Chapter 3 – REVIEW OF EXISTING METHODOLOGIES

3.1 OVERVIEW OF THE SELECTED METHODOLOGIES

3.1.1 CRAMM

3.1.1.1 Introduction

CRAMM is a software-based (Windows-based) security risk assessment and risk management methodology tool. The tool was developed to provide the following:

1) A sound approach to identifying threats and vulnerabilities, and thus being able to establish a sound basis for identifying and stating risks;
2) A more justifiable approach for management to understand risks;
3) A basis for potential savings, in terms of the cost of security; and
4) A sound approach to improve levels of information and supporting system assets protection.

CRAMM is more of a qualitative methodology than a quantitative methodology and, in broad terms, treats security risk assessment as an evaluation of the risks, and security risk management as the identification of the countermeasures to combat the risks. All aspects of security are addressed within the methodology; namely, personnel security, physical security and security of information. It can handle deliberate and accidental threats, and encompasses existing UK government security policy and guidance. For NATO, a NATO profile has been developed, based on NATO security policy and supporting directives and guidance in order to make the tool easier to use and more specifically tailored to NATO CIS.

The methodology allows to use the tool to establish a baseline of information for an organisation or project at any time during its life-cycle, and provides a comprehensive "what-if" capability. This allows to model different scenarios, to assess the impact of changes in a system environment, or changes in policy and directives. It also provides a capability for follow-up reviews, using the previously established baseline of information.

3.1.1.2 Description

There are three fundamental stages to a CRAMM review, which correspond to the stages identified in the current NATO security risk assessment guidance and are, in broad terms, the following:

1) Stage one – Assessing the value of the information, and identifying the assets which support the business process;
2) Stage two – Identifying what threats may affect the system and how vulnerable is the system to those threats; arriving at a conclusion about the risks; and
3) Stage three – Identifying how the risks can be countered, including what improvements are required to existing control measures.

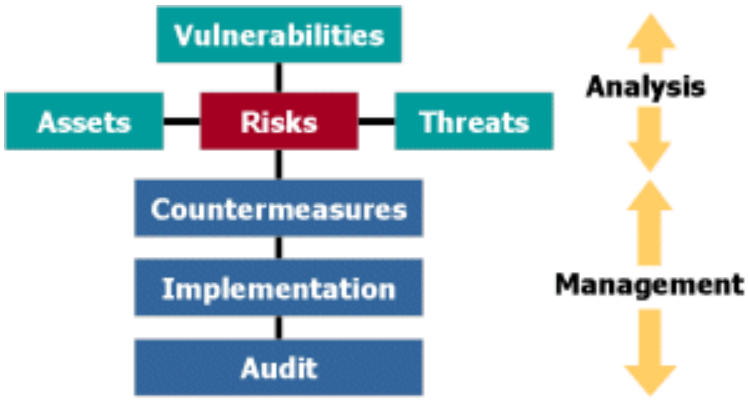

Figure 3-1: High Level Structure of CRAMM Methodology.

Between each stage, there is the capability to produce comprehensive management reports, and conduct management reviews to ensure that the baseline of information is valid.

In stage one, at the start, it is important to identify the purpose of the CRAMM review, where the boundaries of the review are, and the schedule for the review. Equally important is the establishment of a baseline questionnaire (which the tool provides) from which you establish all the information about the physical and data assets. From this, you build up asset models, which show the relationship between data assets and those assets which support those data assets (for example, a computer room and its hardware).

The next step is to apply a valuation to the assets; data assets are valued in terms of impact of disclosure, modification, unavailability and destruction (this is qualitative information based on interviews with the users of information); physical assets are valued in terms of their replacement cost (quantitative information). At the end of this stage, it is recommended to carry out a management review to ensure that you have a sound baseline of information, before moving forward to the next stage. The stage 1 management review helps ensure at an early stage in the risk management process that there is agreement between the operational and security accreditation authorities as to the assets to be protected, and their value to the organisation.

In stage two, you move into the threat and vulnerability assessment. The types of threat that are addressed include the following:

1) Logical threats – For example, hacking, unauthorised use of an application, and malicious software;
2) Communications threats – For example, communications infiltration, and mis-routing;
3) The threat of technical failures to communications and information systems hardware and software;
4) Errors by people – For example, system management errors, or errors by users; and
5) Physical threats – For example, theft, wilful damage, terrorism, fire, water damage, and natural disasters.

The tool contains a built-in, very extensive library of potential threats and vulnerabilities. The threats can either be based on specific knowledge about previous security incidents, or on generic information. The vulnerabilities are based on an understanding of the functions and capabilities that are available within the system environment. The threat and vulnerability assessment arrives at qualitative statements for the threats (in terms of very low, low, medium, high, and very high) and vulnerabilities (in terms of low, medium and high).

The next step is to derive measures of risk, and these are derived from a combination of the threat, the vulnerability, and the asset value. The measures of risk are scaled, so that the security requirements to be established are matched to the degree of risk. Again, at the completion of this stage, a further management review is recommended to ensure the validity of the information, before moving forward to select countermeasures.

In stage 3, the final stage, the countermeasures, dependent upon the scale of the risk, are selected. The tool contains countermeasures groups for each individual threat, addressing, for example, identification and authentication, access control, and physical security. Within each countermeasure group, you have the following structure:

1) A policy statement – Which can be derived, verbatim, from the appropriate security policy document or supporting directives or guidance documents;
2) The security objective of applying this particular countermeasure;
3) Detailed descriptions of the functions associated with the countermeasure; and
4) Specific ways, or options, in which the functionality can be provided.

The capability also exists to apply the costs of the countermeasures (both in financial and man-effort terms). Having selected countermeasures, a management review meeting is required to examine the countermeasures, consider those which may not be applicable, identify those for implementation, and identify those aspects where the risk is to be accepted. A powerful aspect of the tool, which is very relevant here, is the back-track capability. This means that you can, if you are not certain why a particular countermeasure has been recommended, review the asset / threat / vulnerability information that led to the countermeasure decision.

All through the stages, varying degrees of management reports can be produced, depending upon the target audience. One of the benefits, in the final stage, is the ability to produce the security-related documentation used in the accreditation process.

The NATO Profile enhancements, in particular, tailor the management reports and security-related documentation to NATO's needs, for example, with the development of a System-specific Security Requirement Statement (SSRS), the Security Operating Procedures (SecOPs) and security inspection reports.

3.1.2 EBIOS ®

3.1.2.1 History

The EBIOS methodology has been created in 1995 by the DCSSI (Direction Centrale de la Sécurité des Systèmes d'information) a government entity attached to the French Prime Minister within the SGDN (Secrétariat Générale de la Défense Nationale), the French National Security Agency.

Since that date, EBIOS has been used for various projects within public and private sectors, in France and abroad.

In 2000, software was developed to support the methodology and, in parallel the methodology itself has evolved. A new version has been published in 2004 with a new version of the software. This new version includes a compatibility toward international standards (ISO/IEC 15408, ISO/IEC 73, ISO/IEC 17799…).

The software and the method are available on a freeware basis on the DCSSI web site: http://www.ssi.gouv.fr/document/docs/EBIOS/ebios.html.

3.1.2.2 Description

The method includes 5 steps:

1) Context;
2) Security needs;
3) Threats analysis;
4) Identification of security objectives; and
5) Identification of security requirements.

