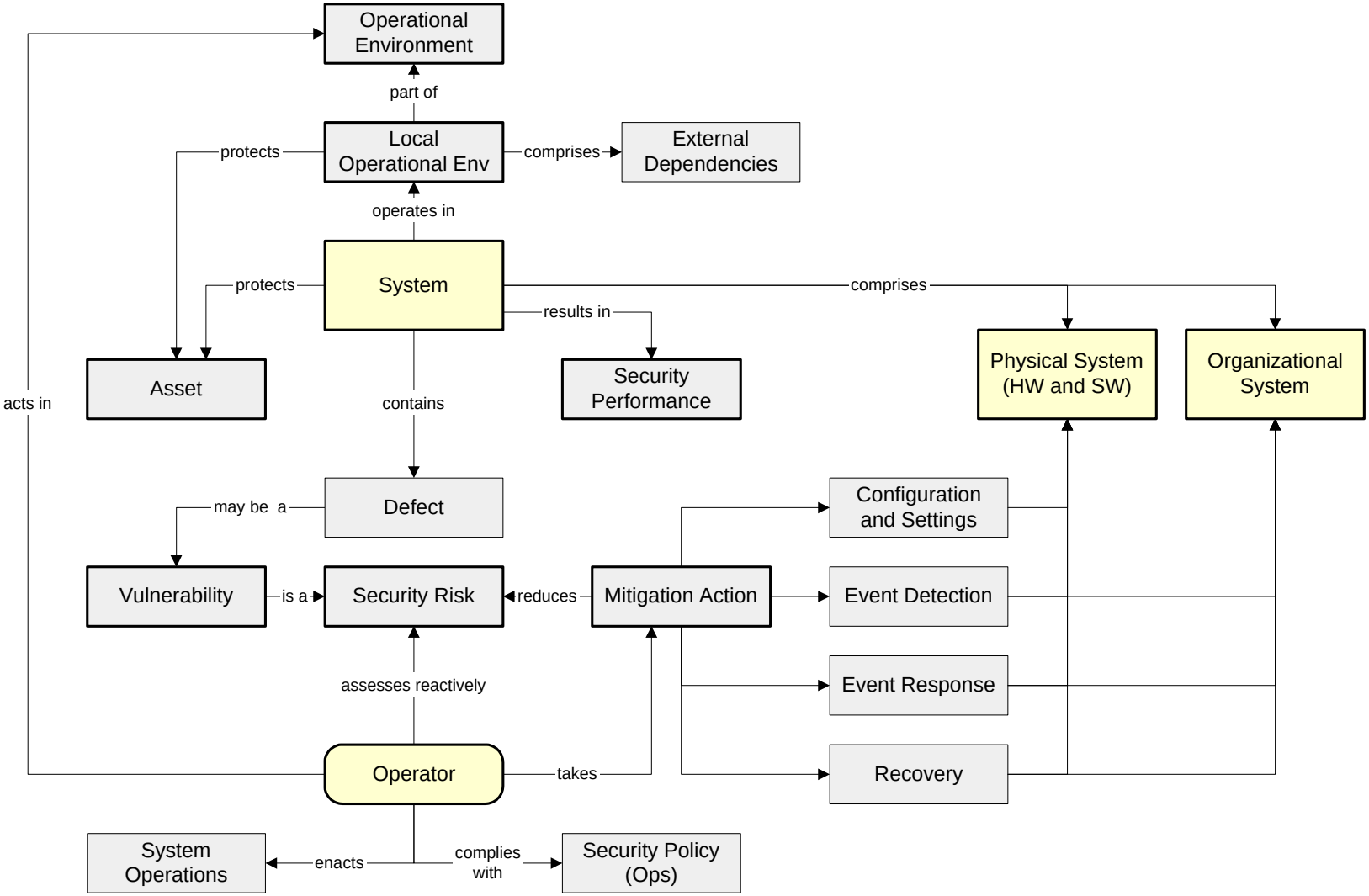


Figure 19 Operator role as the source of mitigation actions during system operations

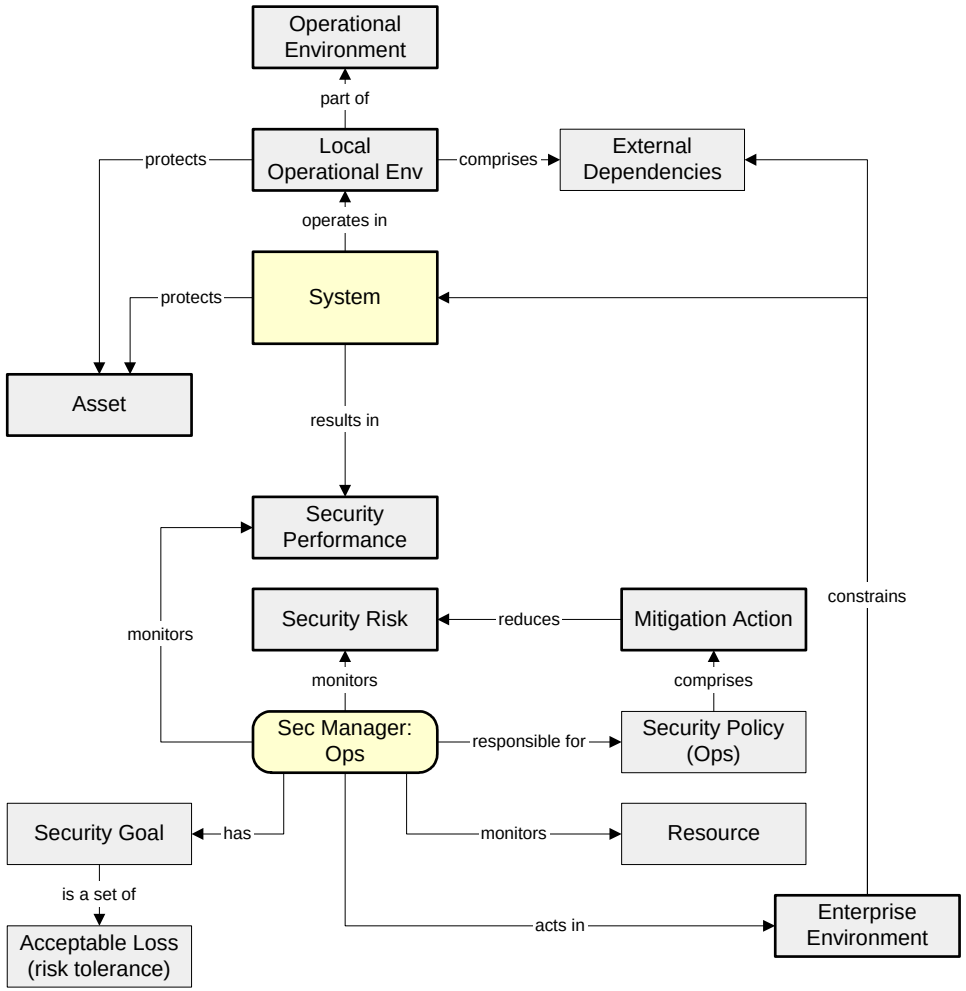


Figure 20 Security Manager (operations) role as a monitor of security performance, compliance and residual risk

