

A Guide to
**RISK ASSESSMENT AND
SAFEGUARD SELECTION**
for Information Technology
Systems

January 1996

MG-3

Points of Contact

Comments, suggestions and inquiries on risk assessment and safeguard selection for information technology systems, should be directed to the Standards and Initiatives Unit, Risk Management Coordinator, tel. (613) 991-7446, Fax: (613) 991-7411, Internet address: riskmgmt@cse.dnd.ca. For additional copies of the document, please contact the ITS Publications Section at (613) 991-7514/7468 or CSE's WWW site at the following address: <http://WWW.cse.dnd.ca>.



©1996 Government of Canada, Communications Security Establishment (CSE)
P.O. Box 9703, Terminal, Ottawa, Ontario, Canada, K1G 3Z4

This publication may be reproduced verbatim, in its entirety, without charge, for educational and personal purposes only. However, written permission from CSE is required for use of the material in edited or excerpted form, or for any commercial purpose.

FOREWORD

This *Guide to Risk Assessment and Safeguard Selection for Information Technology Systems* is a CSE funded project. The aim was to expand on the standards set out in the Government Security Policy (GSP) and thus provide specific guidance for risk assessment and safeguard selection process throughout the Information Technology (IT) system life cycle. The development of this document was based upon and harmonized with, the risk management framework described, in the first of three companion guides titled, *A Guide to Security Risk Management for Information Technology Systems*. The third guide is titled, *A Guide to Certification and Accreditation of Information Technology Systems*. The three guides are designed to provide the user a complete scope of effort in risk management of an IT system life cycle.

Users are encouraged to apply the three guides along the with the RCMP, Information Technology Security Branch document, *A Guide to Threat and Risk Assessment for Information Technology* in their environment. CSE invites inquiries, comments, suggestions for improvement and suggestions for further study such as a methodology for risk management for IT systems.

TABLE OF CONTENTS

POINTS OF CONTACT	i
FOREWORD	ii
LIST OF ABBREVIATIONS AND ACRONYMS	vii
INTRODUCTION	1
1. RISK ASSESSMENT AND SAFEGUARD SELECTION FRAMEWORK	4
1.1 Introduction	4
1.2 Planning	5
1.2.1 Aim	5
1.2.2 Scope	5
1.2.3 Boundary	5
1.2.4 System Description	5
1.2.5 Target Risk and Required Certainty	6
1.3 TRA Preparation	6
1.3.1 Statement of Sensitivity (SoS)	6
1.3.2 Identification of System Assets	6
1.4 TRA Analysis	6
1.4.1 Identify Threat Scenarios	7
1.4.1.1 Asset Sensitivity Analysis	7
1.4.1.2 Threat Assessment	8
1.4.1.3 Vulnerability Assessment	8
1.4.2 Filtering Threat Scenarios	8
1.4.3 Assessing Risk	9
1.4.3.1 Impact Assessment	9
1.4.3.2 Likelihood Assessment	9
1.5 TRA Recommendations	9
1.6 Selecting Safeguards	9
1.6.1 Developing Safeguard Options	10
1.6.2 Analyzing Trade-offs	11
1.6.3 Selecting the Preferred Safeguard Option	11
1.7 Roles and Responsibilities	11

2. PROCEDURAL GUIDANCE	13
2.1 Introduction	13
2.2 Preparation	13
2.2.1 Aim	13
2.2.2 Boundary	14
2.2.3 System Description	14
2.2.4 Scope	15
2.2.5 Statement of Sensitivity (SoS).....	16
2.2.6 Target Risk and Certainty	17
2.3 Risk Analysis Methods.....	17
2.3.1 Analysis Approach.....	17
2.3.1.1 Top Down Analysis	18
2.3.1.2 Bottom Up Analysis.....	18
2.3.1.3 System Decomposition	19
2.3.2 Asset Sensitivity Analysis.....	19
2.3.3 Threat Assessment.....	20
2.3.4 Vulnerability Assessment	21
2.3.4.1 System Vulnerabilities	21
2.3.4.2 Safeguard Effectiveness.....	22
2.3.5 Threat Scenarios.....	23
2.3.6 Impact Assessment	23
2.3.7 Likelihood Assessment.....	24
2.3.7.1 Threat Agents	24
2.3.7.2 Random Events and Natural Disasters.....	24
2.3.8 Risk Assessment.....	24
2.4 Practical Considerations	25
2.4.1 Risk Analysis Data	25
2.4.1.1 Data Organization.....	25
2.4.1.2 Sources of Information.....	26
2.4.1.3 Support Tools	26
2.4.2 Risk Report.....	27
2.4.3 Sensitivity of Risk Assessment Information.....	28
2.5 Recommendations	28
2.6 Requirements Definition	28
2.7 Safeguard Selection	28
2.7.1 Developing Safeguard Options	29
2.7.1.1 Safeguard Groups	29
2.7.1.2 Safeguard Attributes	29
2.7.2 Trade offs	30
2.7.2.1 Safeguard Cost.....	30

2.7.2.2 Safeguard Effectiveness.....	30
2.7.3 Selecting the Preferred Option.....	31
3. LIFE CYCLE PROCESS GUIDANCE.....	32
3.1 Introduction.....	32
3.2 Planning for Change.....	32
3.2.1 Aim and Scope.....	32
3.2.2 Required Inputs.....	33
3.2.3 Risk Assessment Approach.....	33
3.2.4 Safeguard Selection Approach.....	33
3.3 Requirements Definition.....	33
3.3.1 Aim and Scope.....	33
3.3.2 Required Inputs.....	33
3.3.3 Risk Assessment Approach.....	34
3.3.4 Safeguard Selection Approach.....	35
3.3.5 Outputs.....	36
3.4 Architecture Design.....	36
3.4.1 Aim and Scope.....	36
3.4.2 Required Inputs.....	37
3.4.3 Safeguard Selection Approach.....	38
3.4.4 Risk Assessment Approach.....	38
3.4.5 Outputs.....	39
3.5 Detailed Design.....	40
3.5.1 Aim and Scope.....	40
3.5.2 Required Inputs.....	40
3.5.3 Safeguard Selection Approach.....	40
3.5.4 Risk Assessment Approach.....	41
3.5.5 Outputs.....	42
3.6 Implementation.....	42
3.6.1 Aim and Scope.....	42
3.6.2 Required Inputs.....	43
3.6.3 Risk Assessment Approach.....	43
3.6.4 Safeguard Selection Approach.....	43
3.6.5 Outputs.....	43
3.7 Operation.....	43

ANNEX A – GENERIC THREAT AGENTS IN IT SYSTEMS	45
ANNEX B – GENERIC ATTACKS ON AN IT SYSTEM	47
ANNEX C – SYSTEM DOCUMENTS FOR RISK ASSESSMENT AND SAFEGUARD SELECTION	54
ANNEX D – SECURITY SAFEGUARDS	57
GLOSSARY	61
BIBLIOGRAPHY	65

LIST OF TABLES

Table I – Sequences of Threat Events	47
Table II – Risk Report Contents.....	54
Table III– Safeguard Selection Report Contents	55

LIST OF FIGURES

Figure 1 – Risk Management Model	1
Figure 2 – Relationship between Guidance Documents	2
Figure 3 – Risk Assessment Process.....	7
Figure 4 – Safeguard Selection Process	10
Figure 5 – Vulnerability Analysis Relationships	21

LIST OF ABBREVIATIONS AND ACRONYMS

AA	Accreditation authority
CCB	Configuration Control Board
CMP	Configuration Management Plan
CSE	Communications Security Establishment
CSSC	Canadian System Security Centre
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
DSO	Departmental Security Officer
GSP	Government (of Canada) Security Policy
IT	Information Technology
ITS	Information Technology Security
NCSC	National Computer Security Centre (USA)
OA	Operational Authority
SoS	Statement of Sensitivity
ST&E	Security Testing and Evaluation
TCSEC	Trusted Computer System Evaluation Criteria (USA)
TRA	Threat and Risk Assessment
TSEG	Trusted Systems Environment Guideline (CAN)

INTRODUCTION

Purpose

The purpose of this document is to provide guidance for security risk assessment and safeguard selection for information technology (IT) systems.

Scope

The *Guide to Security Risk Management for Information Technology Systems* (MG-02) defines a risk management process for IT systems as shown in Figure 1. This document provides guidance on

- a) **threat and risk assessment** (risk assessment) which defines what is at risk, the relative magnitude of risk, and the causal factors; and
- b) **safeguard selection** which defines what to do about risk when risk is being managed through reduction. Note that transfer, avoidance, or acceptance of risk is outside the scope of this document.

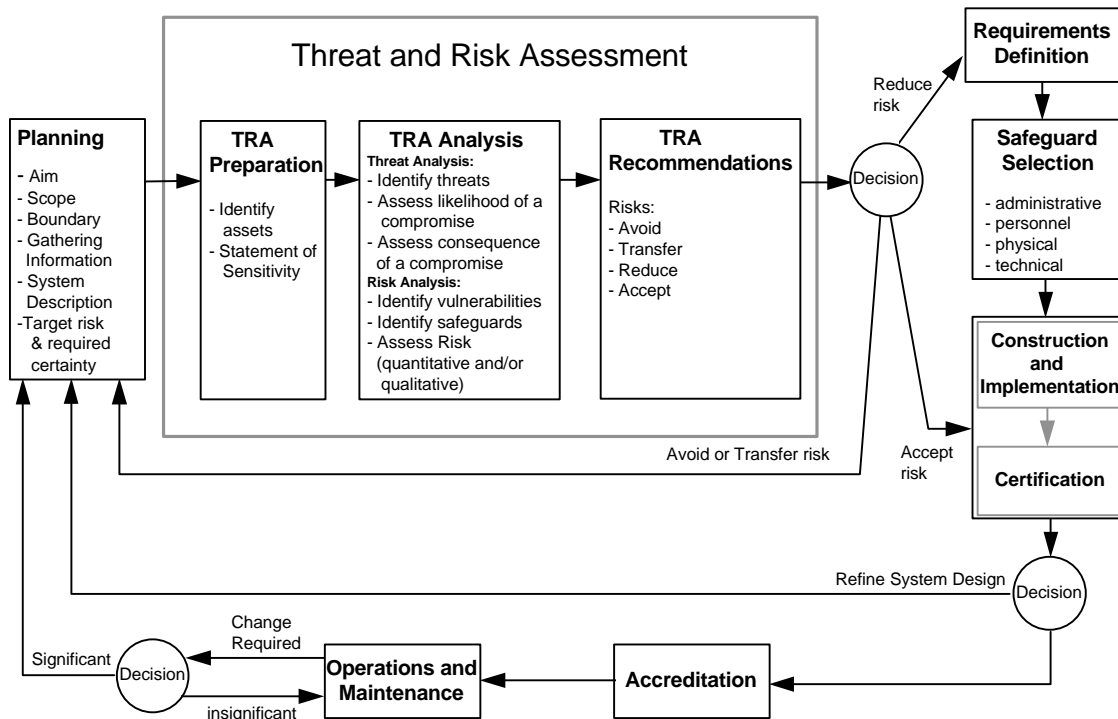


Figure 1 – Risk Management Model

The guidance applies to both proposed and existing systems.

In recognition of the integral role of threats, the Government Security Policy (GSP) refers to the process of assessing risk as a threat and risk assessment (TRA). Throughout this document, the term "risk assessment" will be used since a threat analysis is only one part of risk assessment. Also, the term "risk assessment" used in this guide refers to "IT system security risk assessment" and not other forms of risk assessment (for example, project risk).

Related Documentation

The guidance provided in this document focuses on security risk assessment and safeguard selection for IT systems. For guidance on risk management, the reader should refer to the *Guide to Security Risk Management for Information Technology Systems*. For guidance on the certification and accreditation of IT systems, the reader should refer to *the Guide to Certification and Accreditation of Information Technology Systems*. The relationship between the three documents is illustrated in Figure 2.

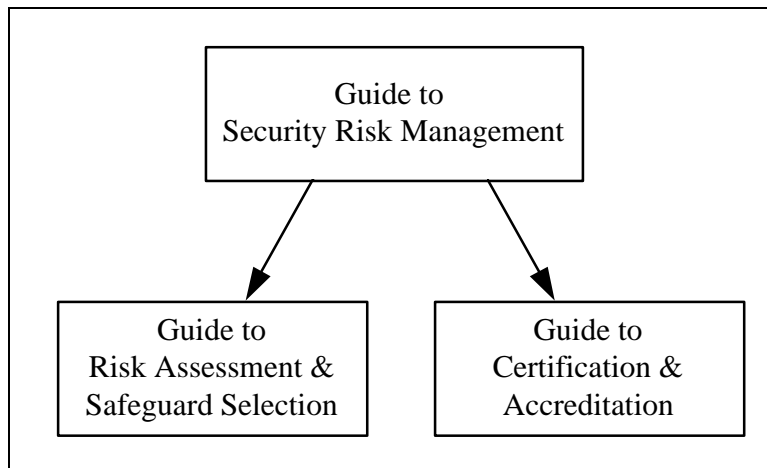


Figure 2 – Relationship between Guidance Documents

Audience

The document is primarily intended for use by risk analysts and security engineers in the performance of risk assessments and safeguard selections. It may also be of value to system and project managers as a means of understanding these two processes.

Document Structure

A list of abbreviations and acronyms used throughout the document immediately follows the table of contents. It may be useful for the reader to have this list handy while reading this document.

The document is composed of three chapters and four annexes. Chapter 1 provides a brief description of what the risk assessment and safeguard selection processes are in relation to risk management. Chapter 2 provides guidance on how to perform risk assessment and safeguard selection independent of a life cycle. Chapter 3 provides

specific guidance on how to perform risk assessment and safeguard selection at the various stages of a system life-cycle. Annex A and B provides guidance on threat agents and threat events. Annex C provides guidance on risk assessment and safeguard selection documentation, and Annex D provides a description of safeguard groupings. A Glossary and a Bibliography are provided at the end.

1. RISK ASSESSMENT AND SAFEGUARD SELECTION FRAMEWORK

1.1 Introduction

Risk is a function of the consequences (or impact) of an undesirable event and the likelihood of that event occurring. Risk assessment is the process whereby risk relationships are analyzed, and an estimate of the risk of asset compromise is developed. Compromise includes unauthorized disclosure, destruction, removal, modification, or interruption. Options for managing risk include reduction, transfer, avoidance, and acceptance.