STEP 1: Context

Step 1.1: Description of the organization hosting the system:

- Identity of the organization
- Main objective of the organization
- The missions
- The business
- The value
- Structure and structure diagram
- Constraints on the organization
- Regulations
- Functional description of the organization Information System

Step 1.2: Description of the target system:

- Description of the project / program:
  - Objectives, responsibilities, etc.
- Identification of the main functions / information
- Functional description of the system (identification of subsystems)
- Hypothesis
- Constraints

Step 1.3: Identification of the systems components:

- Hardware
- Software
- Networks
- People
- Sites
- Construction of a function / entity and information /entity matrix

	H1	H2	H3	S1	S2	S3	N1	N2	X1	X2	X3
Function 1	x			x		x	x			x	
Function 2			x	x	x			x			x

STEP 2: Security Needs

Step 2.1: Identification of the security criteria:

- Availability
- Integrity
- Confidentiality
- Anonymity
- Proof and control

Step 2.2: Definition of scales, for example:

0 = Public

1 = Restricted

2 = Confidential

3 = Secret

Step 2.3: Identification of impacts, for example:

- Service interruption:
  - Inability to provide the service
- Brand image loss:
  - Loss of trust in the IS internally
  - Loss of awareness
- Internal function disturbance:
  - Disturbance for the organization
  - Increased internal charges
- Illegal actions:
  - Incapacity to enforce legal duties
- Contractual offense:
  - Incapacity to fulfill contractual obligations
- Damages to staff/users:
  - Hazards for staff and/or users of the organization

Step 2.4: Determination of security needs:

For each function and information, determination of the security needs:

Function or information X	impact1	impact 2	impact 3	security need	comments
Availability	B11	B12	B13	max(B1i)	
Integrity	B21	B22	B23	max(B2i)	
Confidentiality	B31	B32	B33	max(B3i)	

For each essential element and security criterion security needs are evaluated. These values provide a measure of impacts if the criterion is not fulfilled. The meanings of those values vary from the ways they are computed: A simple max function is used in the following example. Another way would be to

decompose each criterion by damage scenarios, compute the impact for each damage scenario, and finally define the value to be a function of all those computed values.

Each Bxy represents a numerical value for the impact from 0 (= no impact) to 4 (=very serious impact). If we take the information system of a bank as an example, the information "bank account" will be given the following values:

Availability impacts:

Inability to provide the service, value 2 (moderate)

Incapacity to fulfil contractual obligations, value 3 (high)

Integrity impacts:

Lost of trust in the organization, value 4 (maximum)

Confidentiality impacts:

Financial losses, value 4 (maximum)

The AIC (availability, Integrity, Confidentiality) vector associated to this information will then be 3, 4, 4.

This information is summarized in a table with the AIC values for each function/information.

STEP 3: Threats Analysis

Step 3.1: Selection:

- Selection of attacks methods (fire, flooding, theft, trap, …)
- Determination of the related security criteria (e.g. , availability for fire)
- Identification of the threatening agents (natural, human, accidental, …)
- Determination of their capacity:
  - Accidental or random
  - Amount of resources and opportunity
  - Degree of expertise, opportunity and resources

	threatetning events						affected criteria		
	type			cause					
	natural	human	environment	accidental	deliberate	potential	D	I	C
fire	x	x	x	x	x	2	+		
theft			x		x	1	+		+

Step 3.2: Vulnerabilities:

- For each selected attack method, identification of the system vulnerabilities which could allow their realization
- For example, hardware trap:
  - V1: loose control at the site entry
  - V2: use of standard hardware with extension capacity
  - V3: no hardware control plan
- Evaluation of the vulnerabilities level:
  - Very unlikely / not feasible

- Slightly probable / request very expensive equipment and a very high level of expertise
- Fairly probable / request a high level of expertise and/or specific hardware
- Highly probable / request standard equipment and skills
- Certain / can be done by anybody

Step 3.3: Threat Formulation:

- A threat results from the combination of:
  - A threatening agent (with a capacity)
  - An attack method
  - A set of vulnerabilities
  - The entities which present those vulnerabilities
- An "opportunity" value can be associated to each threat calculated from the vulnerabilities levels
- Example:
  - The lack of control at the servers ' room door (V1) allows a visitor (threatening agent) to steal (attack method) a magnetic device (entity) left unattended (V2)
  - Opportunity: 3

STEP 4: Identification of Security Objectives

Step 4.1: Risks Formulation

- A risk results from the combination of:
  - A threatening agent (with a capacity)
  - An attack method
  - A set of vulnerabilities
  - The entities with presents those vulnerabilities
  - The threat capacity
  - The security needs
  - The impacts

Example:

- The lack of control at the servers ' room door (V1) allows a visitor (threatening agent) to steal (attack method) a magnetic device (entity) containing the complete system backup left unattended (V2). The confidentiality of the users data is then compromised as well as the availability of these data in case of system failure
- Opportunity: 3, threat capacity: 1, related security needs: C: 3, A: 2

Step 4.2: Security Objectives:

Security objectives are formulated as the decision to cover the risk but not as the way to achieve that goal. For example:

O.INC-CSQ Measures shall be taken to reduce the effect of a fire in term of financial losses.

Objectives may be related to the system or its environment.

Justification Matrix

For each identified risk, this matrix lists the related security objectives with a justification and an estimation of the coverage level (complete, partial or not covered)

Risk	Security objectives	Rationale	Coverage	Potential
R_TRAP	*O.SYS-COMMAND* *O.SYS-ACTIONS*	*xxxxx*	(1)	

(1): Total, partial, no coverage.

The strength of the security mechanisms implemented to cover the security objectives is determined by the associated potential of the attacker using the following table (issued from the CC):

Table 3-1: Potential of the Attacker

Potential/Strength	Definition
1	A level of the strength where analysis shows that the function provides adequate protection against casual breach of security by attackers possessing a low attack potential.
2	A level of the strength where analysis shows that the function provides adequate protection against straightforward or intentional breach of security by attackers possessing a moderate attack potential.
3	A level of the strength where analysis shows that the function provides adequate protection against deliberately planned or organised breach of security by attackers possessing a high attack potential.

Assurance Level

The assurance level has to be chosen but there is no proposed method for this step. A NATO WG in working on this topic (Infosec Technical and Implementation Guidance for the Assessment of Assurance Levels in Specific Communication and Information Systems (CIS) Environments AC/322-D(2005)0043 26th October 2005).

STEP 5: Determination of Security Requirements

Step 5.1: Functional Requirements

The functional requirements are issued from CC functional components.

A tool is proposed to choose the CC components depending on selected vulnerabilities.
Justification Matrix

For each security objective, this matrix assesses the requested strength of mechanisms and lists the related functional requirement with a justification and an estimation of the coverage level (complete, partial or not covered).

An identification and justification of the coverage problems can then be established.

The tool is available in 4 different languages and can automatically generate reports and security-related documentation to NATO's needs, for example, with the development of a System-specific Security Requirement Statement (SSRS), the Security Operating Procedures (SecOPs).

3.1.3 Overview of Canadian TRA Methodology

The Communications Security Establishment, a Canadian security lead agency, has developed a series of risk management[1] documents to help government departments in meeting the Government of Canada Security Policy (GSP) requirements. The following documents expanded on the standards set out in the GSP:

1) MG2 – Risk Management Framework for Information Technology (IT), 1996. The MG2 provides specific guidance for risk management within an IT system environment and its life cycle;
2) MG3 – A Guide to Risk Assessment and Safeguard Selection for Information Technology Systems, January 1996. The MG3 provides specific guidance for risk assessment and safeguard selection process throughout the IT system life cycle;
3) MG4 – A Guide to Certification and Accreditation for Information Technology Systems, January 1996. The MG4 provides more specific guidance for the certification and accreditation of an IT system throughout its life cycle; and
4) ITSG-04 – Threat and Risk Assessment Working Guide, October 1999. The ITSG-04 provides guidance to an individual (or a departmental team) in carrying out a Threat and Risk Assessment (TRA) for an existing or proposed IT system.

The MG series provides a solid guidance for risk management to managers but lack methodology to assign risk values. A working group was created to develop a TRA working guide to be included as a part of risk management processes. The document produced was the ITSG-04 Working Guide that provides risk ratings with recommendations to reduce the risk to an acceptable level.

In addition to CSE efforts in developing a TRA guideline, the Royal Canadian Mounted Police (RCMP) had undertaking initiatives in the same area. As the lead department for federal law enforcement, with a crime prevention mission, the RCMP is also responsible to provide advice to departments on the process of threat and risk assessments and the conduct of IT system security reviews, inspections and audits. The Security Information Publication – Guide to Threat and Risk Assessment for Information Technology was published in November 1994 and is still in use today by TRA practitioners. RCMP produced a second risk management guide with an emphasis on physical security, Guide to Threat and Risk Assessment Involving On-Site Physical Security Examination, published in 2002.