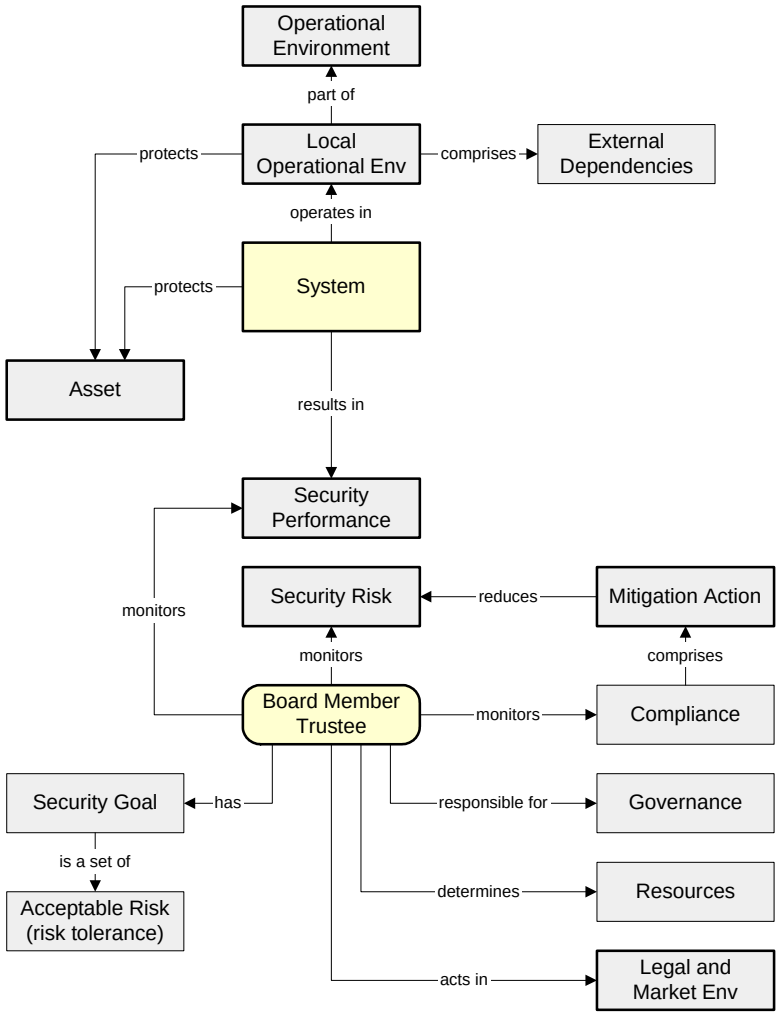


Figure 21 Board Member/Trustee role as a monitor of security performance, governance and residual risk

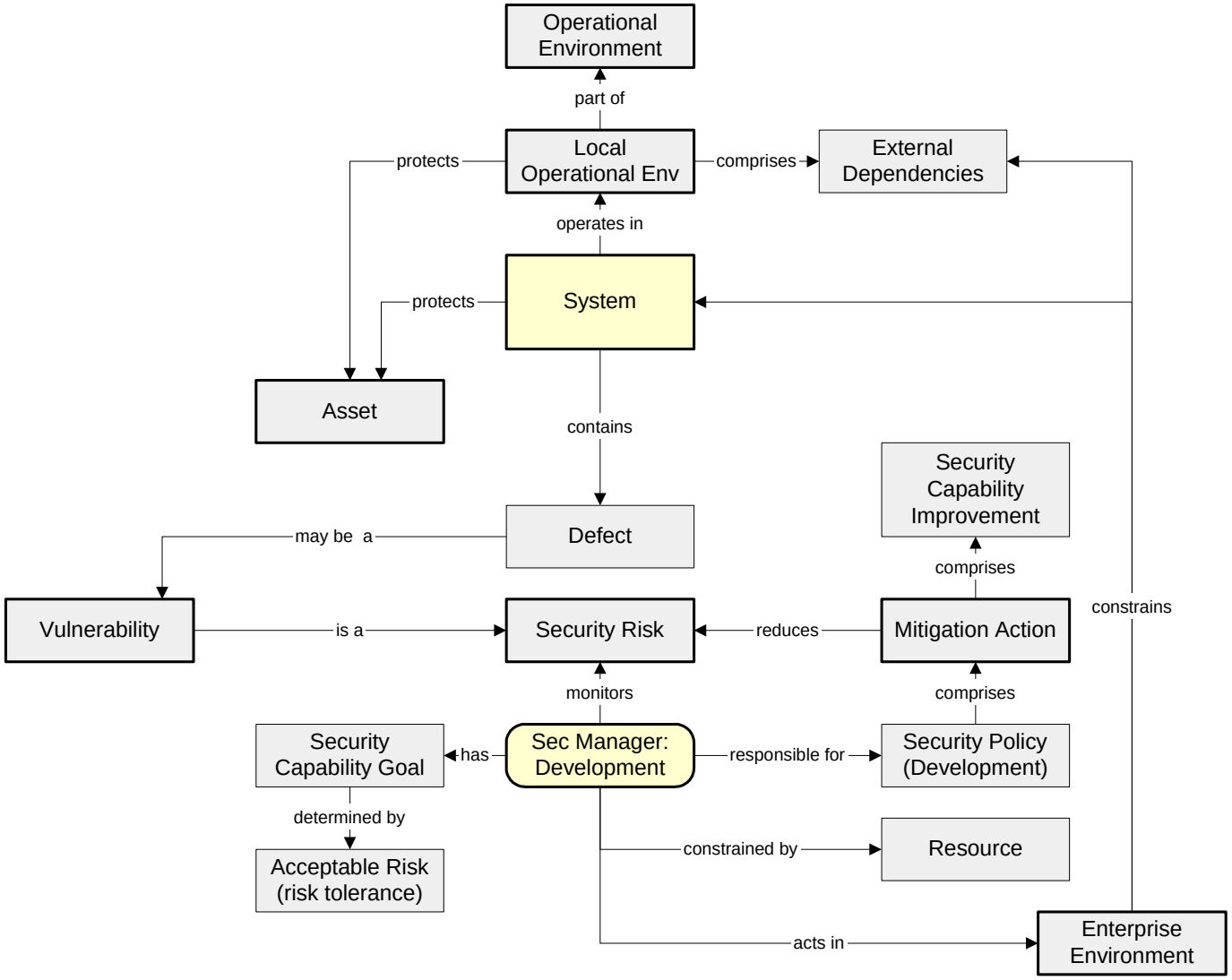


Figure 22 Security Manager (Development) role as a monitor of assessed security and resource usage

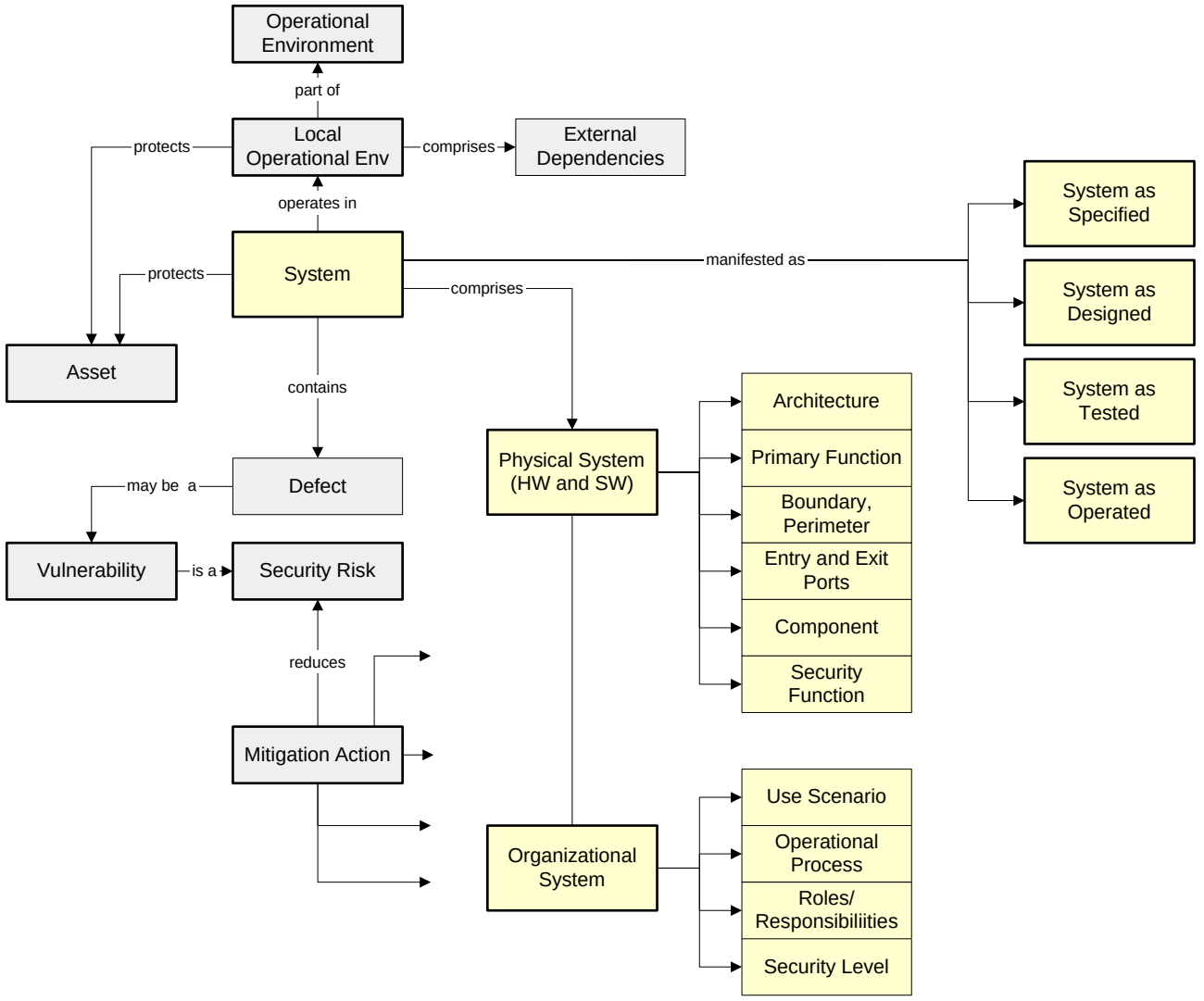


Figure 23 System physical and organizational decomposition; also as represented in different development phases