A risk assessment produces an estimate of the risk to an IT system at a given point in time. It answers the following questions:

- What can go wrong?
- How bad could it be?
- How likely is it to occur?

The resulting measure of risk is also referred to as a risk assessment. Should the management of this risk be through reduction, then the safeguard selection process provides answers to the question:

- What could be done to reduce the exposure?

As shown in Figure 1, the risk assessment process consists of three major elements: preparation, analysis, and recommendations. The output of the risk assessment process is input to a decision process which determines whether to avoid, transfer, accept or reduce risk.

If the decision is to avoid or transfer the risk, the analysis process returns to the preparation stage so that the system description can be changed to remove or move sensitive system assets. If risk is to be reduced, then the requirements definition element is initiated. If the risks are acceptable then construction and implementation can be undertaken. Note that certification is an ongoing activity throughout a system's life cycle, and that risk assessments and security evaluations of the constructed and implemented system are incorporated into certification documentation.

As the system evolves during the life cycle, additional detail is added to the system definition in a cyclical or iterative manner. During each iteration of the system design, the risks are reassessed to determine if the risk is being acceptably managed. At the end of each design iteration, the life cycle process in figure 1 provides a path back to planning for the next design iteration and the next risk assessment.

1.2 Planning

Several items must be prepared before starting a risk assessment. The items required are:

- a) the aim;
- b) the scope;
- c) the boundary;
- d) the system description; and
- e) the target risk and required certainty.

Depending on when the risk assessment is performed during the system life cycle, some of these items may have already been established. The system description might be prepared outside of the risk assessment activities.

1.2.1 Aim

Prior to performing any risk assessment, an aim must be established. The aim influences the style of analysis and the information output from the risk assessment process. The aim identifies: the objectives of the risk assessment process, the type of output required, and critical constraints (for example, time, cost, technology, policy).

1.2.2 Scope

The scope of analysis must be determined. A given risk assessment may focus on a subset of the overall assets, vulnerabilities, threat events, or threat agents. For example, the scope of study might be to determine the risks to a specific asset, or the risks associated with a new type of attack or with evolving capabilities of threat agents.

1.2.3 Boundary

The boundaries of the risk assessment must be defined in terms of physical system boundaries, and in terms of logical analysis boundaries. These boundaries are fundamental in determining the amount of analysis required to complete a risk assessment. For example, the logical analysis boundaries define the required breadth and depth of analysis, while the physical system boundary defines where one system ends and another one begins. For a system that connects to an external system, characteristics of all interfaces must be carefully described.

1.2.4 System Description

A system description provides the basis for subsequent analysis. If a system description is not provided, then one must be developed. Prerequisites to undertaking a risk assessment are: the system requirement (or mission), a concept of operation, and identification of the nature of system assets. The identification of the system must extend to the boundary of the assessment.

1.2.5 Target Risk and Required Certainty

A target risk is established which should be met by the IT system. This target risk will be used to determine if the risk is within acceptable bounds. The required certainty defines the level of certainty required by the risk assessment, and will partially be defined in the aim. The level of certainty determines the level of effort in the analysis. An increased level of certainty will require more detailed analysis.

1.3 TRA Preparation

In addition to the items provided in the previous section, the following items are required:

- a) the statement of sensitivity (SoS); and
- b) the identification of system assets.

Depending on when the risk assessment is performed during the system life cycle, the statement of sensitivity and asset list might be partially or totally complete.

1.3.1 Statement of Sensitivity (SoS)

A statement of sensitivity defines the sensitivity of the information within the system and the importance of the supporting services of the system. An SoS may also define the sensitivity requirements of supporting assets (that is, hardware and software, interfaces, personnel, supporting systems and utilities, and access control measures).

1.3.2 Identification of System Assets

Based on the system description and the statement of sensitivity, a complete list of system assets including information, hardware and software, interfaces, personnel, supporting systems and utilities, and access control measures is required. This list is generally more detailed than the SoS.

1.4 TRA Analysis

The aim of analyzing risk variables is to provide an assessment of the risk associated with operating a system under an existing or proposed set of safeguards.

Figure 3 partitions the risk assessment into its fundamental components:

- 1) identifying threat scenarios;
- 2) filtering threat scenarios; and
- 3) assessing risk.

1.4.1 Identify Threat Scenarios

As shown in Figure 3, threat scenarios must be identified. A threat scenario is an event (or sequence of events) which leads to the compromise of system assets. A threat scenario relates a particular asset to a particular vulnerability (that is, exposure) and a particular threat agent. Assets and threat agents can be independently assessed. Vulnerabilities are assessed by considering the relationships between generic assets and generic threat agents and by identifying relevant threat events. Following these independent assessments, a complete set of all asset/threat agent/vulnerability combinations (that is, threat scenarios) can be generated.

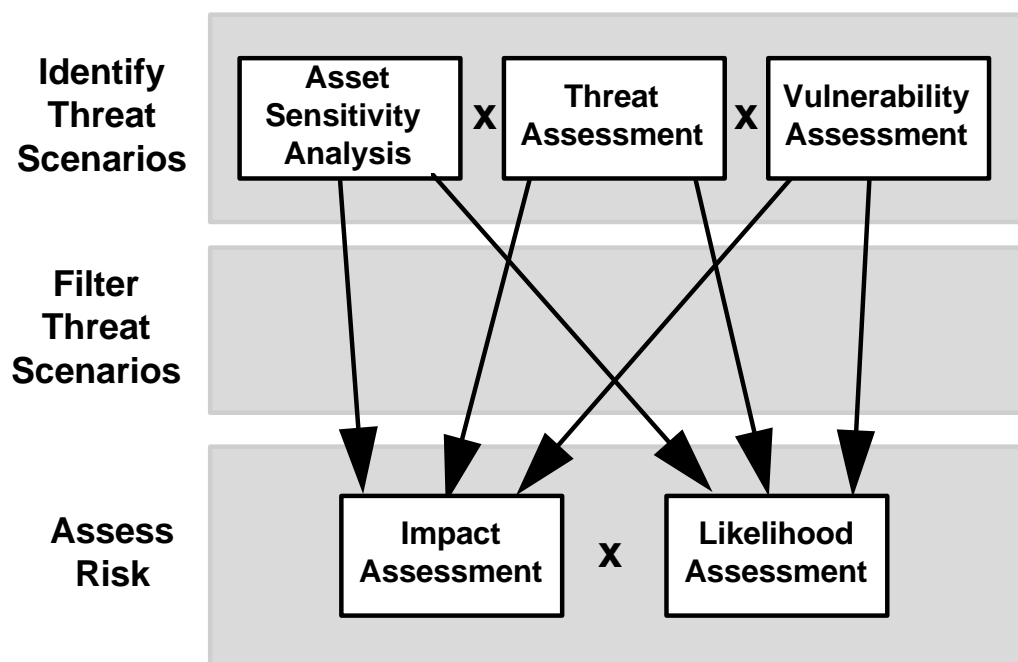


Figure 3 – Risk Assessment Process

1.4.1.1 Asset Sensitivity Analysis

The value of the assets included within the scope of the risk assessment must be estimated. An asset's value is based on:

- its replacement cost;
- its intrinsic value (for example, goodwill); and/or
- the consequences, impact or injury resulting from asset compromise.

The output of the asset sensitivity analysis is an inventory of assets with their sensitivity (that is, their value) with respect to confidentiality, integrity, availability and replacement

value. In many cases, information processed by the system will be the most significant asset.

A Statement of Sensitivity (SoS) is a valuable input to the asset sensitivity analysis since it provides a list of assets and their associated sensitivity. During the asset sensitivity analysis, the asset sensitivities are described in the form used by the risk assessment method. If not included in the SoS, asset sensitivity analysis will also involve determining the sensitivity that system resources (such as storage media and communications interfaces) inherit from the principal assets (information and services).

1.4.1.2 Threat Assessment

Threat agents trigger asset compromise; therefore, the assessment of threats is an essential step in the risk assessment process. A threat agent is the actual perpetrator or causal factor of threat scenarios. Threat agents may be malicious persons or groups, negligent or careless personnel, or they may be random occurrences and natural phenomena.

1.4.1.3 Vulnerability Assessment

The vulnerability assessment identifies the threat events (or types of attacks) that system assets are “vulnerable” to, and characterizes the level of effort (that is, resources and capabilities) required by a threat agent to mount an attack.

Level of effort will be directly related to:

- a) **Safeguard Effectiveness.** In order to assess risk, the effectiveness of individual and combinations of existing, or proposed, safeguards must be considered. Since failure of a safeguard can expose an asset to subsequent attack, it is also important to determine how prone a safeguard is to failure, and whether there are ways that it can be circumvented. To be cost effective, safeguard assessment should consider the need for, as well as the efficiency of proposed or existing safeguards.
- b) **System Vulnerabilities.** Vulnerabilities are characteristics or weaknesses of the system that allow assets to be compromised. Examples of vulnerability are: the portability of high capacity diskettes and laptop computers, and the susceptibility of radio transmissions to be intercepted.

1.4.2 Filtering Threat Scenarios

The total number of threat scenarios produced (that is, the cross product of all assets, all threat agents, and all vulnerabilities) can be very large. Not all threat scenarios need be examined. Therefore, the risk assessment method should filter out some threat scenarios for the following reasons:

- a) some threat scenarios (that is, asset/threat agent/vulnerability triples) may not make sense in the context of the IT system;

- b) the scope of the analysis may not require a complete set of threat scenarios; and
- c) there might be cost, time, or resource constraints that limit the amount of analysis and prohibit exhaustive searches for threat scenarios.

1.4.3 Assessing Risk

Once a filtered set of threat scenarios has been identified, the risk analyst will generate a measure of the risk which is associated with operating the IT system. Risk is a function of impact (that is, consequences) of threat scenarios and their likelihood of occurring. The output of assessing risk is a set of measured values which can be related to the target risk set by the accreditation and operational authorities. The certainty in the risk value should reflect the objective set by the accreditation authority in the Preparation stage. The risk analyst should also produce explanations which support the logic behind the measure of risk (that is, reasoning and deductions).

1.4.3.1 Impact Assessment

Threat scenario impact is determined by examining the sensitivity of the compromised asset. Impact must be assessed using the valuation semantics of the asset (that is, replacement cost, intrinsic value, or compromise impact). Impact assessment is a useful aid in identifying the most serious threat scenarios.

1.4.3.2 Likelihood Assessment

Threat scenario likelihood is determined by examining aspects of the threat agent (such as, capability, resources, opportunity, and motivation), and the level of effort required by the threat agent to mount the attack on the system. The risk analyst must consider all of these variables and the subtle interactions between them. Likelihood is often the most difficult aspect of risk to characterize due to the linkages between these various pieces of information.

1.5 TRA Recommendations

The risk analyst will make recommendations on how to address unacceptable risks. If the recommendation is to reduce risk, security requirements and/or safeguards will be suggested. The risk analyst, having done the risk assessment, may have insights into safeguard selection which the security engineer does not have. If the recommendations are to accept, transfer, or avoid the risk, management recommendations will be made to the authority responsible for the system and its assets.

1.6 Selecting Safeguards

If the risk is greater than the target risk and the operational authority chooses risk reduction, then the requirements definition and safeguard selection process is followed.

The process of selecting safeguards, depicted in Figure 4, shows the inputs and main activities in the selection of system safeguards. Before safeguards can be selected, a

target risk level must be provided, relevant system requirements and constraints must be identified, and a risk assessment must be completed. A review of the risk assessment results provides information required to determine where safeguards must be added to the system to reduce the risk to an acceptable level. The threat scenarios that were identified to have unacceptable risks are reviewed by system designers to determine how and where the system is being attacked. With this information, safeguard options can be developed to reduce the likelihood and risk of the threat scenarios to an acceptable level.

In most cases, one or more safeguard options are available. Safeguard options describe different suites of safeguards which mitigate high risk threat scenarios. The most appropriate option is determined by analyzing trade-offs between system performance, safeguard costs, safeguard effectiveness and reduction of risk. The preferred option is selected after examining the trade-offs for each option.

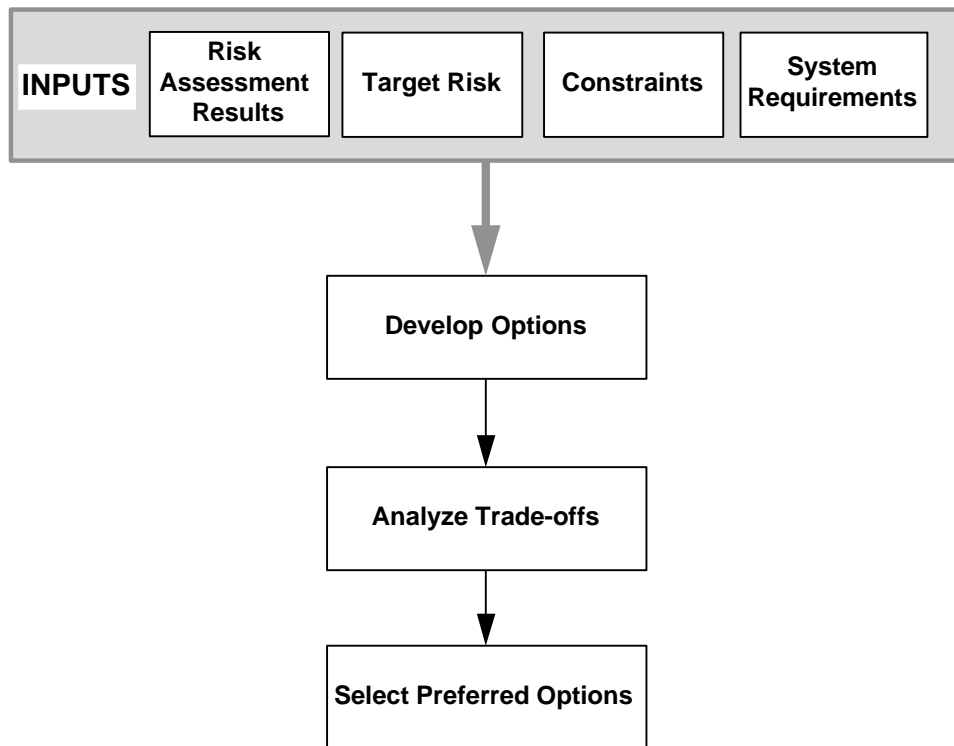


Figure 4 - Safeguard Selection Process

1.6.1 Developing Safeguard Options

The assets which require safeguard protection are identified in the risk assessment. The development of different safeguard options for a system is influenced by the results of the system's risk assessment, the system's requirements and constraints, and the target risk of the system. Safeguard options may incorporate different combinations of physical, procedural, personnel, and technology based safeguards to reduce the level of

risk in a threat scenario to the target risk level. Particular safeguards are chosen based on their attributes.