3.1.3.1 Using TRA in Risk Management

Risk management is the process by which resources are planned, organized, directed, and controlled to ensure the risk of operating a system remains within acceptable bounds at near-optimal cost[2]. Risk management is an iterative and cumulative process. The following figure outlines the Canadian overall risk management process which involves: planning; the TRA; selection of safeguards; system certification and accreditation; maintenance; and monitoring and adjustments to safeguard selections.

Traditional prescriptive approach of mandating (i.e. "shall" implement) specific security controls for systems are not cost effective or are too complex. The current Canadian approach to risk management is a mixed approach that is prescriptive and threat-based. Minimum standards set the prescribed safeguards, which are supplemented through a threat-based process. However, this approach is silent on how

[1] URL: http://www.cse-cst.gc.ca/en/knowledge_centre/gov_publications/itsg/itsg.html.

[2] This definition of risk management is consistent with the ITSG-04, "Threat and Risk Assessment Working Guide", October 1999 Government of Canada, Communications Security Establishment (CSE).

minimum standards are established: Minimum standards should also be determined through a risk management process involving a TRA. It would be interesting to get a single global risk management process because both measure similar risks.

Risk management processes may involve an assurance component. Currently, the Canadian process doesn't include such a component even though it seems that CC assurance levels of safeguards relate to vulnerabilities and risks.

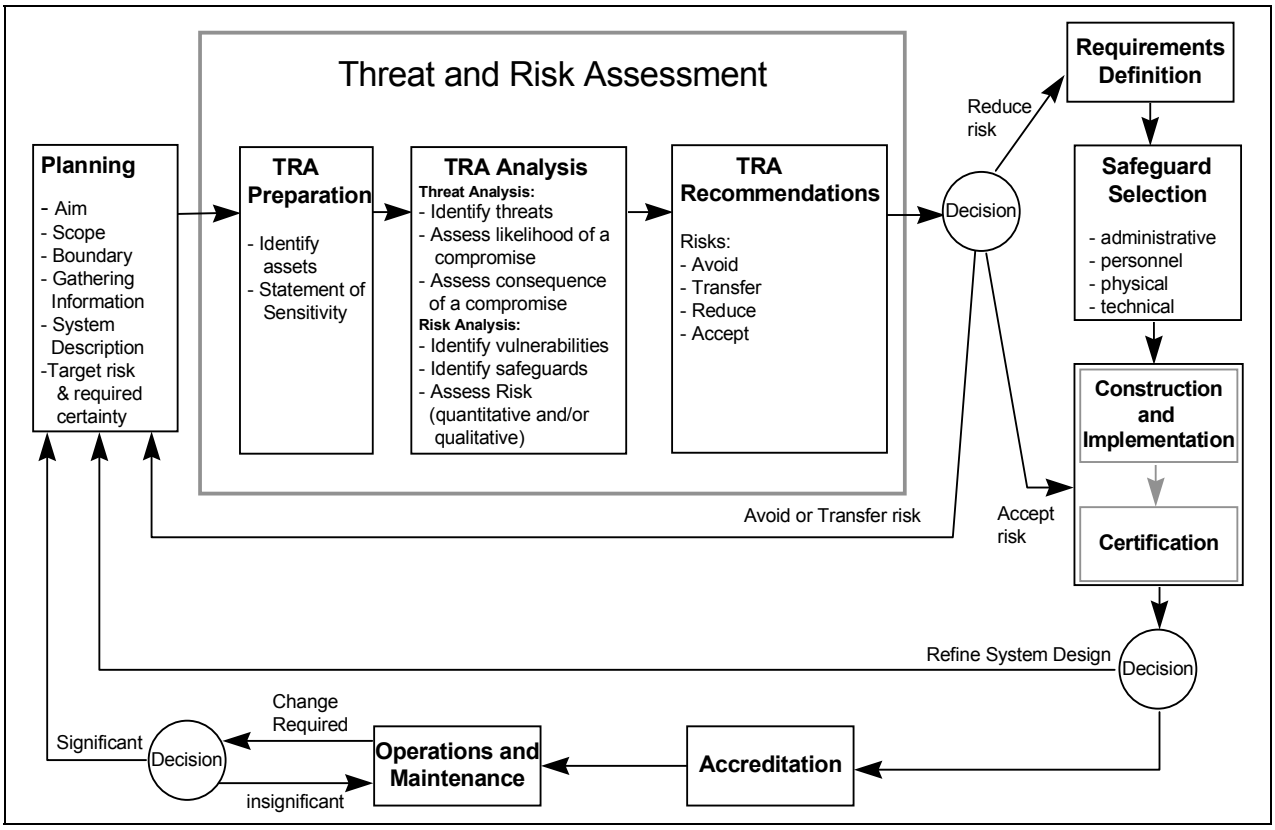

Figure 3-2: Risk Management Model[3].

The TRA in this model is functional and provides the current level of **R**isk caused by the **T**hreat Agents acting on the Critical **A**ssets of an Information System given its **V**ulnerabilities. More precisely, the risk is a function of the values of the assets, the threat agent attributes, and the vulnerabilities, or $R = f\ (A_{Val}, T, V)$. Note that R is a probabilistic measure of harmful impacts of a given type on a system (IT-system) and they are many possible impact types.

3.1.3.2 Risk Management Tools

The current Government of Canada (GoC) information technology risk management scheme is supported by these two basic methodologies, the ITSG-04 and the RCMP TRA guidelines. It must be noted that many government departments have developed their own methodologies to suit their environment but the root to those remains the formal two basic methods with the occasional insight derived from sources such as the National Institute of Standards and Technology Risk framework[4].

[3] This Risk Management Model is extracted from the CSE ITSG-04, ibid.

[4] NIST 800-30 Risk Management Guide for Information Technology Systems, October 2001.

3.1.3.2.1 RCMP Methodology

The RCMP developed two TRA methodologies:

1) The Guide to Threat and Risk Assessment for Information Technology, published in 1994; and
2) Guide to Threat and Risk Assessment Involving On-Site Physical Security Examination, published in 2002.

Since this report concentrates on TRA with respect to IT systems, comments will focus on the first publication. Many practitioners use this methodology because it is widely used and is relatively easy to work with. The analysis is recorded in a table format where the reader can view the overall analysis in scenarios from threat to vulnerability to risk. The methodology is a mix of qualitative and quantitative ratings. The statement of sensitivity is an integral part of the TRA. This methodology is threat centric and can be applied to small networks, simple systems and basic applications.

The RCMP methodology is a four-step process:

1) **Preparation**: Determining what to protect. This process allows the TRA Practitioner to define the environment, identify assets and their values, identify the Confidentiality, Integrity and Availability (CIA) requirements and produce a statement of sensitivity;
2) **Threat Assessment**: Determining what to protect against and consequences of a threat. The Practitioner describes the threats that may target the assets under consideration. The threat concepts of class, likelihood, consequence, impact and exposure are highlighted;
3) **Risk Assessment**: Determining whether existing or proposed safeguards are satisfactory. Risk assessment is "an evaluation of the chance of vulnerabilities being exploited, based on the effectiveness of existing or proposed security safeguards". The Practitioner will evaluate the existing safeguards, list any potential vulnerabilities and provide a qualitative measure for the initial risk; and
4) **Recommendations**: Identifying what should be done to reduce the risk to a level acceptable to senior management. The closing phase of the TRA process includes the proposal of recommendations. Additional safeguards may be necessary to mitigate the risk to an acceptable level. The final residual risk is assessed.

The weakness observed with the RCMP TRA Guide is the lack of depth in the vulnerability analysis and the inconsistency in measuring the residual risk. The method uses qualitative ratings such as high – medium – low, but offers no explanation as to their meanings and the obvious limitation on the granularity of the analysis. The mix of qualitative ratings with numerical value makes the interpretation of the results problematic for senior management. Finally, there is no provision for a remedial or follow-up plan to bring the recommendations to the next step, which is the implementation.

The RCMP TRA Guide is available to the general public on the RCMP – Technical Security Branch web site (http://www.rcmp-grc.gc.ca/tsb/pubs/it_sec/g2-001_e.pdf).