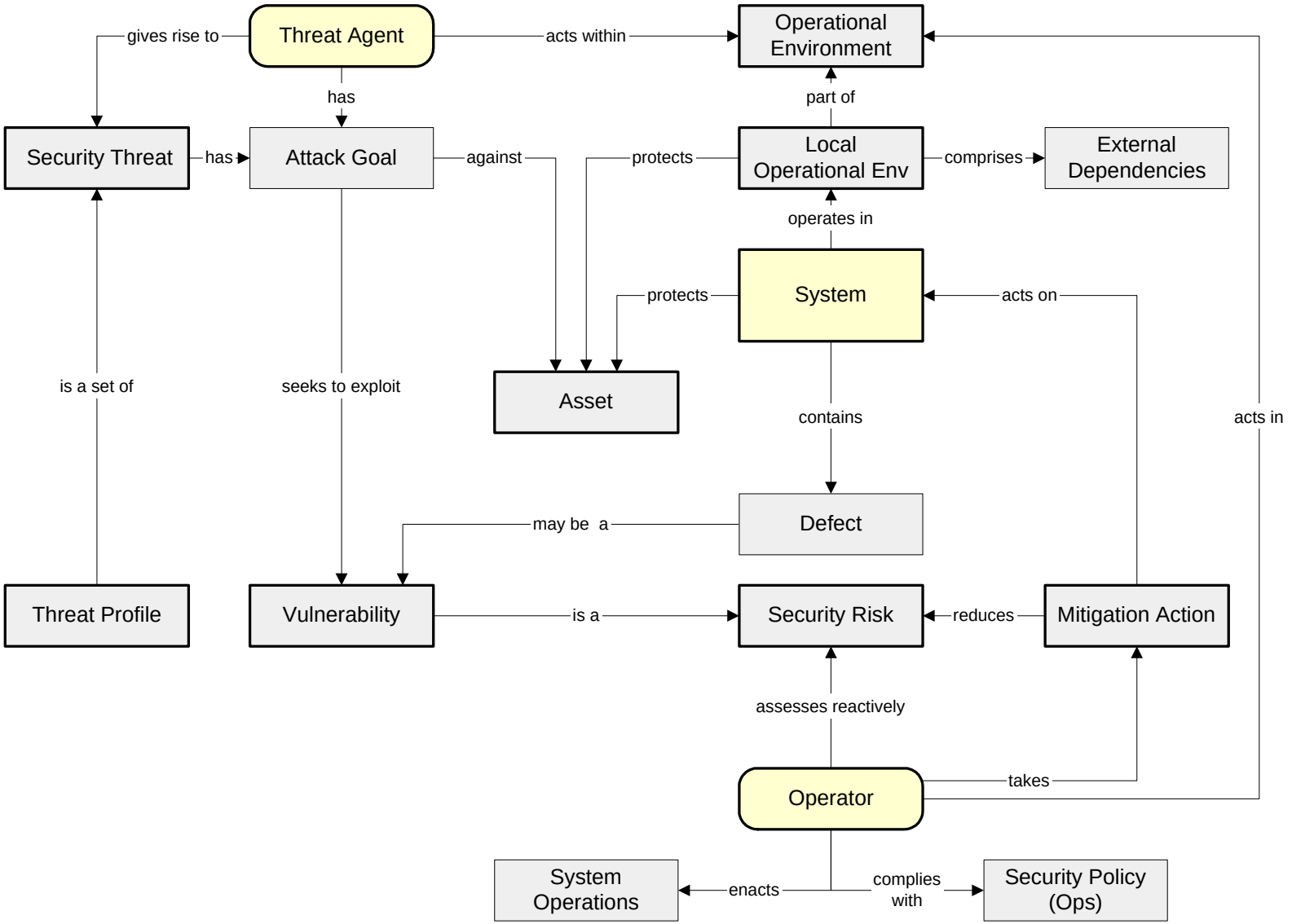


Figure 24 Interaction between Threat Agent and Operator roles

Appendix 4 Security Risk

The concept of risk carries different meanings in different professional communities. Project managers define risk traditionally as:

> An uncertain event or condition that, if it occurs, has a positive or negative effect on a project objective [24]
>
> An uncertain event or set of circumstances that, should it occur, will have an effect on the achievement of the project's objectives [25].

Some writers argue that project risk should be defined as an *uncertain effect* on a project's performance, rather than as a *cause* of an uncertain effect, as implied by the above. More specifically, in this view, risk is defined as [26]:

> the implications of uncertainty about the level of performance achievable by a project.

The advantage of this approach is that it opens up a wider range of issues as potential sources of uncertainty; events, conditions and sets of circumstances are viewed as subsets of the potential sources.

This second approach is more in line with the definition of risk used in the financial investment community. Risk is defined as:

> the downside variability of the level of performance achievable relative to expected outcome. [Markowitz 1959, quoted in [26].

This concept plays a key role in the mean variance approach to portfolio investment. Many project management decisions can be viewed in similar terms; good decisions lead to (1) expected performance outcomes that meet specifications and (2) variances of performances around the expected values that are acceptably small. Risk is associated with the variances, rather than the expected performances themselves.

The safety engineering community defines safety risk as [27]:

> A combination of the frequency or probability of a specified hazardous event, and its consequence.

Risks are classified in terms of severity, determined by assessed likelihood and consequences. The acceptability of a safety risk is judged with reference to the benefits provided by the system and the costs associated with risk reduction. The ALARP Principle (*As Low As Reasonably Practicable*) [28] is an example decision framework. Government agencies are often involved in such judgments. Insurance companies view such risks are *pure* risks, to distinguish them from the speculative risks borne by investors.

It follows that safety risk is associated with an expected performance level of a system (as experienced by those exposed to the risks). The variance around that expectation would be an

additional source of safety risk. A developer or operator may not view the expected performance level as a financial risk, if insurance and other provisions have been made.

It has been argued [26] that safety risk assessment would be refined by recognizing the uncertainty in both the likelihood and the consequence components of safety risk. Single figure estimates would be replaced by probability distributions.

Security risk is defined like safety risk:

> A combination of the frequency or probability of a specified security event, and its consequence.

A security-critical system may be designed and operated to achieve a specified level of expected security performance, with a variance. For the service provider, financial risk would be associated only with the variance, provided appropriate contingencies have been made to cover the consequences of expected performance. This implies that consequences of expected security events are bearable. For the service user, the planned system performance (expectation and variance) would involve exposure to a level of security risk. The user's security risk may also be translated into financial terms. The user's trade-off would be that the benefits arising from using the services outweigh the risks involved. The user of the system is not an investor in it, merely a purchaser of offered services, with no wish to be exposed to risks. Risks are considered acceptable provided they are as low as reasonably practicable, given the price of the service. Legal systems provide the ultimate test of risk interpretations where disputes arise.