1.6.2 Analyzing Trade-offs

Before selecting a safeguard option, the trade-offs between safeguard costs and safeguard effectiveness of each safeguard option are analyzed. Cost considerations include immediate costs of acquisition and installation, operational costs and indirect costs such as loss of functionality or productivity. The life expectancy of the safeguards and the assets to be protected must also be considered.

The effectiveness of a safeguard option in reducing risk is determined by

- a) the vulnerabilities it addresses in the system;
- b) its dependence on other safeguards to operate correctly;
- c) its vulnerability to accidental failure or deliberate evasion;
- d) its acceptability to users and operators;
- e) its requirements for intervention or interpretation by personnel; and
- f) its visibility to the threat agents.

These factors can be used as a basis in which to determine the overall effectiveness of a specific safeguard in reducing threat scenario likelihoods, impacts, and risk. Other factors such as versatility and availability of alternative safeguards may be included in the trade-off analysis.

1.6.3 Selecting the Preferred Safeguard Option

In a risk management approach, the preferred safeguard option provides sufficient protection at an optimal cost. The trade-off analysis assesses the cost (dollars and system performance), the effectiveness, and the risk reduction of a particular option. The preferred option must provide adequate protection at the time of implementation and throughout the system's lifetime. Hence, the best or preferred option may not be the one with the lowest cost.

1.7 Roles and Responsibilities

Several participants, performing different roles, are required to support risk assessment and safeguard selection. Each role provides an essential ingredient to an effective TRA and a secure system design. A participant may perform several roles (for example, the risk analyst might also be a threat expert and system specialist). The roles (as they pertain to risk assessment and safeguard selection) include:

- a) **Risk Assessment Sponsor.** The sponsor helps define the scope of the TRA (that is, aim, boundary, and constraints). The sponsor is usually the Operational Authority (OA).

- b) **IT System Operational Authority (OA).** The OA accepts the risk (and operating conditions imposed by the Accreditation Authority (AA)) of operating the IT system. The OA also determines whether unacceptable risk is to be reduced, avoided, transferred, or accepted.
- c) **Accreditor.** The accreditor, in conjunction with the OA, defines the target risk which must be met and the certainty required in the analysis.
- d) **Risk Analyst(s).** Risk analysts perform the TRA and assesses risk. Risk analysts will use some risk assessment method which may be supported by a risk assessment tool.
- e) **Threat Experts.** Threat experts provide threat information to the risk analyst. Lead agencies (that is CSE, CSIS, and RCMP) can help in compiling relevant threat information.
- f) **User Representatives.** Users provide asset input to the risk analyst as part of creating the Statement of Sensitivity. The risk analyst may also interview users to establish if they represent a threat or a vulnerability to the system.
- g) **System Specialists.** System specialists provide vulnerability information to the risk analyst. Detailed knowledge on the design, operation, and management of the system reduces the uncertainty in assessing system vulnerability.
- h) **Security Engineers.** Security engineers provide safeguard selection recommendations to the OA based on the identified risks. Security engineers should work closely with system engineers for systems under development.

2. PROCEDURAL GUIDANCE

2.1 Introduction

The purpose of this chapter is to provide procedural guidance in performing risk assessment and safeguard selection activities. Guidance for risk assessment and safeguard selection activities that are dependent on the system life cycle is covered under Chapter 3.

This chapter is organized according to the steps in the risk assessment and safeguard selection process described in Chapter 1. It contains the following sections: preparation, risk analysis methods, practical considerations, recommendations, and safeguard selection.

2.2 Preparation

This phase organizes the information required to conduct the risk assessment and safeguard selection. This information is captured in the risk report as described in Section 2.4.2. Some of the preparation phase documents are baselined and used in subsequent risk assessments while others must be done for each risk assessment.

2.2.1 Aim

The risk assessment sponsor, in conjunction with the risk analyst, defines and documents an aim for each risk assessment. The aim defines:

- a) **Objectives.** The life cycle stage will define the high-level objectives of the risk analysis. See chapter 3.
- b) **Required results.** The life cycle stage will define the required results of the risk analysis. See chapter 3.
- c) **Critical constraints.** The following are examples of factors that can critically constrain a risk assessment:
 - i) **Cost.** Lack of funds can limit the scope of the analysis.
 - ii) **Time.** Lack of time can limit the scope of the analysis.
 - iii) **Resources.** Lack of personnel (for example, system specialists) or information (for example, threat briefings) can limit the scope and certainty of the analysis.
 - iv) **Policy/Standards.** The sponsor may restrict the scope to study options and noncompliance with departmental policy and standards. Security policy and standards may dictate a baseline set of security requirements.

- v) **Method and Support Tools.** The sponsor may restrict the analysis to a particular method and support tool (for example, a departmental risk assessment standard).
- vi) **Technology.** The sponsor may restrict the technologies used in safeguard selection to existing safeguard technology¹ or to a type of safeguard².

2.2.2 Boundary

The risk assessment sponsor, in conjunction with the risk analyst, defines and documents the system boundary as part of the first risk assessment of a system. The system boundary is baselined. The system boundary defines the following for each external system interface to the system:

- a) **Detailed interface description.** This includes a description of what assets flow in and out of the system via the interface, the method of transporting these flows, and identification of the end sources. An example is an X.25 interface to a financial system where cheque requisitions flow out of the system being analyzed to a financial officer in the external system.
- b) **External System Assumptions.** Assumptions made about the external systems will affect the context for analyzing potential threat scenarios involving system assets coming from the interface. The assumptions will include any rules associated with connecting to the external system. For example, an external system might be assumed to be a controlled system where the likelihood of threat agents accessing the analyzed system from the external system is very low. However, the connection can only be made if the system being analyzed places several constraints on the connection.

2.2.3 System Description

The risk analyst documents the system description for each risk assessment. Parts of the system description may have been baselined in earlier risk assessments. The system description should provide a security relevant view of the system with enough detail such that it can stand alone. The system description defines the following:

- a) **Operational Requirement.** This is a statement of the business objectives, operational role, functions, and performance requirements of the system. It may be derived from identified capability deficiencies.
- b) **Concept of Operations.** This is a functional description of the system and how it is used to support the mission's business objectives. The functional description should include: information handled, types of applications or processing, users, connectivity between functions, and connectivity to the external world defined by the system boundary.

¹ The sponsor may specify that the risk be managed with existing safeguard technology, and not with the development of new safeguard technology.

² For example, a sponsor may restrict safeguards to procedural safeguards to reduce risk.

- c) **Policy Framework.** Applicable departmental security policies and standards are listed and their relevance to the system is described. These will constrain the safeguard development and focus the risk assessment.
- d) **Location.** This describes the physical location of the system and, where applicable, the surrounding geographical area. The location influences: the presence of threat agents, the availability and effectiveness of safeguards, and system constraints.
- e) **Anticipated Modification or Expansion.** This describes any future plans for modification or expansion. Future plans may impact the present choice of safeguards which should be selected.
- f) **System Design.** This describes the (secure) system design used to support the concept of operations. It includes: the system topology, hardware, software, and interfaces. The system design will become progressively more detailed throughout the life cycle.

The operational requirement, concept of operations, policy framework, location, and anticipated modification are baselined early in the life cycle. The system design will vary depending on the life cycle stage (see *A Guide to Security Risk Management for Information Technology Systems* for details).

2.2.4 Scope

The risk assessment sponsor, in conjunction with the risk analyst, defines and documents the scope of each risk assessment. The scope defines the following aspects of the analysis:

- a) **Focus.** The focus defines the aim's high-level objectives in a finer granularity. This describes specific critical areas which should be examined to the exclusion of, or in greater detail than, other areas (that is, breadth and depth respectively). The focus can be constrained by the aim (for example, cost, time, resources, policy, standards, methodology, tools). Examples of critical areas can be:
 - i) specific assets, threat agents, and/or types of attack (for example, assessing the risk due to a change in a particular threat agent's capability);
 - ii) specific aspects of the system (for example, assessing risk to a key management system after cryptos have been added as a safeguard); and
 - iii) specific requirements for high assurance safeguards. The assurance required of a safeguard will be proportional to the amount of risk reduction it is to achieve. Based on common knowledge or previous risk assessments, specific threat scenarios may be identified as requiring high assurance safeguards (that is, the risk must be significantly reduced to some level). A sufficiently detailed risk assessment is required to indicate that the risk is sufficiently reduced once the safeguard is added.
- b) **Breadth.** This describes the subset of the system design included in the risk assessment. Note that only those system elements which are relevant to security need be included in the risk assessment. For example, if cryptos provide

disclosure prevention across a network (and there are no integrity or availability concerns), then the network need not be included in subsequent risk analyses once it has been determined that the risk is not significant.

- c) **Depth.** This describes the level of detail required from the analysis. The aim (that is, objectives and required outputs based on life cycle stage) generally determines the depth of the analysis. Analysis detail generally increases later in the life cycle as the system design is defined in greater detail. There need not be a homogenous level of detail required for each system element being analyzed (for example, all parts of a complex system may not be at the same life cycle stage, or critical security requirements will require a greater depth of analysis), or for aspects of the analysis (for example, use generic threat agents but detailed methods of attack).

The scope is the most significant factor in determining the level of effort required to perform a risk assessment.

2.2.5 Statement of Sensitivity (SoS)

A SoS must define the sensitivity of information and services assets. From a business perspective, the system possesses information and/or service assets which are used to support the system mission. The SoS must itemize these assets with their associated sensitivity.

A SoS may describe the sensitivity of the supporting assets such as hardware and software, interfaces, personnel, supporting systems and utilities, and access control measures. These supporting assets will be populated during the asset sensitivity analysis in Section 2.3.2.

Asset sensitivity can be described in the following areas:

- a) **Confidentiality.** This describes the consequences of an asset being disclosed. The classification and designation labels assigned to information assets are based on exemptions and exclusions to the *Access to Information Act* and the *Privacy Act*. These labels correspond to levels of injury based on sensitivity and invasion of privacy tests.
- b) **Integrity.** This describes the consequences of an asset not being accurate, complete, or dependable.
- c) **Availability.** This describes the importance of the asset to operations. Responsiveness to asset unavailability should be described.
- d) **Replacement Value.** This describes the cost of replacing the asset.

The operational authority itemizes and documents system assets. If a SoS does not exist then the risk analyst must produce one. SoS preparation can be time consuming. Thus, an existing SoS is a valuable input to the risk assessment.

An asset's sensitivity may be measured in both a qualitative and quantitative manner simultaneously; the result can be a vector, or multivalued measure (for example, \$, loss

of lives, and goodwill). Quantitative measures and/or qualitative measures should be chosen, as deemed appropriate for the type of asset being assessed.

Note that the SoS does not describe all of the IT system assets which inherit the sensitivities of information handled and services provided; this is done during asset sensitivity analysis in Section 2.3.2.

2.2.6 Target Risk and Certainty

The accreditor and operational authority define and document the target risk and the certainty required in the measure of risk:

- a) **Target Risk.** Target risk does not need to be established prior to starting a risk assessment. However, it is required in order to complete the recommendations. It may be beneficial to delay the definition of the target risk until there is a better understanding of the nature of the risk in the system.
- b) **Certainty.** The required certainty must be established in conjunction with the defined depth of analysis in the scope since more detailed analysis will result in greater certainty of results. For some systems, the level of “trust” or assurance that is required may dictate the required certainty.

2.3 Risk Analysis Methods

To develop an assessment of risk, the analyst must review the description of the IT system, identify significant threat scenarios and assess the likelihood and impact of their occurrence. A structured risk analysis method will promote the completeness and consistency of the analysis and provide greater assurance in the final risk assessment. Ideally, the method should provide sufficient guidance to analysts to ensure that the results of the risk assessment are reproducible. It may be helpful if risk analysis methods are supported by good automated tools, especially for large or complex systems.

2.3.1 Analysis Approach

The risk of operating a given IT system is principally determined by the sensitivity of the information that it contains, the dependence of the system mission on the services that it provides and the environment that it operates in. Risk results from the consequences and likelihood of threat agents compromising the information or the system services. To compromise these assets, threat agents will exploit supporting system assets such as:

- a) hardware and software;
- b) interfaces to the system;
- c) personnel;
- d) supporting systems and utilities; and
- e) access control measures (that is, items which define a specific environment which differs from the general environment - for example, a security zone).

Consequently, risk analysis views a system along these lines. When an analysis involves system components which exist in substantially different environments, which contain information that is subject to different controls or which execute on hardware and software with different vulnerabilities, it is natural to decompose the problem into smaller security domains. The term security domain will be used as a generic reference, and does not relate to any specific method of system decomposition.

Two fundamentally different approaches are feasible, top down or bottom up.

2.3.1.1 Top Down Analysis

The top down analysis approach is typically organized according to the business functions or services provided by the system. While it may be natural to break the analysis into security domains, this will be along the lines of different business functions, user or management groups, or planned/existing technology subsystems. The analysis will usually concentrate on system assets, threat agents and general high level attack methods.

This approach is helpful in establishing system specific security policies and high level requirements. If the analysis identifies potential high risk areas, it leads to deductions regarding how “vulnerable” the underlying systems are. For proposed systems, the potential security risks motivate functional security requirements which the system design must satisfy, and provide an initial indication of safeguard assurance requirements.

In the case of existing systems, the analysis will again identify potential high risk areas. For simple, non-controversial systems, this approach may be sufficient to define an acceptable set of safeguards that achieve the target risk. For more complex systems, it will help identify critical areas which require further study.

2.3.1.2 Bottom Up Analysis

The alternative approach applies to the analysis of larger or more complex systems. For new developments, it is used later in the system development cycle to assess risks in a detailed design and to define detailed security requirements. For existing systems, it may be used in a focused analysis of specific high risk areas.

This approach is driven by the amount of uncertainty that can be tolerated in the vulnerability assessment. The most detailed level of analysis corresponds to the most detailed assumption in the vulnerability assessment that must be confirmed (in the case of an existing system) or satisfied (by a proposed system) before the target risk can be met.