3.1.3.2.2 ITSG-04

The MG series is complemented by the ITSG-04 Threat and Risk Assessment Working Guide, published in 1999, another very popular TRA methodology used by security consultants and government employees. This TRA methodology is very comprehensive with ratings for threats and vulnerabilities. The document offers several samples for assets, threats and vulnerabilities in the annexes. The methodology uses quantitative ratings. The statement of sensitivity is an integral part of the TRA. This methodology is considered asset and threat centric and can be applied to complex networks and systems.

The steps of the TRA process can be organized into nine major tasks, each associated with a document produced during the completion of that task. These TRA related documents or deliverables are often combined into a single report. The TRA process tasks are as shown in the following table:

Table 3-2: TRA Process Tasks

#	Task	Major Activities	Document Produced
1	Prepare and Plan	Define the scope and the boundary of the analysis Establish a target level of acceptable risk Collect information for the system description Formulate a system description	Work Plan System Description Preliminary Statement of Sensitivity
2	Collect Data for Analysis	Collect information about threat agents, threat events and vulnerabilities Conduct interviews and site visits Record the existing security architecture	Initial Security Review
3	Analyze Policy and Standards Compliance	Identify applicable security policies and standards Identify and record existing/planned safeguards	List of Non-Compliant Areas
4	Perform an Asset Sensitivity Analysis	Identify the critical assets Analyse asset sensitivities. Determine impacts on the IT system and/or organization with respect to confidentiality, integrity, availability, and replacement value.	Statement of Sensitivity Report
5	Perform a Threat Analysis	Identify potential threat agents Identify potential threat events by which threat agents could impact the assets Analyse the threat agents in terms of capability and motivation Analyse the likelihood of each potential threat event occurring Record the potential threat events by domain and highest-level asset categories	Threat Analysis Report

#	Task	Major Activities	Document Produced
6	Perform a Vulnerability Analysis	Identify the vulnerabilities Assign a vulnerability severity and exposure ratings Determine the overall vulnerability ratings For each domain, record the vulnerabilities with the highest exposure [or] severity rating, and the vulnerabilities with the highest overall ratings Record safeguards that already protect assets from recorded vulnerabilities	Vulnerability Analysis Report
7	Perform a Risk Analysis	Identify possible threat scenarios Estimate the likelihood of each logical threat scenario occurring. Base the estimate on the likelihood the threat agent acting or the natural phenomenon occurring Analyse the potential impact of each logical threat scenario Assess the level of risk from each logical threat scenario. Likelihood of occurrence and potential impacts are considered	Risk Analysis Report
8	Assess System Risks for Acceptability	Review the existing/planned safeguards Assess whether or not existing/planned safeguards provide adequate protection Select additional safeguards for possible implementation	Preliminary Risk Assessment Report
9	Deliver the Final Risk Assessment Report	Prepare the final risk assessment report Present the TRA findings	Final Risk Assessment Report

The drawbacks with the ITSG-04 reveal it to be a long process with a certain difficulty in implementing the process. The method offers more granularity but the use of numerical values with different scales makes it very difficult for the risk owner to understand the results. Finally, there is no provision for a remedial or follow-up plan to bring the recommendations to the next step.

The ITSG-04 TRA Guide is available to general public on the CSE web site (http://www.cse-cst.gc.ca/en/publications).

3.1.3.2.3 A Combination of Both

Several TRA practitioners decided to take advantages of both methods and combine the RCMP TRA Guide and the ITSG-04 to ensure a greater coverage of both threats and vulnerabilities. The terminology is

the same for both methodologies with only the emphasis on the TRA components being different. The combined method allows risk to be calculated based on ratings for threats, vulnerabilities and the "value" of the critical assets. Most often, the combined version will use qualitative ratings with a description of the Low – Moderate – High values. The vulnerability assessment can be dealt with at a very high level or as a particularly in depth analysis. This combined methodology has proven in many cases that the TRA results are more consistent across the analysis. Nevertheless, the depth of the analysis rests with the TRA practitioners and their experience in that field.

3.1.3.2.4 Initiatives in TRA Methodology

Considering the many security events and the related changes in national policies and standards, Canada is currently involved in numerous IT risk management projects to ensure information of national interest and citizen information is adequately managed and protected. Three significant projects can be of value to the NATO Working Group:

1) CSE has undertaken the development of a Threat and Vulnerability Analysis System (TVAS) in order to modernize and improve internal government operations by providing a secure and trusted source from which CSE can provide expert advice and guidance to federal clients allowing effective management of cyber threats and vulnerabilities. TVAS provides incident statistics allowing for the identification of developing trends. This capability allows IT managers to institute effective cyber protection and critical North American infrastructure safeguards. The repositories of threats and vulnerabilities created under this project are unique in the risk management community;

2) CSE and RCMP have started a joint venture with the aim of developing a common TRA methodology that will include analysis of IT systems with a physical security component. The goal is to merge both RCMP TRA guides (Guide to Threat and Risk Assessment for Information Technology and Guide to Threat and Risk Assessment Involving On-Site Physical Security Examination) and the CSE Threat and Risk Assessment Working Guide (ITSG-04). The intent is to develop a common TRA framework that can be used uniformly by all departments. The ultimate goal is to automate the TRA process and use the Threat and Vulnerability Analysis System (TVAS) repositories with links to standard critical assets through relational databases;

3) The Operational Security Standard – Identification of Assets has recently been released (Feb 2005) in draft form for comments. This document supports the Government Security Policy. It provides guidance for departments to identify and categorize assets based on the degree of injury that could result from compromise to their confidentiality, availability, integrity and/or value. The identification and categorization of assets is an integral aspect of security risk management. It is the first step in the threat and risk analysis process and provides the foundation for the cost effective application of graduated safeguards. Assets include government information. The protection of information assets entails the protection of systems and networks where information is created, stored and transmitted; and

4) Treasury Board of Canada is in the process of augmenting the Operational Security Standards to fit the security policy. Currently available on the TBS web site are:

   - Operational Standard for the Security of Information Act;
   - Operational Security Standard – Business Continuity Planning Program;
   - Operational Security Standard: Management of Information Technology Security;
   - Operational Security Standard – Readiness Levels for Federal Government Facilities;
   - Personnel Security Standard and Physical Security Standard;

- Security and Contracting Management Standard; and
- Security Organization and Administration Standard.

3.1.4 US

3.1.4.1 Introduction

The United States has not standardized on any particular risk assessment tool or methodology. Although several tools have been evaluated, each seems to rely on subjective information depending on the system under review, the environment in which it resides and the person performing the evaluation. National Risk Analysis Methodologies are available, but no single methodology has been adopted or is applicable to all systems and all cases. Methodologies vary depending upon the level of assets requiring protection. For instance a more rigorous process is required for systems which process highly sensitive information.

3.1.4.2 Objective

The objective of this section is to provide information about risk methodologies used by both National and Federal agencies within the United States. Furthermore, it will define common steps to determine system risk; it is highly likely that these steps are consistent with international risk methodologies.

3.1.4.3 Basic Risk Methodology

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 and the Federal Information Security Management Act (FISMA) of 2002 provide a foundation for the general risk methodology used within the United States. NIST SP 800-30 is the risk management guide for general information technology systems and FISMA outlines a mandatory set of processes that must be followed for all information systems used or operated by U.S. Government federal agencies or by contractors or other organizations on behalf of U.S. Government agencies. These documents are complementary and provide a model to manage risk associated with information technology systems. NIST SP 800-30 defines three processes for risk management: risk assessment, risk mitigation, and evaluation and assessment. Each of these elements is an important function in implementing, supporting and maintaining system security.

3.1.4.3.1 Risk Assessment

The basic steps which apply to risk assessment are depicted in Figure 3-3.