For system developers and operators, security risks have characteristics that seem to challenge traditional management practices:

1. some security threats may be *learning* (or opportunistic) agents. The possibility that threats may change over time seems to be the main challenge (the degree of malicious intent is, arguably, a secondary issue). A dynamic threat environment is difficult to predict and plan for. This leads to more emphasis on continuous, adaptive management, to maintain established security performance;
2. the components and systems infrastructure of security systems must nevertheless be developed and deployed, i.e. subject to traditional project processes. Design and implementation commitments have to be made to enable infra-structural systems to be realized. The basic challenge seems to be to enable such commitments to be made while keeping an eye on the provision of adaptive security functionality at operations level. Software components enable adaptation (modification of earlier commitments), but at cost and risk, and not in all situations;
3. vulnerabilities in some systems are discovered during operations, possibly as a result of successful intrusions etc., resulting in a dynamic, responsive characteristic in vulnerability management;
4. there is large scope for security countermeasures, especially in the information systems domain. This has led to standardization of security requirements, functions and evaluation criteria in the IT products and systems sector (Common Criteria);
5. the damage arising from failures in security can take a variety of forms; information-related damages may not be local to the managed system in time or space;
6. because threats are often human agents, socio-technical considerations play a part.

It has been proposed [29] to view assurance as the degree of confidence in a risk assessment, i.e. the variance around an expected security or safety risk. This approach is useful because it

recognizes the trade-off that might be available between spending resources on risk reduction and on reducing uncertainty.

The following are tentative proposals / concepts for informing decision makers about security risks.

Justification of Security Investment based on Outcome Observability

A difficulty with all preventative actions (also in the safety domain) is that the successful outcome is a null result – no problems arise. Skeptics will always question the need for investment that does not seem to have any tangible outcome.

A concept called the *observability* of a performance outcome is proposed to tackle this problem.

Suppose the security manager is working to reduce the number of unauthorized, successful accesses per week to an information system. A change in procedures is introduced that increases costs but is successful in reducing the rate of unauthorized accesses. The outcome is observable and understandable to senior managers (who sign the checks) and the investment is recognised as successful.

Now suppose the security manager is aware that some of those who gain access to the IS are attempting to make money transfers that are potentially very damaging to the organization. None has yet been successful. The security manager introduces an additional firewall and reduces the associated security risk. But the *observable* measurable performance outcome is unchanged, as far as the senior manager is concerned.

To justify the investment, the security manager needs two things: (1) objective observable measures that change when the security action is taken and (2) an understandable and convincing model that causally connects the observables with security performance outcomes.

This approach calls for the development of observable performance measurements as part of introducing a change.

Generalizing this concept, we can imagine a set of increasingly 'deep' observables, that require increasingly sophisticated models that link them to end performances. We obtain a spectrum of measurements that link surface measures, close to the desired performance of a system (and deemed objective by the external observer) with deep ones, based on observables distant from the external performance (and deemed subjective by an external observer, unless the causal models are agreed upon). This concept is linked to the role of models in the cognition of learning agents.

For very high-risk events (more common in the safety domain), observable performances are more difficult to find. Near misses and similar events are very important.

Black Box and White Box Risk

Risk assessment based on externally observed performance might be called ' black box' risk assessment, by analogy with black box testing. Risk assessment based on 'internal' measures and causal models would be called 'white box' risk assessment.

Risk Flow Account

Safety processes tend to adopt a once and for all approach (or at least have traditionally) to risk assessment; present a safety case, achieve certification, then operate. The safety case or safety argument is effectively a static distribution of risk, rather like a balance sheet in financial accounting. However, security involves the handling of new risks (threats) and learning behaviors, generating risk exposures and costs for different parties. We could treat the security case as a 'risk balance sheet' – an aggregated risk distribution at a point in time. This could be augmented with a *risk flow account* to show the new risks and mitigation actions undertaken over a period of time.

Safety and Security Risk Compared

Security engineering is a type of *risk management*, and this is the main characteristic shared with safety engineering. Security engineering seeks to reduce the likelihood of future security incidents and the severity of their consequences should they occur. A range of security analytic techniques and risk reduction strategies are deployed to achieve this. The current performance of a system, in terms of security incidents reported, is monitored and used as an input to future strategies. Measures of risk (future performance in terms of likelihood of occurrence and effects) and past-achieved performance are the core measures of security. There are similarities with safety engineering, but also differences of emphasis.

Safety engineering is mainly concerned with hazards arising from weaknesses in the system design, development and operation. Issues external to the system are considered, including environmental effects and exposure times, but these are viewed as relatively static. The main concerns tend to focus on failure scenarios that start with component failures within the system and lead relatively rapidly (i.e. uncontrollably) to accidents, for given operational contexts. The traditional approach has placed emphasis on developing a safe product, having it certified as acceptably safe for operation, and then operating it within defined constraints. Current trends are moving towards a more through-life approach in which a Safety Management System, used in the development phase of a system, is transferred to an operational support role, providing continuous learning and improvement of safety performance.

Security engineering has to deal with a more dynamic threat environment and this affects the risk management approach in two ways:

1. The harmful effects of a security incident may be felt across a range of different timescales and remote from the site of the security incident;
2. Threats evolve in time; concerns are dominated by threat agents that learn and adapt to system vulnerabilities (c.f. the relatively static environmental threats to system safety).

There is greater emphasis on real time response to newly emerging threats. At the large system (and networked systems) end of the scale, predictive analyses, although an important part of planning, cannot be expected to provide for every security risk. The systems involved are too complex and the threat environment changes too rapidly. Managing in this environment requires feedback and resources to respond to unfolding events. These are also the characteristics of *high reliability organizations*, as explored by [30].

The challenge seems to be to commit to security design features that result in systems that are operationally feasible. The concept of a *local security environment* for an entity seems important in this regard; it enables an entity to be designed to a fixed threat specification, while placing responsibility on other parts of the system (and on operations) to maintain the local environment.

Appendix 5 Representative Practices

CISWG Report

The CISWG study [4] identified the following governance issues and indicators at Board/Trustee level for Information Security (similar responsibilities would be expected for product development organizations, at this level):

1. **Oversee Risk Management and Compliance Programs Pertaining to Information Security (e.g. Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley);**
   - 1.1 Percentage of key information assets for which a comprehensive strategy has been implemented to mitigate information security risks as necessary and to maintain these risks within acceptable thresholds
   - 1.2 Percentage of key organizational functions for which a comprehensive strategy has been implemented to mitigate information security risks as necessary and to maintain these risks within acceptable thresholds
   - 1.3 Percentage of key external requirements for which the organization has been deemed by objective audit or other means to be in compliance

2. **Approve and Adopt Broad Information Security Program Principles and Approve Assignment of Key Managers Responsible for Information Security;**
   - 2.1 Percentage of Information Security Program Principles for which approved policies and controls have been implemented by management
   - 2.1 Percentage of key information security management roles for which responsibilities, accountabilities, and authority are assigned and required skills identified

3. **Strive to Protect the Interests of all Stakeholders Dependent on Information Security;**
   - 3.1 Percentage of board meetings and/or designated committee meetings for which information security is on the agenda;
   - 3.2 Percentage of security incidents did not that cause damage, compromise, or loss beyond established thresholds to the organization's assets, functions, or stakeholders;
   - 3.3 Estimated damage or loss in dollars resulting from all security incidents.

4. **Review Information Security Policies Regarding Strategic Partners and Other Third-parties;**
   - 4.1 Percentage of strategic partner and other third-party relationships for which information security requirements have been implemented in the agreements with these parties

5. **Strive to Ensure Business Continuity;**
   - 5.1 Percentage of organizational units with an established business continuity plan

6. **Review Provisions for Internal and External Audits of the Information Security Program;**
   - 6.1 Percentage of required internal and external audits completed and reviewed by the Board
   - 6.2 Percentage of audit findings that have been resolved

7. Collaborate with Management to Specify the Information Security Metrics to be Reported to the Board.

The CISWG study identifies the following responsibilities in the management of general information security:

1. Establish Information Security Management Policies and Controls and Monitor Compliance;
2. Assign Information Security Roles, Responsibilities, Required Skills, and Enforce Role-based Information Access Privileges;
3. Assess Information Risks, Establish Risk Thresholds and Actively Manage Risk Mitigation;
4. Ensure Implementation of Information Security Requirements for Strategic Partners and Other Third-parties;
5. Identify and Classify Information Assets;
6. Implement and Test Business Continuity Plans;
7. Approve Information Systems Architecture during Acquisition, Development, Operations, and Maintenance;
8. Protect the Physical Environment;
9. Ensure Internal and External Audits of the Information Security Program with Timely Follow-up;
10. Collaborate with Security Staff to Specify the Information Security Metrics to be Reported to Management

Some 39 metrics are recommended under these headings, mainly monitoring compliance with the security policy, for example:

1. Establish Information Security Management Policies and Controls and Monitor Compliance

1.1 Percentage of Information Security Program Elements for which approved policies and controls are currently operational

1.2 Percentage of staff assigned responsibilities for information security policies and controls who have acknowledged accountability for their responsibilities in connection with those policies and controls

1.3 Percentage of information security policy compliance reviews with no violations noted

1.4 Percentage of business unit heads and senior managers who have implemented operational procedures to ensure compliance with approved information security policies and controls

3. Assess Information Risks, Establish Risk Thresholds and Actively Manage Risk Mitigation

3.1 Percentage of critical information assets and information-dependent functions for which some form of risk assessment has been performed and documented as required by policy

3.2 Percentage of critical assets and functions for which the cost of compromise (loss, damage, disclosure, disruption in access to) has been quantified

3.3 Percentage of identified risks that have a defined risk mitigation plan against which status is reported in accordance with policy

The CISWG study lists the following elements of an information security program, at technical level:

1. User Identification and Authentication
2. User Account Management
3. User Privileges
4. Configuration Management
5. Event and Activity Logging and Monitoring

6. Communications, Email, and Remote Access Security
7. Malicious Code Protection
8. Software Change Management, including Patching
9. Firewalls
10. Data Encryption
11. Backup and Recovery
12. Incident and Vulnerability Detection and Response
13. Collaborate with Management to Specify the Technical Metrics to be Reported to Management

These responsibilities are mainly concerned with the appropriate exploitation of technical features existing in commercially available IT systems. The security policy is implemented as a set of decisions on how to deploy these security controls (e.g. automatic logging off of users after a selected idle time.)

The recommended metrics generally reflect this orientation, for example:

1. User Identification and Authentication

1.1. Number of active user IDs assigned to only one person
1.2. Percentage of systems and applications that perform password policy verification
1.3. Percentage of active user passwords that are set to expire in accordance with policy
1.4. Percentage of systems with critical information assets that use stronger authentication than IDs and passwords in accordance with policy

This approach can be characterized as the decomposition of the security policy into sets of organizational procedures and actions on the IT infrastructure of the organization.

Return on Security Investment Calculation

Traditional ROI calculations can be applied to security investments: the following table reflects the approach of [15].

Total
Asset Value (AV) of an information asset =
Cost of replacing information
\+ cost of replacing sw, hw
\+ cost of reconfiguration
\+ cost of loss of availability
\+ associated costs (loss of data confidentiality and integrity)

Exposure Factor (EF) of asset = fraction of asset value removed by a particular attack

Single Loss Expectancy (SLE) = financial loss expected from a successful attack
= AV x EF

Probability of an attack of a particular type in a one year period =
Pr(attack)

Annual Loss Expectancy (ALE) = SLE x Pr(attack)

Net Present Value of a security appliance that stops the annual losses =
discounted ALE over selected number of years

Total Cost of Ownership (TCO) of a security appliance =

procurement cost
+ non-recurring costs
+ discounted recurring costs

Return on Investment in security appliance =

(NPV of avoiding losses – NPV TCO) / (NPV TCO)

Table 5 Traditional ROI calculation based on discounted cash flows, from [15]

ISO/IEC 15408 Common Criteria

The Common Criteria (now established as ISO/IEC 15408 [14]) provide a framework for the independent evaluation of the security performance of IT products and systems. The evaluation process involves:

1. the identification of security objectives and requirements, constituting a *Security Target* (ST);
2. the optional use of a standard *Protection Profile* (PP), representing typical sets of security functions;
3. the identification of a *Target of Evaluation (*TOE);
4. the evaluation of the TOE against the PP and security requirements;
5. several evaluation levels (EAL 1 through EAL 7), providing different levels of evaluation rigor, and therefore confidence in the performance.

The Common Criteria (CC) approach provides a means for a system developer to establish assurance that a product or system meets identified security performance standards. Security risk is reduced by assessment against internationally agreed performance standards. The CC framework is built around catalogs of PPs and evaluated products. Extended requirements and evaluation criteria, not in the standard models, can be included.

The CC approach has been used as a guide in developing the proposed PSM model – particularly the concept of integrating assured components into assured systems. Certified components and systems may still contain vulnerabilities, so additional security risk management would remain necessary. Defense systems may require stronger assurance techniques than 'standard' commercial IT applications. A security process following a CC approach would present measurable artifacts and attributes (e.g. scope and progress of assurance activities, costs, security risk reductions and improvements in confidence intervals of these). The assurance activity is itself a form of measurement.

Security Process Maturity: ISO/IEC 21827 SSE-CMM

The SSE-CMM [12] includes eleven Process Areas specifically associated with system security engineering:

PA01 Administer Security Controls
PA02 Assess Impact
PA03 Assess Security Risk

PA04 Assess Threat
PA05 Assess Vulnerability
PA06 Build Assurance Argument
PA07 Coordinate Security
PA08 Monitor Security Posture
PA09 Provide Security Input
PA10 Specify Security Needs
PA11 Verify and Validate Security

There are similarities with the four sub-domains proposed in the PSM model; differences reflect different choices about how to group activities.

> Further Development
> Check the suitability of the proposed security measurement model against the SSM-CMM (ISO/IEC 21827) process areas.

Safety and Security Extensions to the iCMM and CMMI Models

Safety and security extensions to the iCMM and CMMI models have been published recently [9]. A *Safety and Security Application Area* (AA) has been introduced that identifies goals and standards-based *Application Practices* (APs) directed at establishing and maintaining a safety and security capability, define and manage requirements based on risks attributable to threats, hazards, and vulnerabilities, and assure that products and services are safe and secure throughout their life cycle. Goals and practices of the application area are:

Goal 1 An infrastructure for safety and security is established and maintained
AP 01.01 Ensure Safety and Security Competency
AP 01.02 Establish Qualified Work Environment
AP 01.03 Ensure Integrity of Safety and Security Information
AP 01.04 Monitor Operations and Report Incidents
AP 01.05 Ensure Business Continuity

Goal 2 Safety and security risks are identified and managed
AP 01.06 Identify Safety and Security Risks
AP 01.07 Analyze and Prioritize Risks
AP 01.08 Determine, Implement, and Monitor Risk Mitigation Plan

Goal 3 Safety and security requirements are satisfied
AP 01.09 Determine Regulatory Requirements, Laws, and Standards
AP 01.10 Develop and Deploy Safe and Secure Products and Services
AP 01.11 Objectively Evaluate Products
AP 01.12 Establish Safety and Security Assurance Arguments

Goal 4 Activities and products are managed to achieve safety and security requirements and objectives
AP 01.13 Establish Independent Safety and Security Reporting
AP 01.14 Establish a Safety and Security Plan
AP 01.15 Select and Manage Suppliers, Products, and Services
AP 01.16 Monitor and Control Activities and Products

The proposed measurement framework is broadly compatible with the recommendations of the Application Areas. For example, AP 01.06, 07 and 08 place risk assessment at the center of safety and security practice, as does the proposed measurement framework. AP 01.11 involves the objective evaluation of products, covered by the *assurance* and *performance* measurements of the proposed framework. The concept of a 'managed domain' proposed in this paper is similar to an *Application Area*, or a set of *Application Practices*.

> Further Development
> Check the compatibility of the proposed measurement approach with the Safety & Security extensions of the iCMM/CMMI model.

An intention of the *managed domain* concept is that it should make minimum assumptions about how work is organized. One aspect of security and safety performance relates to awareness and flexibility of response. It is assumed that these aspects are addressed in a managed domain by having resources deployed that can respond to unexpected events. The classic process maturity view is appropriate when processes are repeatable and attention can be directed towards evolutionary improvements in efficiency. A managed domain may then be treated mainly as a process or set of processes.

ISO/IEC 17799 Information Security

Widespread concerns about the security of general business IT systems has resulted in the development of standards in this field [31]. *Information security* is defined as the preservation of confidentiality, integrity and availability of information:

- *Confidentiality*; Ensuring that information is accessible only to those authorized to have access;
- *Integrity*; Safeguarding the accuracy and completeness of information and processing methods;
- *Availability*; Ensuring that authorized users have access to information and associated assets when required.