When many IT security mechanisms are used to satisfy security requirements, the system decomposition typically is based on technology and environment lines. A large number of security domains may be introduced into the analysis. This combinatorial explosion must be managed by recognizing common aspects of similar security domains, and reusing existing analysis where possible.

2.3.1.3 System Decomposition

Regardless of which approach is employed, it is frequently useful to decompose the problem into more than one security domain. Each security domain should provide some unique form of protection to the information and/or processes which it contains. Different domains will typically be selected if they involve different:

- a) security environments;
- b) security policies;
- c) system managers; or
- d) combinations of technology and information.

Special attention should be paid to the interfaces between security domains.

The analysis method should avoid redundant work by:

- a) having a single instance of a domain represent a class of domains when security domains are replicated;
- b) assessing each group once and using groups as building blocks if groups of security domains are replicated; and
- c) exploiting common aspects of different security domains (for example, reuse a single IT vulnerability analysis for all occurrences of a platform).

The high level, or business view of the system must not be overlooked in the decomposition. All of the security critical system relationships should be captured. For example, depending on the system architecture, it may be essential to model end-to-end interprocess communication relationships rather than data transmitted via a serial interface.

2.3.2 Asset Sensitivity Analysis

The SoS documents the confidentiality, integrity, and availability sensitivity of information contained in and services provided by the system. It may also include replacement values.

If supporting assets were not identified in the SoS, then the risk analysis activity maps the SoS onto the system to determine the sensitivity of the supporting assets (for example, disk drives, software processes, and communications interfaces). For each security domain, the information, services and supporting assets should be identified. The sensitivity of the supporting assets should then be assessed.

The following types of supporting assets should be considered:

- a) system hardware and software;
- b) interfaces;
- c) personnel;

- d) utilities; and
- e) access control measures.

Each of the above supporting assets can inherit the confidentiality, integrity or availability sensitivity of the information or service which they support.

2.3.3 Threat Assessment

During a risk assessment, threats resulting from malicious activities, accidents, and natural causes may need to be considered. The term threat is used variously to describe threat agents, the attacks they might mount, or the threat events that indicate an attack. In this guide, attacks or threat events are dealt with during the vulnerability assessment. The attributes of the forces which trigger threat events must be identified and characterized in order to assess risk. This is referred to as a threat assessment.

Threat agents fall into one of the following broad classes:

- a) malicious;
- b) accidental; and
- c) nature.

The attributes of interest for malicious threat agents include: motivation, opportunity, intent, resources, and capabilities. The attributes of interest for accidental and nature threat agents include: error rates and natural phenomena rates. These threat agent attributes are assessed during the threat assessment.

A more detailed list of threat agents will be required for most risk assessments. Some examples are provided in Annex A. Departmental methodologies may provide a standard threat agent template that reflects the business and experience of the department. The risk assessment sponsor may wish to extend the list of agents, or focus on a specific subset.

Ranking of threat agents is not an essential step. It is only meaningful in the context of specific threat agent attributes; for example, which agent has the greater capability with respect to a given attack, or is more highly motivated to compromise certain assets. However subjective, it may be useful to rank agents as a means to prioritize analysis or focus on the concerns of the sponsor.

Threat agent attributes are difficult to analyze, since they can change dramatically over the lifetime of a system due to: changing political, economic, military or criminal situations; changing technology; or adaptive attacks from adversarial threat agents. Risk analysts should take into account possible future trends when conducting a risk assessment. The threat assessment should also be reviewed to ensure that the premises on which the risk assessment is founded remain valid.

2.3.4 Vulnerability Assessment

The objective of this activity is to identify and characterize all potentially significant threat scenarios. These threat scenarios require more detailed examination and a subsequent assessment of risk. Figure 5 shows the relationships which must be considered when analyzing vulnerabilities.

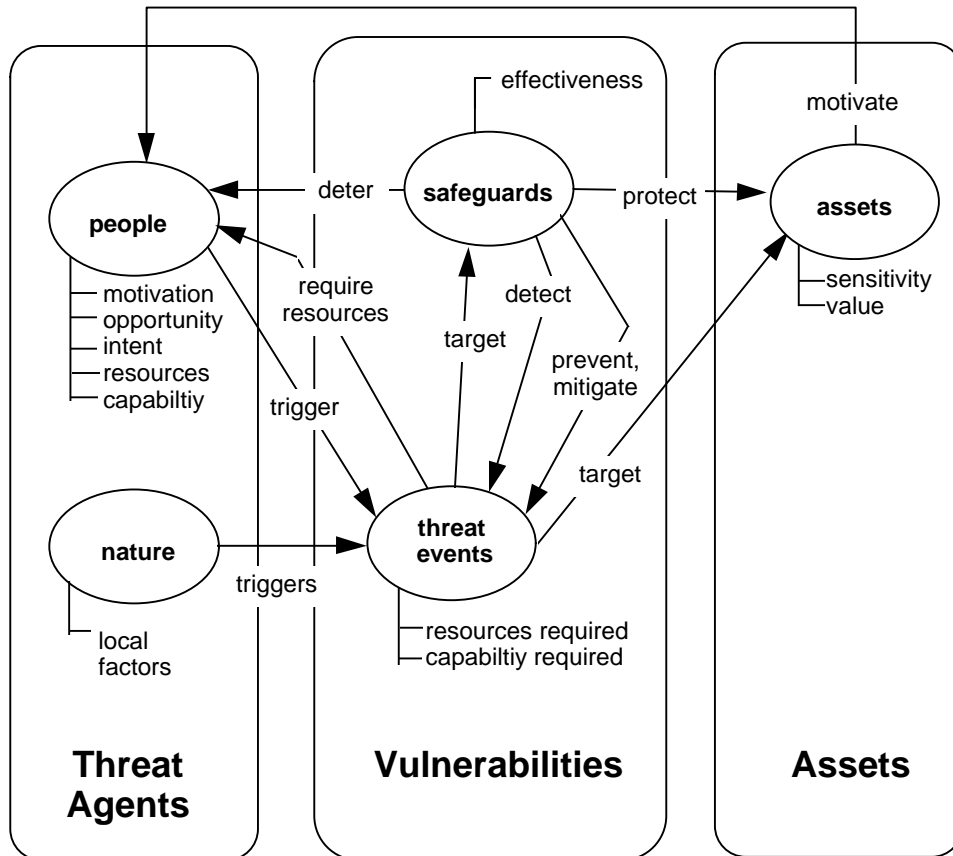


Figure 5 – Vulnerability Analysis Relationships

2.3.4.1 System Vulnerabilities

The system, including supporting assets, will be vulnerable to different types of attack. Analysis of the vulnerability of the system to attack is the key step in the process of identifying threat scenarios. Attacks can thus provide a focus to the system vulnerability assessment.

Based on broad categories of attack, high level architectural vulnerabilities and generic system vulnerabilities can be identified early in the life cycle stage, or as an early step in the analysis of an existing system. An understanding of specific technical and procedural vulnerabilities is often required later in the analysis or system life cycle, and requires more detailed analysis.

Threat agents will require different attributes to mount the different types of attack. The vulnerability analysis will thus influence the type of information required in the threat assessment. Thus, it may be most efficient to conduct these activities in parallel.

Completeness and level of detail included in the vulnerability assessment will affect the confidence that can be placed in the risk assessment. Maintaining good lists of known attacks/vulnerabilities will help provide assurance of the completeness of the analysis. This should include high level generic attacks/vulnerabilities, as well as known technology-specific ones. A more detailed discussion is included in Annex B.

The required depth of analysis will be determined by the amount of uncertainty that can be tolerated in the risk assessment for a given threat scenario. It must be understood and agreed by the sponsor and the risk analyst as part of the scope setting exercise. Some critical threat scenarios may be very sensitive to system vulnerability (for example, very determined threat adversaries and high value assets) and will require detailed study to reduce uncertainty to an acceptable level. In other cases, significant uncertainty might be tolerable and a cursory analysis will suffice.

Ranking of vulnerabilities is not an essential step. It is only meaningful in the context of specific vulnerability attributes; for example, which attack requires the greater capability. However subjective, it may be useful to rank vulnerabilities as a means to prioritize analysis or focus on the concerns of the sponsor.

2.3.4.2 Safeguard Effectiveness

When assessing the vulnerability of a system that includes existing or proposed safeguards, the effectiveness of these safeguards must be assessed. As safeguards serve one or more distinct functions, it is most useful to view them according to a functional breakdown such as:

- a) prevention and avoidance;
- b) detection;
- c) mitigative (that is, containment and recovery); and
- d) deterrence.

Safeguard effectiveness should be assessed in the light of the functions provided by a safeguard and their relationship to attacks and threat agent capabilities.

Since failure of a safeguard can expose an asset to subsequent attack, it is also important to determine how prone a safeguard is to failure, and whether there are ways that it can be circumvented. In this sense, safeguards become supporting assets in their own right and should be included in the list of system assets that may require protection.

In general, when assessing technical vulnerabilities, mechanisms should not be reviewed in isolation, since vulnerabilities can arise from very subtle and complicated technical interactions.

2.3.5 Threat Scenarios

A vulnerability will not result in a risk to a system asset unless there is a threat agent that can exploit it. The challenge thus becomes matching the assessed characteristics of the threat agents with the system vulnerabilities, that is, developing realistic threat scenarios. In this guide, a threat scenario corresponds to a specific threat agent mounting a specific type of attack in an attempt to compromise (in one or more ways) one or more of the system assets.

The range of all possible threat scenarios can be extremely large. Rather than a brute force evaluation of all possible combinations, the search space should be reduced prior to proceeding with a risk assessment. Reductions can be realized in the following ways:

- a) eliminate combinations that don't make sense;
- b) eliminate combinations based on the agreed scope; or
- c) proceed according to agreed threat agent and/or attack rankings.

Many scenarios can be easily ruled out based on the fact that relationships are contradictory. Incongruities may occur in threat/attack relations (for example, a hacker will not be expected to mount a military attack), asset/attack relations (for example, monitoring radio transmissions will not impact integrity) or in asset/threat relations (for example, a hacker will not be motivated by air conditioning equipment).

2.3.6 Impact Assessment

For each threat event scenario, an impact assessment should be developed which reflects the consequences of the threat event. This assessment corresponds to a single loss expectancy (SLE), and can be used to rank the severity of threat scenarios regardless of their probability of occurrence. The impact will be based on:

- a) which assets are targeted;
- b) the sensitivity of the assets; and
- c) the type and degree of compromise.

The semantics of the risk assessment should match the semantics of the asset sensitivity analysis (and thus the semantics of the SoS). For example, if the asset value is measured in terms of goodwill then the impact should be expressed in terms of loss of goodwill. In many cases, the measure used to express the impact will be multivalued.

The impact assessment should also consider the number of instances of the security domain which are found in the system. Where the attack is likely to compromise more than one instance of a domain, this should be accounted for by the impact assessment. Where threat events impact individual instances of a domain (for example, random failures) the presence of other instances of that domain can be accounted for in the likelihood assessment.

2.3.7 Likelihood Assessment

For each threat event scenario, a likelihood assessment should be developed. Different approaches are required for threat scenarios that involve human agents and those which are due to natural causes and random failures.

For independent threat scenarios in individual domains, the likelihood assessment should account for the existence of multiple instances of security domains.

The likelihood assessment considers many variables and subtle interactions between them. This can introduce considerable uncertainty into the likelihood assessment. Where possible, the degree of uncertainty in the likelihood estimate should be noted. While there are problems, such as hardware reliability analysis, which yield to quantitative analysis approaches, it is much more common that qualitative measures such as low, medium and high will be appropriate for likelihood assessment.

2.3.7.1 Threat Agents

Likelihood is assessed by examining the match between characteristics of the threat agent and the level of effort required to carry out an attack . Aspects to consider include:

- a) threat agent motive;
- b) threat agent determination;
- c) the opportunity available to the threat agent;
- d) the match between threat agent resources and the resources required by the attack; and
- e) the match between threat agent capability and expertise required by the attack.

2.3.7.2 Random Events and Natural Disasters

For random events and natural disasters, likelihood estimates can be obtained by consulting historical records. Random events would include mechanical failures, freak accidents, and power failures. Natural disasters would include earthquakes, floods, and hurricanes.

2.3.8 Risk Assessment

As described above, the risk assessment provides a measure of risk for each threat scenario, reflecting its impact and likelihood. The method of assigning risk should account for the number of instances of the security domain, either through the impact or likelihood assessments (or both).

This form of risk assessment is an average loss expectancy (ALE) over a given period of time. It should be recognized that the ALE has the following characteristics:

- a) there is no distinction between high and low probability events; and
- b) high-impact/low-probability events may be overlooked since they may have a comparable risk value to low-impact/high-probability events.

A distinction should be made between high and low probability threat scenarios. High probability threat scenarios correspond to costs which can be expected to be incurred in the near future, while low probability scenarios represent costs that may never arise. Different mitigative approaches would typically be warranted, even though the ALE is identical.

Very low probability events might average down to acceptable levels of risk, even though the impact of these events might be enormous. In some cases, steps to reduce the impact of these events might be warranted; however improbable they may be. Alternatively, single event loss expectancy (SLE) measures will highlight the most catastrophic scenarios, regardless of probability.

The risk measures used must suit the threat scenario which they measure. A quantitative measure of risk can be developed in some cases. For IT systems, however, there is often uncertainty in many of the risk variables, in which case qualitative risk measures are the most reasonable choice. To be most broadly applicable, risk analysis methods should support a range of risk assessment measures and use the measure best suited to the problem at hand.

2.4 Practical Considerations

Certain practical considerations which are pervasive to the risk assessment method are described below.

2.4.1 Risk Analysis Data

2.4.1.1 Data Organization

Careful attention should be paid when organizing the risk analysis data. It is particularly important to have consistent interpretation of the basic risk elements and their attributes. To reduce the number of possible threat scenarios, threat agents and vulnerabilities should each be broken down into the smallest number of distinct types required to characterize the problem. Vulnerability types should be clearly defined and, as far as possible, mutually exclusive. The same requirement applies to threat agents. This will aid in a consistent interpretation and application of the method.

Vulnerabilities should be characterized in terms of the types of attacks. For each type of attack, the required capabilities and resources, the possible targets and the potential outcomes must be understood. For example, loss of confidentiality of transmitted information as a result of radio intercept (which implies the capability of intercepting

radio transmissions). Characteristics of threat agents should be described in the same terms in order to facilitate the identification of threat scenarios.