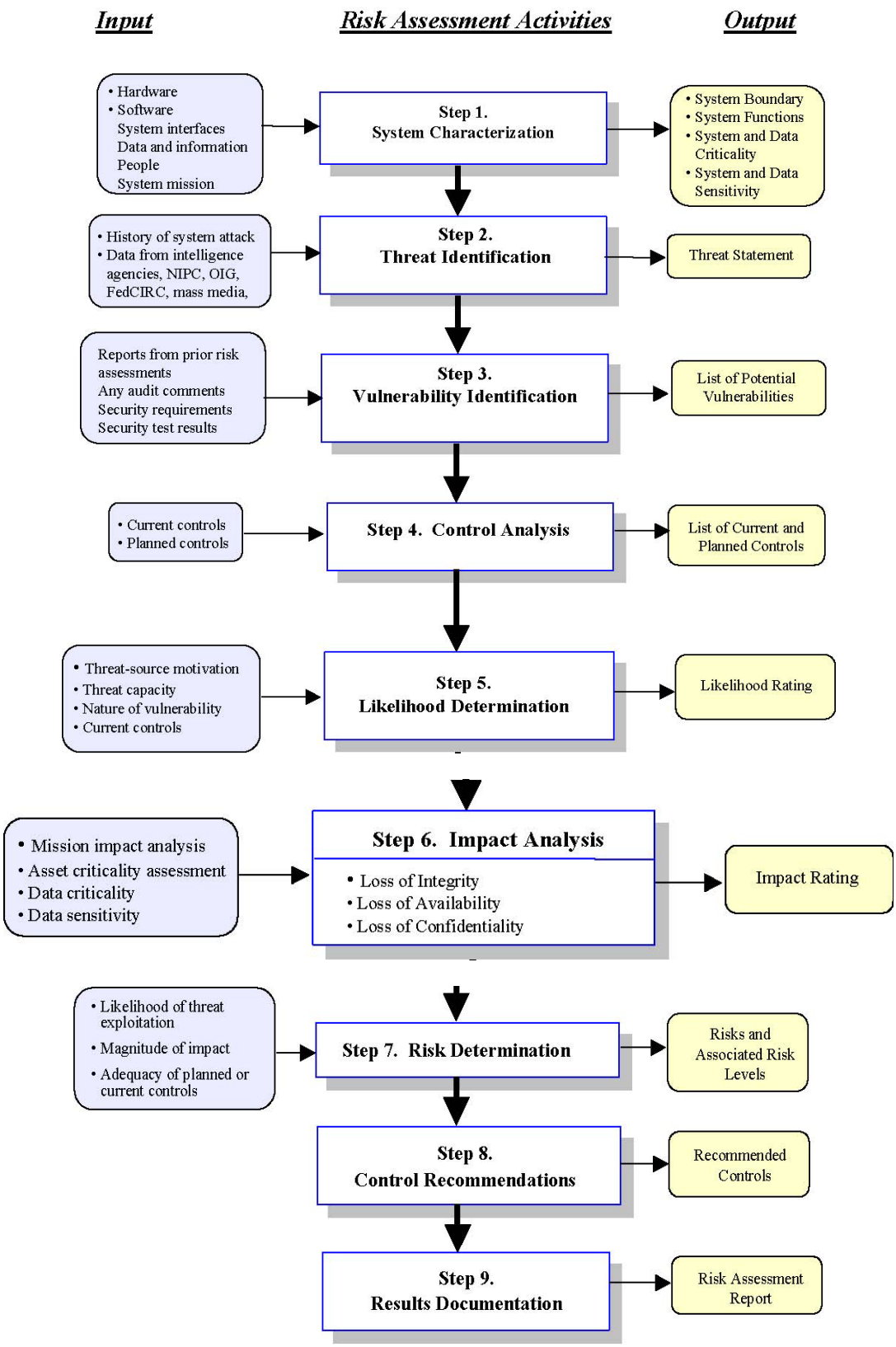

Figure 3-3: Risk Assessment Methodology Flow Chart.

General guidelines for each step in the Risk Assessment Methodology process are defined below:

Step 1) – Characterize the system in terms of scope and boundary. A system may be a single device or a network of computers supporting a common purpose and managed by a single system owner. It may also include assets such as buildings, personnel and network security components. NIST SP 800-18 provides guidance on determining system boundaries. Furthermore, the US Department of Defense (DoD) implements the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) to document systems used within U.S. DoD. This is a fairly involved process and is described in Section 3.1.4.4

Step 2) – Threat Identification. Threats can be categorized as Natural, Human or Environmental. Natural threats are generally related to weather or earthly disturbance such as earthquakes, floods, tornadoes, lightning, etc. Human threats can be intentional or unintentional and are perpetrated by humans. Environmental Threats can be intentional or unintentional and include items such as chemical hazards, pollution and power fluctuations.

Step 3) – Vulnerability Identification may be information obtained from multiple sources, such as open literature, previous security testing, intelligence, etc. Vulnerabilities may include weak system security practices such as easily guessed passwords, lack of physical security, untrustworthy personnel, failure to maintain and update software such as virus scanning and lack of life cycle support.

Step 4) – Control Analysis is the determination of countermeasures to thwart an attacker from exploiting vulnerabilities. Countermeasures can include procedures such as training and implementing strong security polices. It can also include software, hardware and personnel, for instance hosting systems in physically secure spaces with a guard force in place.

Step 5) – Likelihood determination is the process by which an evaluator systematically weighs the extent to which a potential vulnerability will be exploited. Factors used to determine likelihood are motivation and ability of the perpetrator, identified system vulnerabilities and existing countermeasures. For instance a system processing highly sensitive information might be a sought after target for adversaries. However, the risk of detection and attribution could be extremely high. These elements must be balanced to determine the likelihood that a potential attacker would be prone to mount an attack.

The likelihood that a potential vulnerability could be exercised by a given threat-source may be described as high, medium, or low (or more granularly). Table 3-3 below describes three basic likelihood levels.

Table 3-3: Likelihood Definitions

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Step 6) – Impact Analysis is based on a combination of elements and how they affect each other. First, a determination of the impact a successful exploitation may have on the system is required. The evaluator must work with system site personnel and review documentation describing the system. All US Government systems must abide by the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). This is a formal process which documents a system from initial implementation through life cycle management. It includes the operating environment, system security architecture and boundaries, personnel responsible for system maintenance and security, test plans, procedures and results. Once the evaluator has a thorough knowledge about the sensitivity and criticality of the system and its operating environment an impact analysis can be determined. Impacts may be measured in the general terms; High, Medium and Low (or may contain greater granularity). NIST SP 800-30 defines values as depicted in Table 3-4.

Table 3-4: Magnitude of Impact Definitions

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability: 1) May result in the highly costly loss of major tangible assets or resources; 2) May significantly violate, harm, or impede an organization's mission, reputation, or interest; or 3) May result in human death or serious injury.
Medium	Exercise of the vulnerability: 1) May result in the costly loss of tangible assets or resources; 2) May violate, harm, or impede an organization's mission, reputation, or interest; or 3) May result in human injury.
Low	Exercise of the vulnerability: 1) May result in the loss of some tangible assets or resources; or 2) May noticeably affect an organization's mission, reputation, or interest.

An impact analysis can be used to determine cost-benefit criteria. Implementing policy controls such as complex passwords to discourage unauthorized access is an example of a low cost mitigation with high benefit potential. For highly sensitive systems a more rigorous security posture may be required and the cost of implementing additional security features may be high. Each system undergoing impact analysis will be unique. Although there may be many similarities, each system must be treated independently and its security mechanisms and environment must be balanced to produce an acceptable level of risk for the system security manager.

Step 7) – Risk determination is a compilation of information obtained in Steps 1 through 6. Although SP800-30 defines an example matrix to quantify risk levels by assigning values to threat likelihood and threat impact, it is open to the interpretation and experience of the evaluator. The U.S. has not

standardized on any quantifiable risk methodology formula. However the basis for determining risk is common. Figure 3-4 provides a good evaluation tool.