ISO/IEC 17799 provides a code of practice for information security management under the following headings:

- Security Policy
- Organizational Security
- Asset Classification And Control
- Personnel Security
- Physical And Environmental Security
- Communications And Operations Management
- Access Control
- Systems Development And Maintenance
- Business Continuity Management
- Compliance

The ISO standard views security requirements as arising from three sources:

1. assessment of risks to the organization;
2. legal, statutory, regulatory and contractual requirements;
3. particular set of principles, objectives and requirements for information processing that an organization has developed to support its operations.

Security risks are reduced by the implementation of *security controls* (types of action, as defined in this paper).

An associated standard, BS 7799-2:2002 *Information security management systems - Specification with guidance for use* [32] is directed at business managers and defines the concept of an *Information Security Management System* (ISMS). A process-based approach for establishing, implementing, operating, monitoring, maintaining and improving the effectiveness of an ISMS is described. This standard uses the PDCA cycle [33] as a reference for the management of the ISMS. This concept has been adapted for the proposed model.

NIST has developed measurement guidance with reference to security program maturity in the IT domain [34].

It is intended that the proposed measurement approach is compatible with these standards. Their main limitation is that they do not engage with the development or operation of secure systems at detailed technical levels. An objective of the proposed measurement approach is to achieve 'vertical integration' between technical risk assessment and management decision-making.

ACSA Workshop

A workshop held in 2001[31] on the assessment of information system security developed the concept of an *information security* {*metric, measure, score etc*} (IS*). Quoting from the Proceedings:

> An IS* is a value, selected from a partially ordered set by some assessment process, that represents an IS-related quality of some object of concern. It provides, or is used to create, a description, prediction, or comparison, with some degree of confidence.
>
> The expression *information security (IS)** was used in the workshop agenda to avoid long discussions on terminology. The asterisk (*) was used to mean any of the following terms: metric, measure, score, rating, rank, or assessment result (although not necessarily an exhaustive list).

The workshop described a IS* as being formed from a combination of:

1. type of object (technical, process, organization, system) – WHAT you need to measure;
2. purpose (description, comparison, prediction) – WHY you need to measure it and;
3. intended audience (technical expert, decision makers at various organizational levels, external authorities, policymakers) – WHO you are measuring it for.

The proposed model has been informed by this work, but further review is required.

Costing Secure Systems Project

An ongoing project is developing security extensions to the COCOMO II cost estimation model. A number of system parameters have been identified [11] as drivers of security costs. Improved data collection of the costs incurred in the development and operation of secure systems and the resulting performances should enable growth in the accuracy of parametric models.

Further Development
Develop mappings between parameters used in the parametric cost models and measurable concepts, as developed for technical management purposes. Connect estimation parameters with experience accumulated in measurement systems.

Check Lists

Several agencies and organizations publish checklists to aid in the development and operation of security-critical systems. Examples include checklists from the Federal Systems (http://csrc.nist.gov/pcig/cig.html) and the Defense Information Security Agency (DISA) [35]. Checklists may be used to assess security functions. For example, an *Identification and Authentication* function may be checked against:

Identification and Authentication (I&A)	
APP0120:	The application is not PK-enabled
APP0125:	The application utilizes a PKI other than DOD PKI
APP0130:	The application honors invalid certificates
APP0140:	An application user or client authentication process is inadequate.
APP0160:	The application does not enable an application client to authenticate the application server with which it communicates
User Account Management	
APP0210:	Application user IDs are not unique
APP0220:	Inactive user IDs are not disabled
APP0230:	Unnecessary built-in user IDs are not disabled

Risk Management Tools

Risk management tools include [19]:

1. CRAMM
2. FIRM
3. SARA and SPRINT
4. COBRA
5. OCTAVE [36]

Tracking Particular Security Risks

The proposed measurement approach includes the concept of performance and risk tracking systems in each of the four sub-domains identified, combined with tracking of integrated performances and risks. The following are applicable to each sub-domain:

1. counts of identified risks in risk tracking systems and their time-evolving status ('rows' in the tracking systems);
2. measurements associated with performance observables in performance tracking systems;

3. resources deployed and progress of actions;
4. scopes of plans, risks and awareness;
5. outputs of tasks;
6. outcomes of tasks risk management and performance;
7. assurance task progress, costs;
8. competence deployed.

The use of tracking systems, analogous to the *Hazard Tracking System* used in safety engineering [3], and risk tracking systems used in project risk management, seems an obvious approach.

Threat Environment Management

This view of security involves measurement and actions within the entity environment and the triggering of actions in the other sub-domains. Actions available in the environment would depend on the type of entity involved. For publicly accessible IT systems, actions might be directed at reducing motivation and monitoring usage. Defense systems operate under wider permitted ranges of action. There is a link with *Damage Management* in the area of recovering damages, for example, by using legal systems. Some threats (e.g. natural threats) are internal to the entity and have similarity with safety concerns.

The monitoring and assessment of attackers is the principal role, enabling responses to be made in system design and operation. During the development phase, emphasis is on predictive assessment to inform design commitments. During operations, emphasis is on rapid detection and response within the 'space' created by the designs.

A Threat Tracking or Management System would enable counts of numbers of actual and potential attackers in different categories and the status of actions that have been triggered by them. Examples of categories include:

1. Potential/ actual status; success of attacker (in penetrating the security assets, deriving benefit, causing damage);
2. Capability of threat agent;
3. Intention of threat agent;
4. Numbers of potential attackers in each type;
5. Priority indicator, based on risk (involves other sub-domains);
6. Scope of threat (in terms of parts of system attacked, identified vulnerabilities);
7. Number of threat vectors in a threat type; (e.g. ADDER score [20])
8. Time rates of appearance and capability/ learning rates.

Table 6 shows example sketches of tracked counts of threats, vulnerabilities and events.

Vulnerability Management

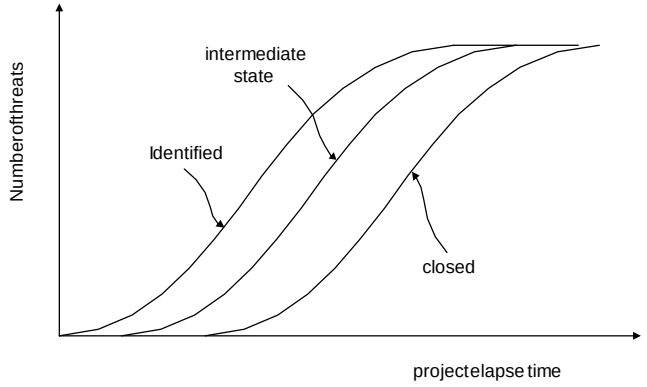
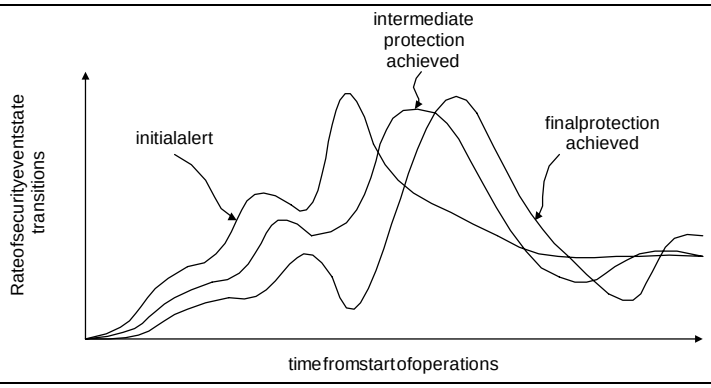
This view of security involves actions within the entity itself, including both entity design and operations/ policy actions. The designs and policies influence and constrain the actions available in the Event and Damage sub-domains.

Many different kinds of action are possible, depending on the type of entity involved, and whether the context is a development project or an operational system/ organization. The actions

of this sub-domain are generally preventative (pro-active) in nature, in terms of the delivery of security. For 'standard' IT product and systems, well-recognized countermeasures to known kinds of attack have been developed. The Common Criteria approach provides an internationally recognized process for independently evaluating the assurance of IT products and systems against standard security functions. Such an approach enables a market in evaluated standard security function products. Assurance levels provide confidence in the security performance of products and systems and are one way to reduce risk. Other kinds of non-standard system will require more specific analyses and assurances.