The relationships between specific types of assets, threat agents, and attacks (namely, vulnerability information) is extremely useful information to the risk analyst. Much of this information is generally applicable to IT security. Standard relational information should be maintained and made available for subsequent risk analyses. Without access to this type of information, additional unnecessary analysis will be required. Examples of "corporate knowledge" might be: simple lists of known attacks on particular technologies and/or products, complicated large relational databases, or expert system inferencing rules to determine likelihood.

2.4.1.2 Sources of Information

The risk analysis process requires information on the vulnerabilities of the system under review. A range of vulnerability information may be required, depending on the scope of the analysis, from information on generic vulnerabilities of a system architecture through to technical vulnerabilities of specific implementations and security mechanisms.

Vulnerability information can be obtained from: previous analyses, information databases and lists; product reviews or evaluations by security authorities; and institutional security records. Where this information is deficient, vulnerability information can be obtained through detailed analysis of a system and/or security testing.

Threat information can be gathered from a variety of sources including: departmental security records, experience at similar institutions, and lead agencies (that is, CSE, CSIS, and RCMP). Departments should develop databases of recognized threat agents and threat event history, and attempt to maintain the currency of this information. These threat databases can be a valuable aid to risk analysts when assessing risk to the department's IT systems.

Care must be taken to ensure that information obtained from external sources is properly interpreted. A threat assessment, for example, might conclude that threats from a particular source are high without indicating whether this reflects capability or motivation.

2.4.1.3 Support Tools

Except for relatively simple risk analyses, some form of (semi-) automated tool support may be very desirable. The typical risk assessment will involve a large number of component assessments which must be tracked, maintained and modified. Without good tools, it will be difficult for the analyst to efficiently manage this data.

The tool should allow the risk analyst to effectively exploit an existing risk analysis knowledge base by providing generic vulnerability relationships, by suggesting what type of additional information is required to characterize threat agents or attacks and by automatically eliminating unrealistic threat scenarios. It should also enhance productivity

by automatically incorporating changes in the underlying assumptions (for example, the characteristics of threat agents) into subsequent assessments.

Other capabilities which are desirable in a risk analysis tool include:

- a) the flexibility to support a range of technologies;
- b) support for the analysis of both existing and planned systems;
- c) recognition of Government and departmental policies and standards;
- d) the ability to backtrack to identify the detailed threat scenarios;
- e) the ability to temporarily add safeguards, reassess risk, and then roll back to the original system configuration;
- f) a facility for modifying and/or updating the knowledge base;
- g) the ability to suggest safeguards appropriate to the level of analysis detail; and
- h) good reporting capabilities.

Additional factors to consider when selecting a product include initial cost, the availability of support and training, the amount of risk analysis and tool specific expertise required of the user and the potential of the tool to improve risk analysis productivity.

There are a number of risk assessment or analysis methods and automated packages available in the marketplace. Unfortunately, many of these are audit oriented and are most applicable to in-place systems. Such tools typically provide extensive checklists of security factors to consider and can be valuable in ensuring that all aspects of the IT security problem have been addressed. Their use is often limited, however, when applied to security problems that must be addressed during system development.

2.4.2 Risk Report

The principal output of a risk assessment will be a risk report. This report should:

- a) clearly identify the system under review;
- b) include the system description;
- c) state the aim of the risk analysis;
- d) outline the scope of the study;
- e) summarize the analysis approach used in the study;
- f) itemize the detailed risk assessment (for example, in a risk summary table);
- g) provide explanations which support the assessment of risk; and
- h) identify options for reducing risk.

A template for the system risk report is included in Annex C.

While detailed risk assessments are required to support requirements definition and safeguard selection activities, summaries of the risk results will usually be required by

management to support decision making activities. The summary risk results should highlight areas of concern and outline management options. The detailed risk assessment results can be referred to when answers to "why" and "what can we do" questions arise.

When a risk assessment involves detailed analysis of vulnerabilities that might be reusable in subsequent studies, this information should be added to the corporate knowledge base (by adapting and extending lists, augmenting the database, or adding inference rules).

2.4.3 Sensitivity of Risk Assessment Information

Threat scenarios are essentially "how to" descriptions of potential attacks. This information would be of great interest to threat agents. Additionally, the list of threat scenarios considered may show limitations in the risk assessment (that is, threat scenarios which were not considered and could be potential weaknesses). Therefore, the risk assessment information is sensitive and should be classified or designated as:

- a) the highest system asset; and
- b) greater than the highest system asset if threat scenarios are applicable to other systems of higher assets (for example, crypto vulnerability information might be Top secret since the crypto may be used in systems up to that classification).

2.5 Recommendations

The risk analyst will usually recommend further refinements to existing, or proposed, safeguards in order to reduce the risk to an acceptable level. If no appropriate safeguards are available, the risk analyst may suggest changes to the system design to remove or move sensitive assets, in order to avoid or transfer the risk. If the risk is acceptable, the risk analyst will suggest that the life cycle process proceed to the next step.

2.6 Requirements Definition

Security requirements are defined by examining the threat scenarios that result in unacceptable risk, and determining what security attributes is required to reduce the risk.

2.7 Safeguard Selection

Engineering secure solutions presents some difficult challenges. The expense of safeguards, in terms of cost, system performance, user acceptance, and a myriad of other factors, must be balanced against the resulting reduction of risk.

2.7.1 Developing Safeguard Options

In the design of the overall system, technical and non-technical safeguards must be specified. Technical safeguards are technology based, and non-technical safeguards are procedural, administrative, physical and personnel based.

2.7.1.1 Safeguard Groups

The description of safeguards in the IT system should be partitioned in a structured manner, to ensure that all required security issues have been addressed. There are several ways to group system safeguards in system documentation, such as:

- a) Administrative and Organizational Security
- b) Personnel Security
- c) Physical and Environmental Security
- d) Hardware Security
- e) Software Security
- f) Operations Security
- g) Communications Security (COMSEC)
- h) Transmission Security (TRANSEC)
- i) Cryptographic Security (CRYPTOSEC)
- j) Emission Security (EMSEC)
- k) Network Security (NETSEC)

A more detailed description of the possible safeguard groups is found in Annex D.

2.7.1.2 Safeguard Attributes

The selection of safeguard options will be based on three main attributes: function, strength, and correctness. The function of a safeguard describes the type of protection that a safeguard provides. The basic types of security functions are: avoidance, deterrence, prevention, detection, containment, and recovery. These functions reduce the likelihood or impact of a threat scenario in the calculation of risk in a system by influencing the threat agents, the asset values or sensitivities, and/or the system vulnerabilities. For example, a deterrence safeguard will deter a threat agent from attempting an attack, thereby reducing the likelihood of an attack.

The strength of a safeguard provides an indication of the effort which would be required to overcome it. The target strength depends on the security requirement being satisfied by the safeguard. The actual strength is determined by the correctness of implementation, by the security requirements it satisfies, and by the supporting safeguards that it requires to operate. A measure of strength generally applies to safeguards which reduce system vulnerabilities, and provides an indication of the

capabilities and resources which are required for a threat agent to overcome the safeguard.

Safeguard correctness is an indication of the lack of flaws in the safeguard implementation. If a safeguard is implemented incorrectly, it is ineffective and will not mitigate the risk. For example, security programs based upon administrative procedures have sometimes failed because they were not implemented correctly. Therefore, it is important to have a sufficiently high level of assurance in the correct implementation of the chosen safeguard. The minimum level of correctness is suggested in the risk assessment recommendations when the risk is at an unacceptably high level.

2.7.2 Trade offs

If more than one safeguard option exists, then the most appropriate option must be selected. To aid the selection process, the cost and the effectiveness of each safeguard option must be assessed to ensure that the most appropriate safeguard option is selected.

2.7.2.1 Safeguard Cost

Cost considerations impact on virtually all management decisions, including safeguard selection. The acquisition installation costs of a safeguard or a suite of safeguards is relatively easy to identify. Other costs must also be considered to determine the overall cost. Other costs include training requirements and ongoing operating expenses such as power, personnel and maintenance costs. Indirect costs such as reduced or improved productivity due to the safeguard functionality must also be considered. Other cost factors to consider include the life expectancy of the safeguard and the asset it protects, and the incremental cost to certification that the safeguard adds.

2.7.2.2 Safeguard Effectiveness

Safeguard effectiveness is a measure of the effect that a safeguard has on the likelihood and impact of a threat scenario. Multiple factors will influence the overall effectiveness of a specific security safeguard. Additionally, an examination of safeguard attributes described in Section 2.7.1.2 will provide useful information which can be used in conjunction with the other factors in the trade off analysis:

- a) **Vulnerabilities Addressed and Dependency on Other Safeguards.** When choosing between safeguard options, the number of vulnerabilities that a safeguard option addresses provides a measure of the option's flexibility. However, other factors such as its dependence on other safeguards and its vulnerability to attacks must be assessed. Safeguards which rely upon other security features for successful operation are generally less desirable than those which operate independently. Conversely, a safeguard option which supports or enhances other safeguards is generally a desirable option.
- b) **Vulnerability to Failure/Evasion.** The vulnerability of the safeguard option to accidental failure and deliberate evasion must also be assessed. Its reliability, robustness, complexity, maintenance and ease of use are important

considerations. Generally, the less vulnerable safeguard is more desirable than the more vulnerable option.

- c) **User Acceptability.** The acceptability by users and operators are also important considerations in assessing the safeguards effectiveness. If a safeguard requires that the users and operators rigorously and conscientiously apply it, then the safeguard should be convenient, easy to use and user friendly. Otherwise, it will not always be applied, and will not be very effective. For example, an access control mechanism based on multiple unpronounceable passwords can be frustrating for the users, and therefore, counterproductive. Other examples affecting acceptability include real or imagined safety concerns with certain devices like retinal scanners.
- d) **Human Intervention.** Safeguard options with a requirement for human intervention or interpretation are generally less reliable than automated options, especially if they are awkward or inconvenient to manage. Only the most diligent individuals will continually respond quickly and accurately, and will not ignore or disable the safeguard. Conversely, safeguards that do operate independently can be made more effective with human intervention as a backup or response capability.
- e) **Visibility.** Highly visible safeguards such as a chain link fence or well publicized access control system are more likely to have desirable deterrent effects. However, visibility may make the safeguard more susceptible to tampering by providing a threat agent the opportunity to study its vulnerabilities.

2.7.3 Selecting the Preferred Option

The results of the trade off analysis will provide an indication of the cost, the effectiveness and the reduction of risk for each safeguard option. The options should be ordered to reflect the degree of satisfaction from a security standpoint. A preferred option should be highlighted with a brief explanation indicating why it was chosen. The consequences of selecting another option over the preferred option should also be discussed.

3. LIFE CYCLE PROCESS GUIDANCE

3.1 Introduction

This chapter provides detailed life cycle guidance for risk assessment and safeguard selection. Guidance is presented in the context of the advice in Chapter 2 and the six stage system life cycle introduced in the *Guide to Security Risk Management for Information Technology Systems*. At each stage of the life cycle, critical deliverables will be baselined, or frozen. Other activities will then proceed using these baselined items as inputs. Any changes to baseline deliverables must proceed in a controlled manner, and lead to review and, if required, update of subsequent deliverables.

The life cycle of a typical IT system (or change to a system) proceeds through a series of iterations which successively refine the system specification and implementation. Within each iteration, risk assessment, and possibly safeguard selection, may be conducted. Depending on the stage of the life cycle, risk assessment may be used to generate security requirements or to assess the risk associated with existing (or proposed) safeguards. Safeguard selection might generate high level or detailed security requirements.

In practice, when developing IT system design alternatives or the detailed design, risk assessment and safeguard selection will occur concurrently rather than sequentially. Significant interaction between these activities is usually required for efficient system development and safeguard optimization. These activities are inherently iterative, particularly within these life cycle stages. Hence, concepts and rough drafts should be exchanged between the risk analyst(s) and security engineer(s), in order to gain insight and promote effective trade-off analysis.

3.2 Planning for Change

During this stage of the life cycle, the need for change is reviewed, program options are examined, the risks associated with each program option are assessed, and a decision is made on whether to proceed with a program of change.

3.2.1 Aim and Scope

At this life cycle stage, the aim of the IT system risk assessment and safeguard selection is to determine the types of security risks that will need to be addressed in the program options, and the types of technology that will be needed to address the security risks.

3.2.2 Required Inputs

The following inputs are required:

- a) **System Description.** The description may only contain location information and the sensitivity of assets within the system. Any description on location environments should be included.
- b) **System Mission.** A description of the primary functions of the system and how the system will be used.
- c) **Program Options.** A description of how the program will be implemented.

3.2.3 Risk Assessment Approach

At this life cycle stage, a high-level assessment of system risk is required. The environment where system assets are located will identify the threat agents to be used in the risk assessment. These threat agents are assessed in conjunction with the sensitivity of system assets in an environment to determine the types of security risks which will need to be addressed within the system design.

3.2.4 Safeguard Selection Approach

Safeguards are not specified. However, the security engineer may be able to indicate whether adequate safeguards are available within the timeframe of the system's implementation, and what the required level of effort would be if the safeguards were to be built by the project.

3.3 Requirements Definition

During this life cycle stage, functional, operational, and security requirements for the IT system will be developed and baselined. The security requirements will be influenced by key risk factors which are identified in the risk assessment process.

3.3.1 Aim and Scope

The risk assessment process will be used to develop functional security requirements for the proposed, or modified, system. The process considers assets, threat agents, and generic methods of attack to identify key risk factors which will determine the functional security requirements. In most cases, specific IT platforms and processes have not been identified, and the focus must be on generic attack on the system. To maximize the options available to system and security engineers, the functional security requirements should be expressed in functional terms which permit a broad range of solutions.

3.3.2 Required Inputs

The following inputs are required:

- a) **IT system description.** The content of the IT System Description is described in Section 2.2.3. The operational requirement, concept of operations, policy

framework, location, and anticipated modification/expansion elements of the IT System Description should be populated and baselined. Some of these elements may have been populated in a previous life cycle stage. The system design element should be populated based on a high-level description of the IT system (excluding any IT safeguards and including any known environmental safeguards).

- b) **Statement of Sensitivity.** A preliminary Statement of Sensitivity is produced during this life cycle stage as discussed in the *Guide to Security Risk Management for Information Technology Systems* and Section 2.2.5.
- c) **Aim.** The aim of the risk assessment is to determine all key risk factors (possibly constrained by cost, time, resources, policy/standards, and method/tool). If a complete list of risk factors is required, the IT system is assumed to have no inherent safeguards (note that environmental safeguards may exist).