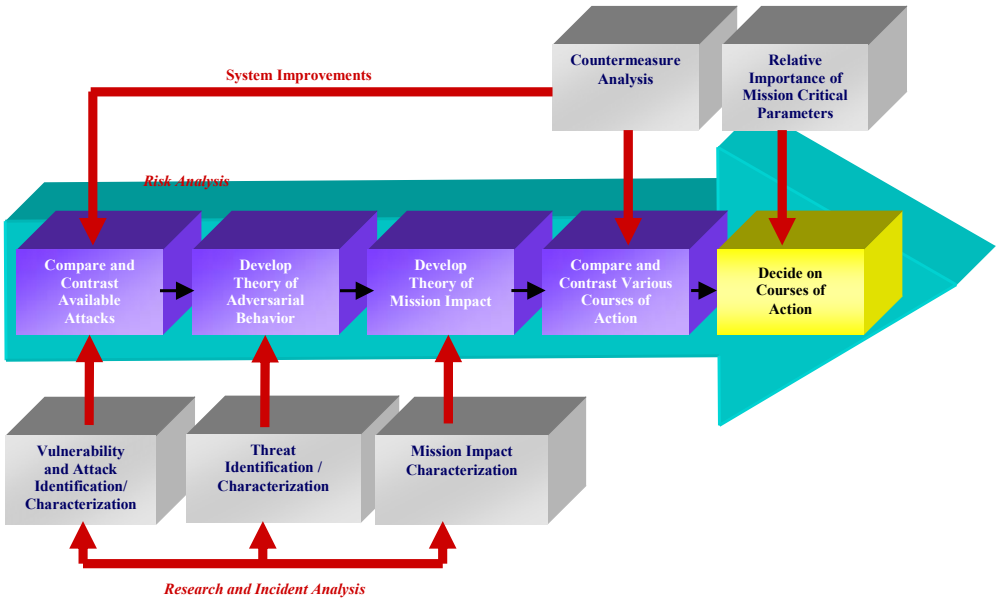

Figure 3-4: Risk Decision Flow Chart.

Risk associated with any system is a function of the comparison of known vulnerabilities, an adversary's inclination and ability to exploit those vulnerabilities and the consistency of security management throughout the life cycle of the system. Unfortunately, the determination of risk level is more dependent on the thoroughness of system documentation and experience of the evaluator than on any methodology.

Step 8) – Control recommendation is the process by which mitigations are introduced to reduce or minimize system risk. Control recommendations are based on the risks identified in Step 7. Control mechanisms may be physical, procedural, software or policy based. A determination must be made as to which control mechanisms to implement, this determination may be based on feasibility, operational impact, effectiveness, level of security required, cost and level of risk acceptance.

Step 9) – Resulting documentation is the residual risk after security controls have been implemented. This document serves as a resource for managers to understand remaining risks and vulnerabilities associated with their information system. Under FISMA and DITSCAP, U.S. Federal agencies use resulting documentation as basis for accrediting a system, whereby the accreditation authority accepts risk for the system and issues an authority to operate (ATO).

3.1.4.3.2 Risk Mitigation

Risk mitigation is the process by which system evaluators and system managers determine which security controls to implement. Determination of available mitigations is based upon the risk assessment process. Again, there are various methodologies for determining risk mitigation, but they follow a common theme. Figures 3-5 and 3-6 support somewhat differing approaches but the end result is to implement security measures that minimize risk to an acceptable level based on mission need. It is the responsibility of system managers to prioritize security controls against identified risks and determine a means for implementing and maintaining those controls.

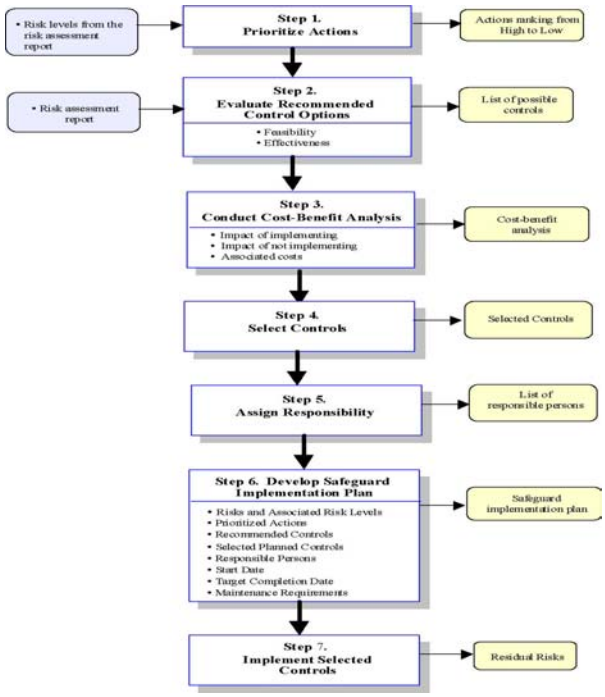

Figure 3-5: Risk Management Process.

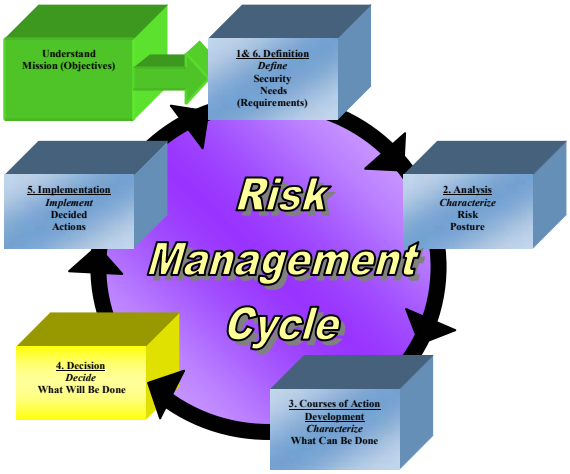

Figure 3-6: Risk Management Cycle.

3.1.4.3.3 Evaluation and Assessment

Most information systems require periodic updating, resulting in re-evaluation of system security posture. The U.S. DoD accredits systems for no more than three years; therefore the risk assessment process must be re-visited periodically. In addition, security patches and software updates are mandatory based on newly discovered vulnerabilities. It is important for information technology professionals to remain diligent in maintaining fixes because most information systems are interconnected to other networks. Vulnerabilities in a single system may propagate throughout a national or global network if left unchecked. An equally important factor in maintaining a secure environment is training. Often personnel are transferred to new jobs without providing training to new personnel in system security practices.

3.1.4.4 Department of Defense (DoD) Information Technology Security Certification and Accreditation Process (DITSCAP)

The DoD Information Technology Security Certification and Accreditation Process (DITSCAP) is a standard process used to implement and maintain the security of information systems which connect to the Defense Information Infrastructure. The primary goal of the DITSCAP is to provide evidence that IT systems implement sound security practices to certify and accredit usage. All system information is documented in a System Security Authorization Agreement (SSAA); this is a formal agreement between certifying officials and site personnel. The DITSCAP consists of four phases:

Phase I: Definition – During this phase, information is collected concerning the system and its environment, security requirements, level of effort and resource allocation. In this phase the SSAA is initiated.

Phase II: Verification – This phase includes identifying and analyzing security vulnerabilities of the target system. Implementing security controls to minimize system risk and verifying that these controls are in place.

Phase III: Validation – During phase III, testing is performed to validate security controls are applicable and effective. Test results are compiled and residual risk is documented, based on this evidence the approving official determines whether to accredit operation and connection of the system.

Phase IV: Post Accreditation – The final phase serves to ensure the approved level of risk is maintained throughout the life cycle of the system. Periodic validation and review of security and configuration management are included in this phase.

The SSAA is a living document that is maintained as long as the system remains operational. The SSAA contains the following characteristics:

1) Describes the operating environment and threat.
2) Describes the system security architecture.
3) Establishes the C&A boundary of the system to be accredited.
4) Documents the formal agreement among the DAA(s), Certifier, user representative, and program manager.
5) Documents all requirements necessary for accreditation.
6) Documents all security criteria for use throughout the IS life cycle.
7) Minimizes documentation requirements by consolidating applicable information into the SSAA (security policy, concept of operations architecture description, etc.).
8) Documents the DITSCAP plan.
9) Documents test plans and procedures, certification results, and residual risk.
10) Forms the baseline security configuration document.

3.1.4.5 Conclusion

Although certain risk methodology tools can assist in determining system risk, results are only one aspect of the overall process. A thorough understanding of system mission, operating environment, system risk and mitigations and life cycle management are required. But, the main determination of system risk lies with the competency and experience of information professionals performing the evaluation.

3.1.5 Czech Methodology

The main steps of this method are:

- Assets identification;
- Threats identification;
- Evaluation of Probability of Threats realization;
- Evaluation of Vulnerability of Assets to the Threats; and
- Calculating of Risk value for every Asset and Threat pair.