Some applications have well-developed approaches to vulnerability management. For example, a Vulnerability Management System (VMS) is described as assigning one of four severity categories to a *Potential Discrepancy Item*:

- Category I findings are any vulnerability that provide an attacker immediate access into a machine, gain super-user access, or bypass a firewall;
- Category II findings are any vulnerability that provides information that has a high potential of giving access to an intruder;
- Category III findings are any vulnerability that provides information that potentially could lead to compromise;
- Category IV vulnerabilities, when resolved, will prevent the possibility of degraded security.

Measure	Tracking
Identified threats to an entity; plot of number of threats against project elapse time. Threats are managed in terms of initial detection, intermediate protection and final closure. Applicable to development phase; number of threats levels off at a maximum, representing all envisaged threats. Separate charts for threats of different severities. Similar charts would be used for high-priority vulnerabilities.	
Rate of security event state transitions during operations phase. Rates of initial detection, intermediate protection and closure should be equal, asymptotically. Areas under curves should be equal.	

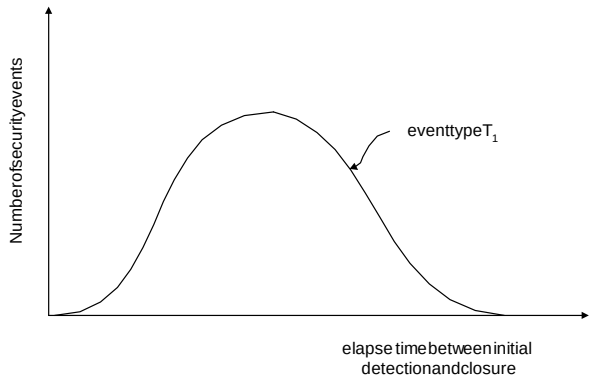
Statistical data – time to 'process' security events i.e. elapse time between initial detection and closure, for many events of type T_1.	

Table 6 Example tracking of security threats and events

A Vulnerability Tracking System would enable counts of numbers of identified vulnerabilities in different categories and the status of risk mitigation actions triggered by them. A vulnerability being managed by a Common Criteria approach would be tracked with reference to a management system tailored to the tasks involved.

Many techniques and technologies are involved in removing vulnerabilities and reducing associated security risk. Examples in the software security domain include:

1. Language-based security
2. Operating Systems Security
3. Secure Middleware
4. Malicious Code Detection
5. Intrusion Tolerance
6. Trust Management
7. Program Analysis

Vulnerabilities in an entity are reduced by two means: (1) application of known best practice methods, tools etc., based on shared domain understanding and (2) identification of particular vulnerabilities for the entity of concern. Explicit identification and tracking of vulnerabilities is directed at the second of these.

Security Event Management

This view of security involves actions that respond to attack events (and actions that prepare for them). The detection and annunciation (signaling) of events is included in this view. Security functions of interest in this sub-domain are those that involve fast response to events. Actions arising in this sub-domain include preventative / pro-active and reactive actions.

Security Event Tracking provides a source of objective performance measurement. The form of security event will vary depending on the type of entity involved. Many events will be of in the form of an attack scenario; a successful intrusion will involve a sequence of states or conditions, some of which might be observable.

The actions taken in response to security events are also measurable.

A security event may be modeled as a multi-stage scenario (Figure 25); this can comprise deterministic and probabilistic steps. Measurements may be available to detect the transition of an entity or threat agent to an intermediate state i.e. a state prior to a successful intrusion or an occurrence visible to an end-user. Such observable events enable assessment of security performance and risk reduction based on objective data, but without necessarily incurring actual security breaches. Probability tree representations support the use of event detection to revise risk assessments. Security actions triggered by such measurements can be represented as modifications to event trees.

> Further Development
> Explore use of probability trees in the dynamic re-assessment of risk following security events.

Damage Management

This view of security involves actions that respond to damage arising from attack events (and actions that prepare for managing damage). This domain also covers potential damage assessment for the purposes of assessing the value of the security entities. Also of interest is the design of systems and policies (e.g. interfaces, boundaries, role/responsibilities) that can reduce the risk of damage propagation, given an intrusion. Damage effects may not lie exclusively within the fields of action and measurement of the other security sub-domains, depending on the type of entity involved.

A Damage Tracking System would enable the recording of the effects of successful attacks, responses to them and the achieved outcomes. The damage sustained by a system or organization arising from security attacks, whether intentional, opportunistic or accidental, is the final objective test of the success of investments in security.

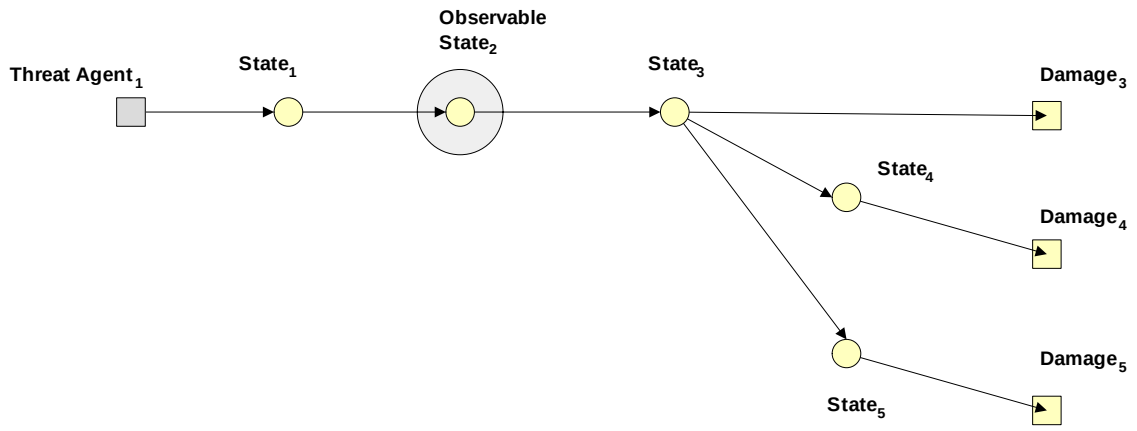


Figure 25 Security event scenario comprising five states. State 2 is observable

Appendix 6 Security Management – Learning Loop Models

The uncertainties involved in security assessment and the fact that threat agents learn and evolve over time, has resulted in security processes being viewed as 'living' systems. We cannot plan everything ahead of time and then execute; the future is insufficiently predictable. We cannot assume that threat profiles and vulnerabilities will remain static. Most security management frameworks include a closed-loop learning cycle [32], [15]. The Capability Maturity Models are based on a continuous learning concept at process level, directed mainly at continuous process improvement in repeatability and efficiency terms.

Need to augment 'static' models with needs-driven learning and adaptation to evolving threats.

This section proposes a 'control loop' model that represents the distribution of security learning across different parts and levels of a system. The objective is to extend the loop model of ISO/IEC 17799 into a form more suited to a net-centric, distributed environment.

The learning in this case is about threat agents and the vulnerabilities in the systems for which we are responsible. This may involve increased costs and doing new things.

Tracking and responding to changing threats requires an adaptive, *learning* view of security engineering and operations. Figure 26 shows a control loop model at the three levels of system security management, organization management and board/trustee level management. The management of particular security risks is associated with a short cycle-time, inner 'control' loop. The learning arising from this activity informs the development of good practice models and planning that subsequent actions are expected to comply with. This model maps onto the classic PDCA cycle [33] that is used in [22].

The control loop model is similar to the measurement 'learning loop' of PSM and ISO/IEC 15939 [2]. However, the PSM 15939 model assumes loose coupling between the processes that generate information needs (viewed as external financial and risk management processes) and the measurement process. The generation of information needs and associated actions are externalized, as far as the measurement process is concerned. The proposed model brings the identification of needs and management action into the learning loop, implying a tighter coupling between measurement and action. The need for this arises from the dynamic nature of security management and the fact that security is a specialized form of risk management.

This model places the assessment of 'particular' risks at the heart of security management. The four areas of security risk (threat, vulnerability, event, damage) are each sufficiently rich to be treated as a separately managed and measured *sub-domain*. These sub-domains are viewed as loosely coupled; there are security actions associated with each sub-domain independently of the others, as well as actions concerning integrated aspects. The control-loop model of Figure 26 is applied to each sub-domain of Figure 11 and to their integration. This seeks to represent the time evolving growth in security capability (and tracking of evolving situations) within each of the four areas.