The aim of the safeguard selection is to determine a complete list of functional security requirements (possibly constrained by cost, time, resources, policy/standards, method/tool, and technology). These will be derived from baseline requirements identified in the system specific security policy and from the key risk factors identified above.

- d) **System Boundary.** The system boundary is described in Section 2.2.2. The system boundary is baselined during this life cycle stage.
- e) **Scope.** The risk sponsor may choose to focus the risk assessment and safeguard selection on project-specific issues. The breadth of analysis will generally include all of the IT system contained within the system boundary. The depth of analysis will usually address specific assets and threat agents (based on available information), and general vulnerabilities.
- f) **Target Risk and Certainty.** The target risk must be established prior to the end of the risk analysis and baselined at that point. The required level of certainty in the risk assessment (at this stage and also prior operations) should also be established.
- g) **Threat Briefings.** Threat briefings pertinent to the Government of Canada, the department, and the IT system should be collected. Lead agencies (that is, CSE, CSIS, and RCMP) can help in compiling relevant threat information. A discussion of generic threat agents is included in Annex A.
- h) **Generic Vulnerability Information.** A discussion of generic vulnerabilities is included in Annex B.

3.3.3 Risk Assessment Approach

The risk assessment proceeds as follows:

- a) Depending on the complexity of the system and the focus of the analysis, the system might be decomposed into domains according to the guidance in Section 2.3.1.3.

- b) An asset sensitivity analysis should be performed based on the preliminary SoS. During this analysis, the sensitivity of the IT resources (such as hardware, software, interfaces and support systems) should be determined. Asset sensitivity should be documented for each domain.
- c) A detailed threat analysis should be done based on the compiled threat briefings to identify and characterize significant threat agents.
- d) A general vulnerability analysis should be done based on the high level system description to determine significant attacks on the system.
- e) A list of realistic threat scenarios based on meaningful products of assets, threat agents, and vulnerabilities is then compiled.
- f) An impact statement for each threat scenario should be developed to the level of detail in the asset sensitivity analysis.
- g) A general assessment of likelihood should be made for each threat scenario with some indication of its uncertainty.

If a target risk has not yet been identified, it should be done now with consideration given to the identified threat scenarios. The target risk will describe the level to which threat scenarios should be mitigated and help determine the key risk factors.

Key risk factors such as high asset sensitivity, significant threat agents, and significant system vulnerabilities are identified in a review of the risk assessment results. The ranking of the impact of threat scenarios containing these key risk factors is a useful means of ranking the risk factors, and identifying those which should influence security requirements.

3.3.4 Safeguard Selection Approach

Once the key risk factors have been identified and prioritized, functional security requirements should be developed. These security requirements are high level statements of countermeasures which will mitigate the risk factors. They are stated in functional terms, and do not require fine detail.

The functional security requirements should be partitioned in a structured manner, to ensure that all required security issues are addressed. Requirements for confidentiality, integrity, availability, and accountability should be provided for components in the IT system. Functional security requirements should satisfy applicable security policies and standards which govern the system. The level of detail that is required to validate that the functional security requirements meet the applicable policies is determined by the validation requirements described in the *Guide to Certification and Accreditation of Information Technology Systems*. The initial risk assessment should help ensure that applicable standards are applied in a cost effective manner.

The system constraints are always a major factor in the definition of the security requirements, since these will introduce limitations and trade offs. Finally, it is important to keep in mind the operational requirements for the system. Important decisions

regarding the system's security features will likely be influenced by their operational impact on the system.

The functional security requirements should be subjected to a quality test. The objective of this test is to ensure that the requirements are:

- a) consistent (are there conflicting or ambiguous requirements?);
- b) complete (do they address all key risk factors and security standards mandated by policy?);
- c) appropriate (are requirements cost effective, and not unnecessarily restrictive?);
- d) implementable (is there confidence that the requirements can be met?); and
- e) verifiable (can tests demonstrate the degree to which requirements have been met?)

Assistance in identifying appropriate security requirements is available from lead government agencies, and institutions are encouraged to consult with these lead agencies should they have any questions or require assistance.

The level of protection and assurance required for security functions should be specified, where appropriate, with a reference to particular threat scenarios and the level of risk reduction required of the safeguard. Reference to the system specific security policy requirements should also be provided for certification purposes.

3.3.5 Outputs

The output of the risk assessment should be:

- a) a prioritized list of risk factors;
- b) a summary of system risk; and
- c) target risk.

The output of the safeguard selection activity should be a statement of functional security requirements.

3.4 Architecture Design

During the architecture design stage, secure system architecture alternatives are developed with recommendations for specific safeguards. For each architecture alternative, a risk assessment is conducted to establish the level of risk associated with the recommended safeguards. Risk is one of the key inputs to the cost benefit analysis which will result in the selection of a preferred design.

3.4.1 Aim and Scope

The aim of safeguard selection is to select safeguards for each preliminary design alternative as part of the engineering process. The aim may be constrained by cost,

time, resources, policy/standards, method/tool, and technology. The safeguard suite for each alternative must meet the functional security requirements.

The aim of risk assessment is to provide a detailed measure of risk for each preliminary design alternative to establish the level of risk reduction associated with its suite of safeguards. This process may be iterative as part of the safeguard and design engineering process. The aim may be constrained by cost, time, resources, policy/standards, and method/tool.

The scope of these activities will be highly dependent on the particular IT system. For a large or complex system, design options may correspond to significantly different system architectures. In the case of simpler systems, this step may involve examining one or two minor design alternatives.

3.4.2 Required Inputs

The following inputs are required:

- a) **Baselined System Boundary.**
- b) **IT system description.** The system design element will differ for each design alternative and will include the selected suite of safeguards. All other elements of the system description were baselined during the Requirements Definition life cycle stage.
- c) **Scope.** The risk sponsor may chose to focus the risk assessment and safeguard selection based on project specific issues. The breadth of analysis will generally include all of the IT system contained by the system boundary. The depth of analysis will generally be dictated by the level of detail in the system description.
- d) **Statement of Sensitivity.** The preliminary Statement of Sensitivity produced during Requirements Definition may be refined for each design alternative as discussed in the *Guide to Security Risk Management for Information Technology Systems*.
- e) **Target Risk and Certainty.** The target risk was baselined during the Requirement Definition. The level of certainty required in the analysis will generally be dependent on the assurance requirements (that is, the amount of risk reduction) of the functional security requirements.
- f) **Threat Briefings.** Threat briefings pertinent to the Government of Canada, the department, and the IT system should be collected. Lead agencies (that is, CSE, CSIS, and RCMP) can help in compiling relevant threat information. A discussion of generic threat agents is included in Annex A.
- g) **Vulnerability Information.** More detailed vulnerability information is required based on the technology choices made in each design alternative (for example, specific vulnerabilities of client/server architectures might be required for one design alternative, and mainframe vulnerabilities may be required for another).

- h) **Requirement Definition Risk Assessment.** Information from the previous risk assessment may be used if elements of the analysis (for example, the asset sensitivity valuation or the threat analysis) are still valid.

3.4.3 Safeguard Selection Approach

A set of projected system architecture options will have been developed as possible candidates which fulfill both the operational and the security requirements of the system. These system architecture options contain high level system descriptions, and should include general detail on system configuration and assets.

These architecture options should now be further developed into preliminary design alternatives. A set of technical security safeguards with proposed levels of assurance should be developed for each preliminary design alternative. The implications for supporting operational safeguards (that is, administrative, physical, operational, and personnel) should also be examined and documented. For each preliminary design alternative, the system specific security policy is refined into a Technical and Operational security policies in order to reflect the technical and non-technical split in safeguards.

The technical safeguards must satisfy the functional security requirements developed in the requirements definition stage. Guideline documents such as the *Trusted System Environment Guideline* provide guidance on choosing appropriate safeguards. The statement of sensitivity provides much of the information required to make effective use of these documents. Policy, standards and criteria documents such as the *Government Security Policy*, *Canadian Trusted Computer Product Evaluation Criteria*, *Technical Security Standards for Information Technology*, and the *DoD Trusted Computer System Evaluation Criteria* contain important safeguard information.

Safeguard details should describe, at a high level, physical security, operational security, administrative security, personnel security, COMPUSEC, CRYPTOSEC, EMSEC, TRANSEC, and NETSEC. For certification purposes, references to the system specific security policy, functional security requirements, and the key risk factors should be available for validation of the selected safeguards.

3.4.4 Risk Assessment Approach

A risk assessment should be performed for each proposed preliminary design alternative. Each risk assessment should include the following:

- a) The decomposition from the Requirement Definition risk assessment should be evaluated for its applicability to the preliminary design alternative; further refinements to the decomposition for a preliminary design alternative may be required.
- b) If there have been any changes to the preliminary SoS or the Requirements Definition decomposition, the asset sensitivity analysis should be updated to reflect these changes.

- c) If additional or more detailed threat briefings are available, the threat analysis should be updated to reflect the additional information.
- d) A detailed vulnerability analysis should be done based on the Requirement Definition vulnerability analysis and vulnerability analysis information of each proposed preliminary design alternative that may be available.
- e) A list of realistic threat scenarios based on meaningful products of assets, threats, and vulnerabilities is then done. The number of threat scenarios may change based on changes to the asset, threat, or vulnerability analyses.
- f) An impact statement for each threat scenario should be developed to the level of detail in the SoS.
- g) An estimate of likelihood, including an indication of the uncertainty of the information should be developed for each threat scenario.
- h) At this point measures of the risk can be derived.

Since the system is still in a design stage, there will be areas where there is a high degree of uncertainty in the risk assessment results. The purpose of the risk assessment is to identify vulnerabilities to the extent possible and develop an estimate of the associated potential risk. This approach will help focus any subsequent detailed risk analysis.

System composability issues must be considered in systems which are composed of smaller systems with different security properties and levels of assurance. The interaction of security services in the overall system may produce undesirable system vulnerabilities which must be identified. *Composable Trusted Systems* contains research results in the area of system composability.

The resulting risk assessments for each preliminary design alternative will be inputs to a trade-off analysis which will recommend a preliminary design alternative based on cost, operational, and security considerations. If required (that is, a preliminary design alternative still has some unacceptable risk), additional security requirements may be recommended in order to reduce the risk.

3.4.5 Outputs

For each preliminary design alternative, the following are required:

- a) technical and operational security policies;
- b) a proposed set of safeguards (including additional safeguards resulting from the risk assessment); and
- c) an assessment of risk.

At the end of this stage, the selection of a preliminary design will be made based on the assessed risk and the associated costs of the selected safeguards.

3.5 Detailed Design

The detailed design stage begins once the system architecture has been selected, and results in a complete system specification, suitable for implementation.

3.5.1 Aim and Scope

The aim of the safeguard selection at this stage of the life cycle is to develop detailed technical and operational security specifications for the chosen preliminary design.

The aim of the risk assessment is to assess the risk associated with the detailed design. The availability of additional technical detail will allow a more thorough risk analysis to be conducted; critical vulnerabilities should be examined in detail. During the detailed risk assessment, all aspects of the original risk assessment are reviewed to ensure their validity. Vulnerabilities will be more clearly understood, and the detailed risk assessment can focus on critical vulnerabilities and a thorough analysis of risk in these areas.

3.5.2 Required Inputs

The following inputs are required:

- a) **Baselined System Boundary.**
- b) **IT system description.** The system design element will be the detailed design developed during this life cycle stage. All other elements of the system description were baselined during the Requirements Definition life cycle stage.
- c) **Scope.** In general, the risk analysis and safeguard selection will focus on security critical areas of the system. The depth of analysis will generally be detailed for assets and threats, and very detailed for vulnerabilities.
- d) **Statement of Sensitivity.** The SoS may be refined based on the detailed design as discussed in the *Guide to Security Risk Management for Information Technology Systems*.
- e) **Baselined Target Risk and Certainty.**
- f) **Vulnerability Information.** More detailed vulnerability information will be required based on the safeguard and technology choices made in the detailed design.
- g) **Chosen preliminary design alternative Risk Assessment.** The risk assessment from the previous life cycle stage should be used as a basis for analyzing risk in the detailed design.

3.5.3 Safeguard Selection Approach

In this stage, the high level architecture and safeguards are expanded into a detailed design. Since the physical location is known, physical and TEMPEST surveys may be needed to provide additional information on the required physical and technical

safeguards. Computer security expertise may be required in order to properly address relevant security issues.

The technical security policy, operational security policy, and security safeguards developed during the architectural design stage should influence the development of the detailed design. The required level of assurance of the system and its components, and the risk assessment from the previous design stage should also influence the detailed design.

As indicated in the *Guide to Security Risk Management for Information Technology Systems*, the detailed system design should include

- a) A complete listing and description of all system components, including hardware, software and firmware;
- b) A detailed specification for each of the system (including security) components;
- c) A full description of how each of the system components are to be interconnected, including information on networking protocols and security mechanisms;
- d) A profile of system users, together with their respective security clearances, roles and privileges;
- e) A detailed description of all technical safeguards, in support of the technical security policy;
- f) A detailed description of the system's expected physical environment;
- g) A description of physical, personnel and administrative safeguards; and
- h) Specifications for construction of computer rooms (environmental specifications).

3.5.4 Risk Assessment Approach

Once the detailed design has been completed, a detailed risk assessment is performed. The detailed risk assessment should consist of the following steps:

- a) The decomposition from the preliminary design alternative risk assessment should be evaluated for its applicability to the detailed design; further refinements to the decomposition may be required.
- b) If there have been any changes to the SoS or the preliminary design alternative decomposition, the asset sensitivity analysis should be updated to reflect these changes. The asset inventory should be updated to include supporting assets, as well as any modifications or additional information not previously available.
- c) The threat analysis should be reviewed. More information on specific threat agent capabilities is typically required.
- d) A very detailed vulnerability analysis should be done based on: the preliminary design alternative vulnerability analysis, the detailed system design, the detailed design safeguard effectiveness, and more specific vulnerability information obtained during this life cycle stage. Administrative, physical, personnel, procedural, and technical safeguard mechanisms should be reviewed to identify the effectiveness with which assets are protected against the previously identified

threat events. The vulnerability assessment should not be entirely dependent on known threat agents or the preliminary design alternative threat scenarios since future threat agents may be capable of exploiting these vulnerabilities.