After identifying the assets, they are valuated. Assets value vary from 0 (negligible: Asset loss, damage or security violation has only slight or no influence on IS operation and security) to 5 (very high: Asset loss, damage or security violation means outage of the whole IS operation or perhaps total loss of IS security as a whole or important part).

The values should be applied to the costs of obtaining and maintaining a particular Asset and also to the potential impact on organization behaviour in case of loss or damage of the Asset.

Criteria used to determine assets values:

- Non compliance with law and/or regulations;
- Damage or break-up of business;
- Loss of good reputation, negative influence on organization image;
- Reduction of security for organization members;
- Unfavourable impact of law;
- Violation of business secret;
- Breaching the purchase order; and
- Financial loss.

The threat probability is estimated by a value from 0 (the threat cannot occur) to 6 (the threat occurrence is certain or the threat occurs often or regularly or it is a case of continuously threatening status (defect) assessment).

Vulnerability evaluation is then performed. It includes identification of:

- Weak point; and
- Existing security mechanisms.

Weak points can be:

- Physical environment;
- Employees, management and administrative procedures a mechanisms; and
- HW, SW, communication equipment, company premises, etc.

Weak points can be used by the threat to damage assets and business procedures supported by assets.

Vulnerabilities are reduced by existing security mechanisms.

An asset vulnerability to the threat is estimated from 0 (the threat cannot occur for the asset) to 4 (the asset is insufficiently resistant to the threat occurrence or is not protected at all).

The risk value is calculated with the following formula:

Final risk = Asset value * Probability of threat occurrence * Vulnerability of assets group

According the value of the final risk are defined as:

- High risk in the range 61 – 90
- Medium risk in the range 31 – 60
- Low risk in the range 1 – 30

3.1.6 Spanish Method MAGERIT

MAGERIT risk analysis is a methodical approach to determine the risk, following specific steps:

1) Determine the relevant assets for the organisation, their inter-relationships and their value i.e. what prejudice (cost) would be caused by their degradation.
2) Determine the threats to which those assets are exposed.
3) Determine what safeguards are available and how effective they are against the risk.
4) Estimate the impact, defined as the damage to the asset arising from the appearance of the threat.
5) Estimate the risk, defined as the weighted impact on the rate of occurrence (or the expectation of appearance) of the threat.

In order to organise the presentation, steps 1, 2, 4 and 5 are handled first, skipping step 3, so that any estimates of impact and risk are "potential" if no safeguards are deployed. Once this theoretical scenario is obtained, the safeguards are incorporated in step three, providing realistic estimates of impact and risk.

The following figure shows this first pass, the steps of which are described in the following sections [5]:

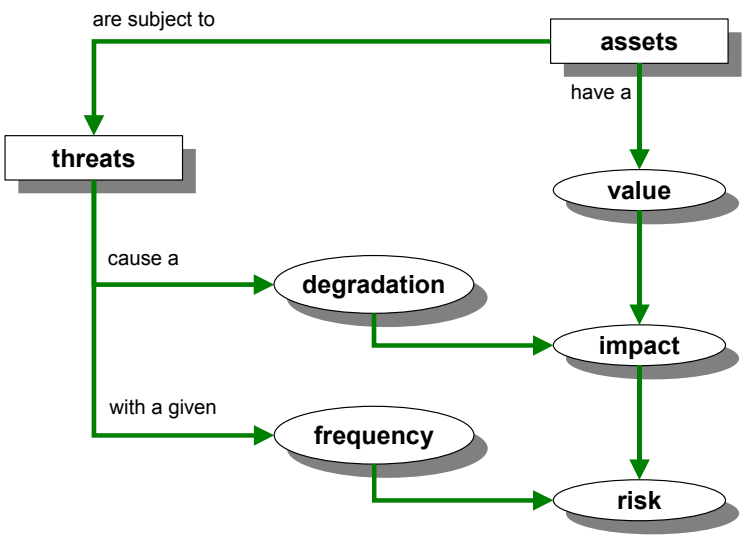

Figure 3-7: MAGERIT Main Steps.

[5] Readers familiar with Magerit v1.0 will notice the absence of the "vulnerability" concept (the potential or possibility that a threat will occur to an asset) which is incorporated using the degradation measurements of the asset and the frequency with which the threat occurs.

3.1.6.1 Step 1: Assets

The assets are the resources in the information system or related to it that are necessary for the organisation to operate correctly and achieve the objectives proposed by its management.

A type can be assigned to each asset. Dependencies can also be established . A "higher asset" is said to depend on the "lower asset" when the security needs of the higher one are reflected in the security needs of the lower one. In other words, when the appearance of a threat in the lower asset has a prejudicial effect on the high asset. Informally, this could be interpreted as the lower assets being the pillars that support the security of the higher assets.

Although it is necessary to adapt to the organisation being analysed in each case, the group of assets can frequently be structured into layers, where the upper layers depend on the lower ones.

Assets are the valuated, either in a qualitative or quantitative way.

3.1.6.2 Step 2: Threats

The next step is to determine the threats that may affect each asset.

Once it has been determined that a threat may damage an asset, the asset's vulnerability[6] must be estimated considering two aspects:

Degradation: The amount of damage done to the asset.

Frequency: How often the threat appears.

Degradation measures the damage caused by an incident if it occurs.

Degradation is often described as a part of the asset's value and therefore expressions appear such as that an active has been "totally degraded," or "very slightly degraded". When the threats are not intentional, it is probably enough to know the physically damaged part of an asset in order to calculate the proportional loss of value. But when the threat is intentional, one cannot think of proportions since the attacker may cause a great deal of damage selectively.

Frequency[7] puts degradation into perspective since one threat may have terrible consequences but very unlikely to occur while another threat may have very small consequences but be so frequent as to accumulate into considerable damage.

Frequency is modelled as an annual occurrence rate with the following typical values:

100	very frequent	daily
10	frequent	monthly
1	normal	annually
1/10	infrequent	every few years

[6] Readers familiar with Magerit v1.0 will notice the absence of the "vulnerability" concept (the potential or possibility that a threat will occur to an asset) which is incorporated using the degradation measurements of the asset and the frequency with which the threat occurs.

[7] Measured as the average number of occurrences of the threat over a specific period. Typically, it is estimated annually. For example, if a fault occurs in a system's air conditioning on an average of five times a year, that is the frequency: 5.

3.1.6.3 Step 4: Determination of the Impact

Impact is the measurement of the damage to an asset arising from the appearance of a threat. By knowing the value of the assets (in various dimensions) and the degradation caused by the threats, their impact on the system can be derived directly.

3.1.6.3.1 Accumulated Impact

This is calculated for an asset taking into account:

- Its accumulated value (its own plus the accumulated value of the assets that depend on it).
- The threats to which it is exposed.

The accumulated impact is calculated for each asset, for each threat and in each evaluation dimension, being a function of the accumulated value and of the degradation caused.

Because the accumulated impact is calculated on the assets that carry the weight of the information system, it allows the determination of the safeguards to be adopted in the working media: protection of equipment, back-up copies, etc.

3.1.6.3.2 Deflected Impact

This is calculated for an asset taking into account:

- Its intrinsic value.
- The threats to which the assets on which it depends are exposed.

The deflected impact is calculated for each asset, for each threat and in each valuation dimension, being a function of the intrinsic value and of the degradation

Because the deflected impact is calculated on assets that have their own value, it allows the determination of the consequences of the technical incidents on the mission of the information system. It is therefore a management presentation that helps in making one of the critical decisions of a risk analysis: accepting a certain level of risk.

3.1.6.3.3 Aggregation of Impact Values

The above paragraphs determine the impact of a threat on an asset in a certain dimension. These single impacts may be aggregated under certain conditions:

- The deflected impact on different assets may be aggregated.
- The accumulated impact on assets that are not inter-dependent and that do not depend on any higher asset may be aggregated.
- The accumulated impact on assets that are not independent must not be aggregated because this would imply overrating the impact by including the accumulated value of the higher assets several times.
- The impact of different threats on the same asset may be aggregated although it is useful to consider to what measure the different threats are independent and may be concurrent.
- The impact of a threat in different dimensions may be aggregated.

3.1.6.4 Step 5: Determination of the Risk

Risk is the measurement of the probable damage to the system. Knowing the impact of the threats to the assets, the risk can be derived directly simply by taking into account the frequency of occurrence.