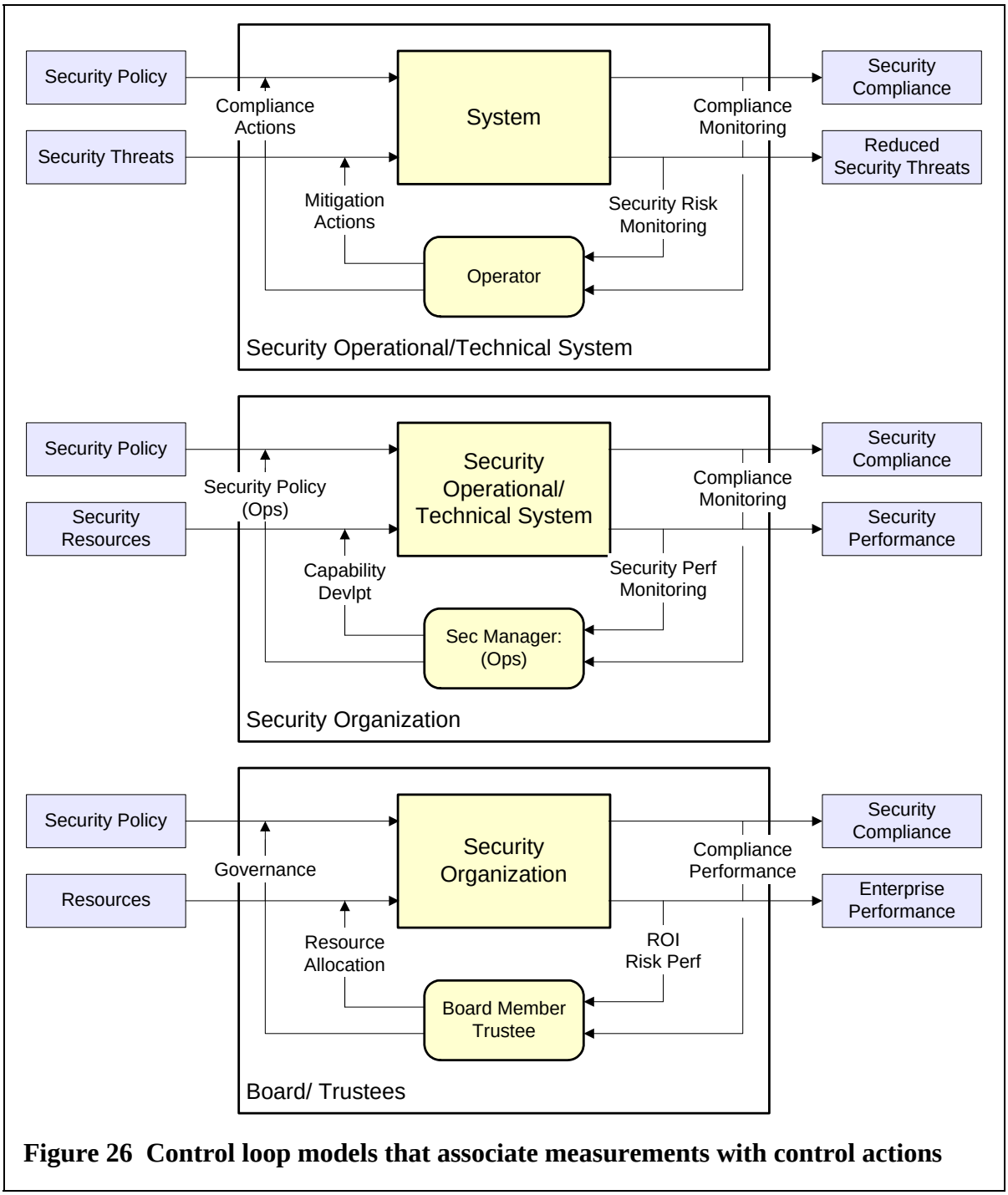


Figure 26 Control loop models that associate measurements with control actions

In the general case, security actions will arise from:

1. The work in each of the security sub-domains;
2. The trade-offs and cross-couplings assessed at the *system security* level;
3. For development projects, trade-offs considered at system engineering level (i.e. trades with other system properties); for operations, trade-offs involved in security policy and service provision.

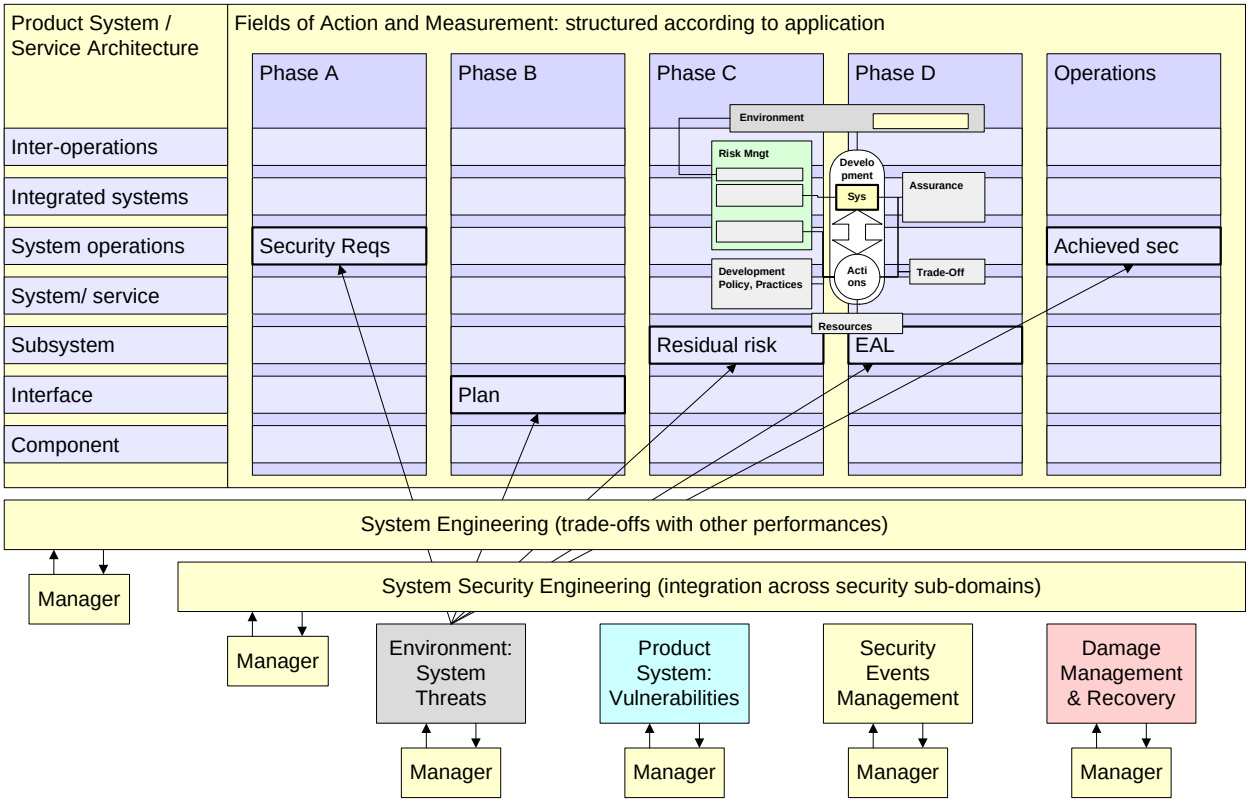


Figure 27 'Field of action' associated with security engineering and management

The actions arising from security engineering and operations are varied and will usually apply to many different parts and aspects of a system of interest. Security properties have to be considered in the context of other properties and risks. It is proposed to model this by a conceptual *field of action* (Figure 27). The 'field of action' is shared with other processes and managed domains. Measurements are drawn from a similar *field of measurement.* Some measurements will be generic such as costs and progress to complete; others will be particular to the entity involved. Measurements may be drawn from a wider field than the field of action – for example, downstream outcomes beyond the scope of action responsibility of a particular manager. Similarly, damages may be assessed on a wider field, for example, including client systems.

The two-loop control model provides a route to the layered PSM model of Figure 26. The slower learning loop provides input to longer-term capability / process development.
The 'field of action' of Figure 27 has been structured into product components and project phases. The domain structure will vary depending on the application; operations may be structured according to the security policy. This structuring is indicative – other categorizations of actions and measures may be more appropriate in different applications.