- e) A complete set of threat scenarios, relative to the identified system vulnerabilities, should be assembled. These scenarios should be further refined, in terms of detail. The results from the asset review, safeguard review and vulnerability assessment are used in analyzing threat scenarios, in the specific context of security mechanisms and functional characteristics of the system architecture.
- f) An impact statement for each threat scenario should be developed to the level of detail in the SoS.
- g) A detailed estimate of likelihood, with some indication of the uncertainty should be developed for each threat scenario.
- h) At this point measures of the risk can be derived.

3.5.5 Outputs

Detailed specifications ready for implementation, and a revised statement of risk are the outputs from this life cycle stage.

3.6 Implementation

The system implementation stage constructs and installs the designed system and the supporting mechanisms and procedures. From the security perspective, this phase includes security testing and verification, finalizing the assessment of the risk, and the system accreditation decision.

Where the certification reports indicate that not all security requirements have been satisfied, the accreditor may request a risk assessment of the non-compliance. This assessment will support the accreditor's decision to grant a waiver, or require that the non-compliance be addressed.

3.6.1 Aim and Scope

The aim of the risk assessment is to identify any residual vulnerabilities or compromising side effects, and to assess the impact on risk associated with any identified non-compliance uncovered during security testing and verification.

The scope of the risk analysis will be limited in breadth to critical vulnerabilities, and a focused analysis of non-compliance. At this point, risk analysis can be conducted at a very detailed level.

Safeguard selection will typically be limited to enhancing secure operating procedures to account for any identified vulnerabilities or deficiencies in technical security measures.

3.6.2 Required Inputs

The following inputs are required:

- a) **Baselined System Boundary.**
- b) **Baselined IT system description.**
- c) **Scope.** The scope of analysis at this point will be restricted to a detailed analysis of non-compliance with the system specifications and procedures, and resolution of any unacceptable risks.
- d) **Baselined Target Risk and Certainty.**
- e) **Vulnerability Information.**
- f) **Detailed Design Risk Assessment.** The risk assessment from the previous life cycle stage should be used as a basis for analyzing risk in the implementation.

3.6.3 Risk Assessment Approach

Where the certification reports indicate that not all security requirements have been satisfied, or there are unexpected vulnerabilities not foreseen during previous risk assessments; the accreditor may request a risk assessment. If a risk assessment is requested, a review of the Detailed Design risk assessment is performed focusing on the areas of non-compliance, in order to determine any change in the measure of risk. This risk assessment will support the accreditor's decision to grant a waiver, or require that the non-compliance be addressed.

3.6.4 Safeguard Selection Approach

Once security testing and evaluation has been completed the secure operating procedures should be updated, if required, to address any additional vulnerabilities.

3.6.5 Outputs

The outputs include a statement of risk and finalized secure operating procedures. The statement of risk describes the residual risks and vulnerabilities, and is formally accepted by Accreditation and Operational Authorities to demonstrate their acceptance of the residual risks and vulnerabilities.

3.7 Operation

Given the dynamic nature of IT systems, technological advances, and changing threat environment, a risk assessment should be undertaken periodically to ensure that the risk remains within the target risk (that is, acceptable limits). Additionally, the GSP requires

that risk assessments be performed every five years, at a minimum. Risk should also be re-assessed when:

- a) a security breach or attempted security breach is detected;
- b) significant changes to threats to the IT system occur; or
- c) the system requirements change.

If a previous risk assessment exists, it should be reviewed to determine if it remains valid. If no previous risk assessment exists, a risk assessment of an operational system will help determine the necessity and sufficiency of existing safeguards, in addition to the acceptability of the risk. Risk assessments on operational systems should follow the same approach outlined in this life cycle description. An initial high level risk analysis may provide a sufficiently certain assessment of risk, or it may identify security critical areas requiring a more detailed analysis. When (potentially) unacceptable risks are identified, a detailed risk assessment is required.

If changes are required to the security posture of the system, they should be undertaken according to the system life cycle described in this chapter.

ANNEX A – GENERIC THREAT AGENTS IN IT SYSTEMS

1. Threat Agent Categories

A threat agent breakdown into broad categories is as follows:

- a) **Outsider** - The threat agents are persons who are not legitimately associated with the system.
- b) **Insider** - The threat agents are persons legitimately associated with the IT system. This can include unintentional damage through human error or accident. It can also include intentional damage or compromise by dishonest or disgruntled employees.
- c) **Other** - These threat agents include a wide variety of sources such as natural disasters (for example, fire, storm, flood, etc.) and mishaps such as equipment or power failure.

1.1 Outsider Threat Agents

The outsider threat agent could be a member of a foreign national intelligence agency, criminal elements such as drug traffickers, rival companies or agencies, etc. Each threat agent will have a motivation for targeting IT system assets. Examples include:

- a) foreign national intelligence agencies will likely be motivated to collect information on economic, military, political or high technology targets;
- b) a hacker may be motivated out of curiosity to learn how the technology works;
- c) a "technical wizard" hacker may be motivated by the challenge;
- d) a hostile intelligence service or criminal hacker may be motivated to commit fraud and steal communications services; and
- e) a terrorist group might be motivated to inflict maximum damage on IT systems and organizations for a variety of political, ideological or personal reasons.

Each threat agent will have some assumed level of capability to mount certain types of attacks on an IT system Examples include:

- a) military and national intelligence services have used advances in telecommunications and IT systems to perform espionage attacks. This includes the development of a variety of techniques and platforms for gathering information that range from the employment of satellite technology (and other airborne surveillance platforms) to advances in the more traditional activities of wire-tapping and the planting of clandestine listening devices. Supercomputer technology is routinely employed in code breaking efforts and extensive use is made of the latest advances in IT systems to collate and analyze vast quantities of information. While these

advanced efforts have more traditionally been focused on military and national interest targets, there is evidence that with shifts in the global balance of military power, at least some national intelligence efforts are now focusing on industrial espionage. It would be reasonable to expect that advanced techniques may also proliferate to other areas and enhance private industrial espionage and criminal efforts.

1.2 Insider Threat Agents

Insider threat agents can be broken into two distinct classes: intentional and unintentional. The unintentional insider will cause damage to the IT system unintentionally through negligence or through an accidental error. The intentional insider threat agent will maliciously cause damage to the IT system. These threat agents may be disgruntled, dishonest, persuaded or subverted personnel, where personnel includes employees, contractors, and consultants.

1.3 Other Threat Agents

The other threat agents category spans natural phenomena and random occurrences such as fire, flood, earthquake, power failure, and equipment malfunction. An examination of historic information may be useful in assessing the likelihood of these threat agents.

2. Finer Granularity of Threat Assessment

At an even finer granularity, one could consider specific threat agents in the IT system's environment. Here one may be interested in examining the threat agents in more detail and look at factors such as: motivation, assets targeted, and capability for a carrying specific types of attack. For detailed risk assessments, this finer granularity of threat agent assessment will be required. For example, it may be necessary to determine whether the threat agent has the motivation and capability for mounting a successful attack on an IT system.

3. For Help

The "lead agencies for security" in the Government of Canada (that is, CSIS, CSE and RCMP IT Security Branch and the Commercial Crime Division) may be able to provide assistance in determining the threat agents that would be motivated to "attack" a specific IT system. Useful categories to research, independently or with the help of lead agencies, may be:

- a) listings of the most current IT security incidents;
- b) plausible methods of attacking a specific IT architecture;
- c) identification of potential threat agents; and
- d) assessment of the technical capabilities of threat agents.

ANNEX B – GENERIC ATTACKS ON AN IT SYSTEM

1. Introduction

In the vulnerability analysis, the system analyst tries to determine how “vulnerable” system components are to attacks or threat events. In this annex, generic attacks or threat events will be outlined. These threat events can be used to describe most threat agent attacks. However, as IT technology advances it may be necessary to expand the list to include new types of attacks. Or, if more detail is required, a generic threat event may be replaced with several detailed threat events.

The threat events listed in this annex are grouped by generic attacks on component types. The component types that were considered are:

- a) Environment;
- b) Equipment;
- c) Interfaces;
- d) Processes; and
- e) Personnel.

Threat events were not considered for information components, since the compromise of information will be considered in the impacts or consequences of a successful attack on the above components.

2. Sequences of Threat Events

When identifying threat scenarios, a threat agent will generally use a sequence of threat events to compromise system assets. The following table indicates some possible sequences of events. Note: the list is by no means complete.

Table I – Sequence of Threat Events

Event 1	Event 2
Physically Access an Environment	Alter Equipment Attack on Personnel Logically Access a Process Physically Damage or Destroy Equipment Theft of Equipment
Electronically Access a Process	Logically Access a Process

Event 1	Event 2
Intercept/Transmit on an Interface	Alter data on the Interface Exploit Covert Channel Logically Access a Process Traffic Flow Analysis
Cutting Cable on Interface	
Jam/Flood Interface	
Software failure in Process	
Environmental Extremes on Equipment	
Hardware failure in Equipment	
TEMPEST Attack on Equipment	
Physical Attack on Environment	
Loss of Personnel	

3. Attacks on IT System Environment

3.1 Physical Attack

A physical attack on an IT system's environment implies attacking the environment that houses all or portions of the IT system using force. For example, a car bomb, armed thugs, artillery attack, etc. This type of attack may disrupt the service that the IT system provides.

3.2 Physical Access

Gaining physical access to an IT system environment implies gaining access to a building, floor, or room that houses all or part of the IT system. System personnel will have a legitimate need for physical access while outsiders must surreptitiously gain access (for example, by breaking and entering during off-hours, or by sneaking past access control checks).

Threat agents may attempt to gain unauthorized access to computer facilities by simply going through access control points along with or behind an authorized person. An outsider with a few simple props, such as carrying some typical computer equipment or wearing a lab-coat embossed with a common computer company logo, may "piggyback" past access control points that are not carefully monitored.

4. Attacks on Equipment

4.1 Alter Equipment

The alteration of equipment implies a change in the equipment's configuration that will not make the hardware totally unavailable. That is, changes in the configuration will not prevent the equipment from operating but would allow the threat agent to alter the way the equipment operates.

4.2 Environmental Extremes on Equipment

This threat event implies the failure of equipment due to environmental extremes such as very high or very low temperatures, high humidity, wind storms, tornadoes, lightening, flooding, rain, and earthquakes.

4.3 Hardware Failure of Equipment

This threat event only pertains to IT system hardware, and not to support equipment such as air conditioners. For example, an air conditioner failure will cause an extreme temperature environment and would not be considered in hardware failure.

4.4 Physically Damage or Destroy Equipment

This threat event includes vandalism to system equipment.

4.5 TEMPEST Attack

The threat agent mounting this type of attack requires the right type of monitoring equipment to intercept electromagnetic emissions. Attacks range from analyzing direct radiation from visual display units traveling through free space, to tapping into secondary conductors (for example, power lines) that might carry signals bearing information, to acoustical monitoring and analyzing the sounds of certain types of equipment. The known attacks have focused on military targets and foreign missions. There is no reason why such attacks would be limited to these areas; considering general increases in technical capability and shifts in the targeted assets by foreign intelligence services to include industrial and economic espionage. It should be noted that attackers utilizing this attack have sometimes resorted to the planting of clandestine transmission devices within IT systems to enhance the range of signals that can be detected; this type of attack typically implies collusion with repair or supply facilities or cooperation with an insider.

4.6 Theft of Equipment

This threat event pertains to the unauthorized removal of IT system equipment.

5. Attacks on Interfaces

5.1 Intercept/Transmit on interfaces

A threat agent mounting this type of attack must be capable of accessing the interface medium (for example, satellite link, microwave link, VHF radio, LAN cable), decoding and/or transmitting the signaling on the media (for example, T1 mux, T3 mux, packetized data, NetBios & Ethernet). The threat agents that have mounted this type of attack range from intelligence, to various individuals and organizations involved in criminal activity, terrorism and industrial espionage. There are historic examples of voice and data interception by threat agents wire-tapping or intercepting transmissions on microwave circuits, satellite or other radio frequency transmissions. This type of attack could also involve the tapping of switching equipment or communications lines out of the direct control of the IT system's Operational Authority.

An attack against transmission systems such as microwave may involve the collection and recording of large amounts of information that is later analyzed with the assistance of computers, for items of specific interest. During the years of the cold war, the capability and techniques to perpetrate this type of attack have grown significantly. Though Wide Area Networks (WANs) have been targeted in the past, the employment of any broadcast techniques, such as some of the new wireless Local Area Networks (LANs), will greatly open up the opportunity for this type of attack.

5.2 Cutting Cable Interface

This threat event is only applicable to cable interfaces where a threat agent has physical access to the cable.

5.3 Altering Data on Interfaces

This threat event pertains to a threat agent modifying messages that are transmitted on an interface. This threat event also includes replay attacks where the threat agent copies messages and replays them at a later time.

5.4 Jamming/Flooding Interfaces

This threat event primarily pertains to radio interfaces that can be jammed or flooded by an over-abundance of radio signals at the receiver. For example, a radiating source from a nearby radio station may "jam" incoming transmissions from the intended source. Also, a base station receiver for cellular phones may be flooded with requests for communications transmission, and may be unable to set up channels due to repeated transmission collisions from the users.

5.5 Exploiting Covert Channels

For a threat agent to exploit a covert channel, there must be a "listener" and an inside signaller (that is, either a person or malicious code). A covert channel is a communications

channel in an IT system that allows the transfer of information in a manner that circumvents security controls. Two common covert channel types have been identified:

- a) Covert storage channels involve functions or features of the IT system that permit the direct or indirect writing of information to a storage location and the direct or indirect reading of that information by another process. For example, packet lengths can be manipulated to signal information across a network that would otherwise be prohibited by typical read and write access controls.
- b) Covert timing channels involve the passage of information through signaling from signaler to listener based on modulation related to response time. For example, packet timing can be manipulated to signal information across a network that would otherwise be prohibited by typical read and write access controls.

5.6 Traffic Flow Analysis

This threat event implies that a threat agent is listening to all information transmitted on an interface, and will be able to deduce other information based on the flow of information. For example, the increase or decrease in the amount or type of information being transmitted may provide useful clues about more sensitive information in the organization. For example, an increase in traffic to a regional office may indicate the “important” event in the news will likely occur at the regional office. For effective traffic flow analysis, the threat agent may require access to several interfaces.

6. Attacks on Processes

6.1 Software Failure

This threat event includes software crashes as a result of an unstable process state. This includes software bugs that were missed during the software development process.

6.2 Logical Access

Gaining logical access to the IT system through an IT process will give a threat agent certain privileges to IT system assets. System personnel and software entities will have legitimate need for logical access while outsider threat agents must surreptitiously gain access by masquerading as a legitimate system user or software entity (for example, by guessing passwords, or by accessing known trap doors in an operating system). Once logical access is gained, a number of subsequent events are possible depending on the access rights acquired, or the entity being masqueraded.

Impacts of a logical access may be:

- a) Disclosure of information if the threat agent has read privileges.
- b) Theft of services if the threat agent has execute privileges. For example, theft of commercial communications services, such as the fraudulent use of long distance telecommunications services including privately owned Private Branch Exchanges (PBXs)

- c) Modification of information if the threat agent has write/modify/append privileges. Note that this includes the introduction of viruses, logic bombs, Trojan Horses, worms, etc. onto software in storage.
- d) Modification of Services if the threat agent has write/modify/append privileges. Note that this includes the introduction of viruses, logic bombs, Trojan Horses, worms, etc. to processes.
- e) Deletion of information if the threat agent has write/delete privileges.
- f) Disruption of services (for example, by removing processes).

Threat agents may use many means to gain logical access:

- a) coercion and bribery;
- b) tricking legitimate system users into unintentionally revealing access codes and passwords;
- c) "dumpster diving" (that is, scavenging in trash receptacles) to obtain access codes and passwords;
- d) electronic scavenging of buffers, cache memory or electronic media for residual information, since many operating systems do not do a thorough job of erasing buffers or overwriting media;
- e) false login screens and password collecting programs to record passwords;
- f) taking over an active account if a legitimate user logs off incorrectly and leaves the user account active on the IT system. This situation can happen when a dial-up or direct connect session is interrupted by faults, errors or anomalies in the interconnected systems, and the communications controller fails to terminate the session.

6.3 Electronic Access

Accessing a node remotely from another node in the system, or from a location outside the system via departmental, government, or public communications infrastructure (for example, the Public Switched Telephone Network).

Hackers may employ auto-dial programs with PCs and modems to perform random searches for computers of interest. A variety of techniques may be employed to break access codes and passwords. Hackers typically try default system or maintenance passwords. They may employ dictionary attacks against copies of encrypted password files attempting to defeat one-way encryption protection or they may use a variety of password-cracking algorithms that attempt to exploit vulnerabilities in system or interface designs.

Hackers usually attempt to masquerade as legitimate users or otherwise appear innocuous or invisible. They may use techniques such as the recording and playback of legitimate

messages to obtain sensitive information such as passwords, or to fool legitimate users with false information.

7. Attacks on Personnel

7.1 Attack on Personnel

This threat event implies that personnel are attacked by threat agents.

7.2 Loss of Personnel

This threat event implies that personnel become unavailable due to illness or accidents.

ANNEX C – SYSTEM DOCUMENTS FOR RISK ASSESSMENT AND SAFEGUARD SELECTION

The System Risk Report produced in the risk assessment activities may contain the following contents for each life cycle stage. The contents may re-structured into a more appropriate document structure.

Table II – Risk Report Contents

System Risk Report	PFC	RD	AD	DD	SI	SO
I Introduction						
- role/users/location	*	*	**	**	C	
- authorities	*	*	C			
II System Overview						
- System Description (security relevant view)	*	**	C			
- Operational requirement	*	**	C			
- Concept of Operations	*	**	C			
- Policy Framework	*	**	C	***	C	
- Location		*	C			
- Anticipated modification and expansion		*	**			
- System Design		*	C			
- System Boundary						
III Risk Assessment						
- Aim		*	*	*	*	
- Scope		*	*	*	*	
- Statement of Sensitivity		*	**	***	C	
- Target risk and certainty		*	*	C	C	
- Asset sensitivity assessment		*	**	***	C	
- Threat assessment		*	**	***	C	
- Vulnerability assessment			*	**	C	
- Summary of risk			**	***		
IV Recommendations						

Legend:

- | | |
|--|------------------------------|
| * broad outline of information | PFC = Plan for change |
| ** expanded information | RD = Requirements Definition |
| *** well-defined and detailed information | AD = Architectural Design, |
| C completed at the end of the previous stage | DD = Detailed Design |
| | SI = System Implementation |
| | SO = System Operation |

The Safeguard Selection Report produced in the safeguard selection activities may contain the following contents for each life cycle stage. The contents may re-structured into a more appropriate document structure.

Table III – Safeguard Selection Report Contents

Safeguard Selection Report	PFC	RD	AD	DD	SI	SO
I System Overview (See System Risk Report) - Summary of risk - Target risk and certainty		*	**	***	C	
II Security Requirements/Specifications - Administrative and organizational - Personnel - Physical and environmental - Hardware - Software - Operations - COMSEC - TRANSEC - CRYPTOSEC - EMSEC - NETSEC		*	***	C		

III Safeguard Options - Safeguard option description - Cost analysis <ul style="list-style-type: none"> - acquisition - installation - training - productivity - life expectancy - certification - Safeguard effectiveness assessment <ul style="list-style-type: none"> - dependency - vulnerability - acceptability - required intervention - visibility 			***	C		
III Preferred Safeguard Option - Trade off analysis		*	**	***	C	

Legend:

- * broad outline of information
- ** expanded information
- *** well-defined and detailed information
- C completed at the end of the previous stage

- PFC = Plan for change
- RD = Requirements Definition
- AD = Architectural Design,
- DD = Detailed Design
- SI = System Implementation
- SO = System Operation

ANNEX D – SECURITY SAFEGUARDS

Example groupings of IT security safeguards.

1. Administrative and Organizational Security

These safeguards are administrative and procedural controls to:

- a) develop and implement contingency plans;
- b) apply classification/designation labels to assets;
- c) investigate security breaches;
- d) review audit trails and logs;
- e) provide software design standards;
- f) provide test plans for new or revised application programs;
- g) provide accountability controls within an organization.

2. Personnel security

These safeguards develop and implement personnel security policies for providing:

- a) position requirements;
- b) employee screening requirements;
- c) contract personnel security requirements; and
- d) security orientation and awareness.

3. Physical and environmental security

These safeguards provide physical and environmental security measures such as:

- a) physical and access control systems;
- b) environmental controls;
- c) fire safety controls;
- d) storage area controls; and
- e) proper housekeeping procedures.

4. EDP security

4.1 Hardware

These safeguards provide security services for hardware in the areas of:

- a) configuration control;
- b) contracting;
- c) maintenance;
- d) test and acceptance; and
- e) change control practices.

4.2 Software

These safeguards provide security services for software in the areas of:

- a) system development life cycle standards;
- b) programming standards and controls;
- c) documentation;
- d) change controls and software security systems;
- e) audit trails;
- f) operating systems security features;
- g) system test and evaluation process; and
- h) information and database administration.

4.3 Operations

These safeguards deal with operational security services such as:

- a) separation of duties;
- b) processing states;
- c) transfer of operational control;

- d) operating procedures and controls; and
- e) media controls.

5. Communications Security (COMSEC)

5.1 Transmission Security

The component of COMSEC that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis.

- h) operational procedures and control;
- i) frequencies and call signs; and
- j) methods to prevent interception, exploitation and deception.

5.2 Cryptographic Security

The component of COMSEC that is specific to cryptographic security services:

- a) cryptographic equipment and material;
- b) configuration control;
- c) cryptographic equipment maintenance;
- d) storage of COMSEC material;
- e) disposal and destruction of superseded COMSEC material;
- f) emergency COMSEC procedures; and
- g) COMSEC security practices and operational procedures.

5.3 Emission Security

The component of COMSEC, with which the term TEMPEST is associated, which consists of all the measures taken to deny unauthorized interception and analysis of compromising emanations from crypto-equipment, information processing and telecommunications equipment.

- a) equipment and facilities requirements;
- b) equipment interconnection and system integration; and
- c) maintenance of TEMPEST equipment.

5.4 Network security

These safeguards deal with network security services such as:

- a) operational policy and procedures;
- b) administrative responsibilities;
- c) architecture and functionality; and
- d) "cascade" issues (e.g. connecting computers handling different security levels).

GLOSSARY

Sources: Each definition is followed by a corresponding reference from which it was obtained.

CDITS Canadian Dictionary Of Information Technology Security, Version 1.1, April 1989

CTCPEC Canadian Trusted Computer Product Evaluation Criteria, Version 3.0e, January 1993

GSP Government Of Canada Security Policy, June 1994

MBW2 Proceedings, Second Risk Management Model Builders Workshop, Ottawa, June 1989

NEW New Definition

TSEG Trusted Systems Environment Guideline, December 1992

Accreditation

Formal declaration by the responsible management approving the operation of an automated system in a particular security mode using a particular set of safeguards. Accreditation is the official authorization by management for the operation of the system, and acceptance by that management of the associated residual risks. Accreditation is based on the certification process as well as other management considerations. (TSEG)

ALE

Average loss expectancy. A risk assessment measure which indicates the average loss expected over a given period of time. (NEW)

Asset

An asset is a component or part of the total system to which the department directly assigns a value to represent the level of importance to the "business" or operations/operational mission of the department, and therefore warrants an appropriate level of protection. Assets types include: information, hardware, communications equipment, firmware, documents/publications, environmental equipment, people/staff, infrastructure, goodwill, money, income, organizational integrity, customer confidence, and organizational image. (EUROPEAN COMMUNITY)

Assurance	The degree of confidence that a safeguard(s) correctly implement(s) the system specific security policy. (CTCPEC)*
Attack	See threat event.
Availability	The accessibility of systems, programs, services and information when needed and without undue delay. (NEW)
Baseline	An element of a system which cannot be changed without formal approval. (NEW)
Capability	The ability of a threat agent to act, or to be effective. (MBW2)
Certification	The comprehensive assessment of the technical and non-technical security features of an information technology system, made in support of accreditation, that establishes the extent to which a system satisfies a specified security policy. (CTCPEC)
Compromise	Unauthorized disclosure, destruction, removal, modification or interruption to an IT system asset. (GSP)*
Confidentiality	The quality or condition of being sensitive to disclosure. (GSP)
Consequence	The result of the occurrence of a threat event, expressed as a (usually undesirable) change in the state of security for an asset or information. Used synonymously with impact and injury. (MBW2)*
Determination	The willingness of a threat agent to act. (MBW2)
Event	A change in system state. In general, an event has a trigger, a means or mechanism, and an effect or consequence. An event may be undesirable from a security point of view, in which case it is called a threat event (see below). (MBW2)
Impact	A measure of the degree of damage or other change caused by a consequence. (MBW2)*
Integrity	The quality or condition of being accurate or complete. (GSP)
Means	The mechanism or medium that is used by a threat agent in the occurrence of a threat event. (MBW2)*
Motivation	Something that induces a threat agent to act against a system. (NEW)
Resources (characteristic of Threat Agent):	The equipment, money, people, knowledge, etc. available to a threat agent to initiate an attack. (NEW)

Risk	A measure indicating the likelihood and consequence of events or acts that could cause a compromise of system asset(s). (NEW)
Risk Assessment	An evaluation of risk based on the effectiveness of existing security safeguards, the likelihood of system vulnerabilities being exploited and the consequences of the associated compromise to system assets. (NEW)
Safeguard(s)	An approved minimum security measure(s) which, when correctly employed, will prevent or reduce the risk of exploitation of specific vulnerability(s) which would compromise an IT system. (NEW)
Security domain	A system subset with a unique instance of the type of information, the environment including access control and/or the vulnerabilities inherent in the hardware/software. (NEW)
SLE	Single-event loss expectancy. A risk assessment measure which indicates the loss incurred for a single occurrence of a threat scenario.
State	A description of the system assets, threats, security safeguards, and their environment, when a given set of conditions holds. State descriptions are useful for modeling changes that occur between one state and another. (MBW2)*
Statement of Sensitivity	A profile of an existing or proposed system, documenting characteristics of the data (to be) processed, the (proposed) user community, and the requirements to address confidentiality, integrity and availability concerns. (TSEG)
Supporting Asset	System components which support the primary assets. Supporting assets may include hardware, software, interfaces, personnel, supporting systems & utilities and access control measures. (NEW)
System	A set of elements such as personnel, physical, environment, safeguards, technology, etc. that are combined together to fulfill a specified purpose or mission. (NEW)
Target	The objective of a hostile threat agent. (MBW2)
Threat Agent	A person, organization, thing or entity that desires to or is able to trigger an event which can compromise the security of an asset or information. (MBW2)*

Threat Assessment	An evaluation of threat agent characteristics including resources, motivation, intent, capability and opportunity. (NEW)
Threat Event	An event or occurrence that has the potential to compromise the security of an asset or information. Synonymous to attack. (MBW2)*
Threat Scenario	A specific threat agent mounting a specific type of attack in an attempt to compromise (in one or more ways) one or more system assets. (NEW)
Value (attribute of Asset)	A measure or statement of the utility of an asset or information, or (alternatively) the cost if it is compromised. The value can be stated in quantitative or qualitative terms. Utility and cost are contextually dependent, based on the needs and situation of the organization. Value is therefore not necessarily an objective term. (MBW2)
Vulnerability	A characteristic of the system which allows a successful threat event to occur. (NEW)

* Minor rewording for compatibility with GSP

** Minor rewording from definition in original source

BIBLIOGRAPHY

- 1) Communications Security Establishment, *A Guide to Certification and Accreditation of Information Technology Systems*, 1996, 40 pages.
- 2) Communications Security Establishment, *A Guide to Security Risk Management for Information Technology Systems*, 1996, 38 pages.
- 3) Communications Security Establishment, *Canadian Dictionary of Information Technology Security*, Version 1.1, 1989, 154 pages.
- 4) Communications Security Establishment, *The Canadian Trusted Computer Product Evaluation Criteria*, Version 3.0, 1993, 233 pages.
- 5) Communications Security Establishment, *Trusted System Environmental Guideline (TSEG)*, 1992, 84 pages.
- 6) LEE, E.S., et al, Computer System Research Institute, University of Toronto, *Composable Trusted Systems*, ISSN 0834 1648, 1992.
- 7) National Security Agency, *Department of Defense Trusted Computer System Evaluation Criteria (TCSEC, Orange Book)*, WD 5200.28-STD, 1985, 127 pages.
- 8) Royal Canadian Mounted Police, *Technical Security Standards for Information Technology (TSSIT)*, 1992.
- 9) Treasury Board Secretariat; *Information and Administrative Management Component; Security*, 1994.