The risk increases with the impact and with the frequency.

3.1.6.4.1 Accumulated Risk

This is calculated for an asset taking into account:

- The accumulated impact on an asset arising from a threat.
- The frequency of threats.

The accumulated risk is calculated for each asset, for each threat and each valuation dimension, being a function of the accumulated value, the degradation caused and the frequency of threat.

Because the accumulated risk is calculated on the assets that support the weight of the information system, it allows the determination of the safeguards that must be employed in the work media: protection of equipment, back-up copies, etc.

3.1.6.4.2 Deflected Risk

This is calculated for an asset taking into account:

- The deflected impact on an asset due to a threat.
- The frequency of the threat.

The deflected risk is calculated for each asset, for each threat and in each valuation dimension, being a function of the intrinsic value, the degradation caused and the frequency of the threat.

Because the deflected risk is calculated on the assets that have intrinsic value, it allows the determination of the consequences of technical incidents on the mission of the information system. It is therefore a management presentation that helps in making one of the most critical decisions in a risk analysis: accepting a certain level of risk.

3.1.6.4.3 Aggregation of Risks

The above paragraphs determine the risk to an asset of a threat in a certain dimension. These single risks may be aggregated under certain conditions:

- The deflected risk on different assets may be aggregated.
- The accumulated risk on assets that are not inter-dependent and do not depend on any common higher asset may be aggregated.
- The accumulated risk on assets that are not independent must not be aggregated since this would imply overrating the risk by including the accumulated value of higher assets several times.
- The risk of different threats on the same asset may be aggregated although it is useful to consider to what measure the different threats are independent and may be concurrent.
- The risk of a threat in different dimensions may be aggregated.

3.1.6.5 Step 3: Safeguards

The above steps have not included the safeguards deployed. Thus, the impacts and risks to which the assets would be exposed if they were not protected in any way are measured. In practice, it is unusual to find unprotected systems: the measures described indicate what would happen if the safeguards were removed.

Safeguards enter into the calculation of the risk in two ways:

Reducing the frequency of threats

These are called preventive safeguards. Ideally, they completely prevent a threat from occurring.

Damage limitation

There are safeguards that directly limit any degradation while others allow the immediate detection of the attack to stop the progress of the degradation. There are even some safeguards that are limited to allowing the quick recovery of the system when the threat destroys it. In all of these versions, the threat occurs but the consequences are limited.

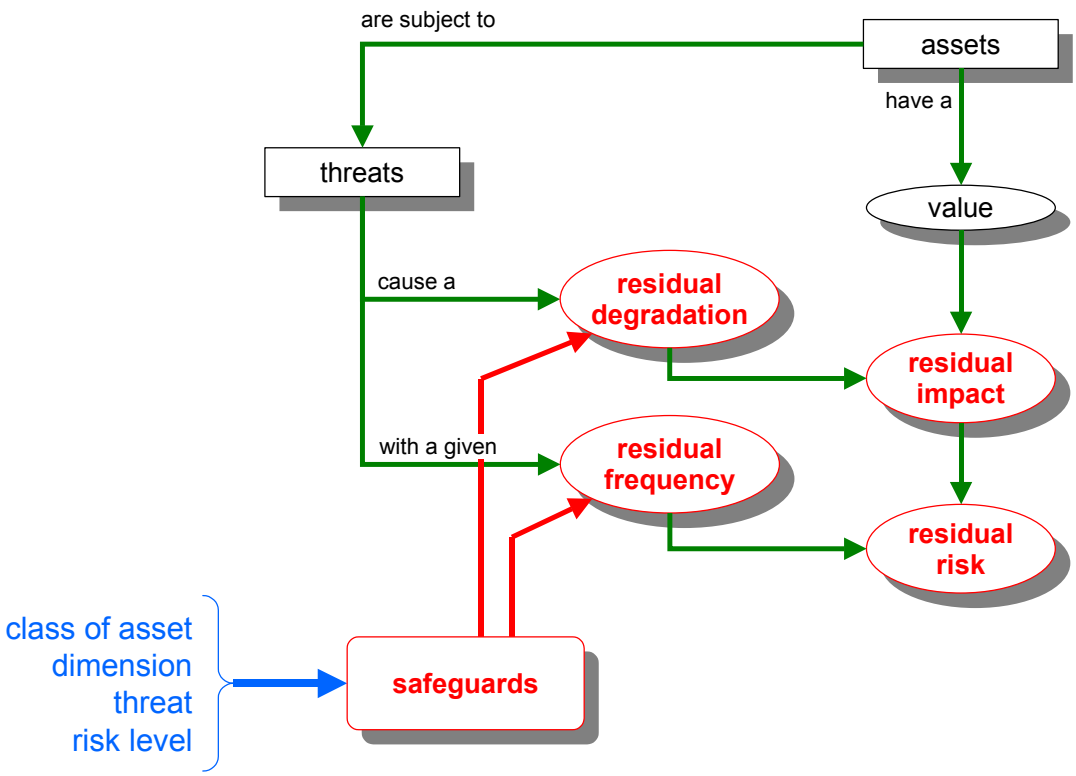

Figure 3-8: MAGERIT Main Steps, including Safeguards.

As well as being classified by their existence, safeguards are also classified by their effectiveness against the risk that they prevent.

3.1.6.6 Revision of Step 4: Residual Impact

The calculation of the residual impact is simple. Since neither the assets nor their dependencies have changed, only the size of the degradation, the impact calculations are repeated with this new degradation level.

The size of the degradation, taking into account the effectiveness of the safeguards, is the proportion that remains between perfect effectiveness and real effectiveness.

The residual impact may be accumulated on the lower assets or deflected on the higher assets.

3.1.6.7 Revision of Step 5: Residual Risk

The calculation of the residual risk is simple. Since neither the assets nor their dependencies have changed, only the size of the degradation and the frequency of threats, the risk calculations are repeated using the residual impact and the new rate of occurrence.

The size of the degradation is taken into consideration in calculating the residual impact.

The size of the frequency, taking into account the effectiveness of the safeguards, is the proportion that remains between perfect effectiveness and real effectiveness.

The residual risk may be accumulated on the lower assets or deflected on the higher assets.

3.2 COMPARATIVE ANALYSIS

By analysing the studied methodology, a synthetic comparative table can be proposed (Table 3-5).

Table 3-5: Comparative Analysis

CRAMM	EBIOS	RISKAN	TRA	MAGERIT	Comments
Gathering background information	Step 1.1: Description of the organization hosting the system		Prepare and plan Define the scope and the boundary of the analysis Establish a target level of acceptable risk Analyze policy and standards compliance	Process P1: Planning	
Gathering background information	Step 1.2: Description of the target system		Prepare and plan Collect information for the system description Formulate a system description Collect data for analysis Conduct interviews and site visits Record the existing security architecture	Process P1: Planning	
Modelling the system	Step 1.3: Identification of the systems components	Assets identification	Perform an asset sensitivity analysis Identify the critical assets	Assets identification	

CRAMM	EBIOS	RISKAN	TRA	MAGERIT	Comments
	Step 2.1: Identification of the security criteria Step 2.2: Definition of scales Step 2.3: Identification of impacts			Assets valuation	For Defence systems, theses items may be defined once and for all (or at least for types of systems: C3S, tactical systems, real time systems, …)
Valuing assets	Step 2.4: Determination of security needs	Assets value	Perform an asset sensitivity analysis Analyse asset sensitivities	Assets valuation	This is a common step but can a common calculation method be set up?
Identifying threats to assets groups	Step 3.1: Selection Selection of attacks methods (fire, flooding, theft, trap, …) Determination of the related security criteria (e.g. , availability for fire)	Threats identification	Perform a threat analysis Identify potential threat events by which threat agents could impact the assets	Threats identification	A list of attack methods (or threats according to other methods) could be provided as a WG result

CRAMM	EBIOS	RISKAN	TRA	MAGERIT	Comments
Identifying threats to assets groups	Identification of the threatening agents (natural, human, accidental, …) Determination of their capacity	Evaluation of probability of threats realization	Collect data for analysis Collect information about threat agents, threat events and vulnerabilities Perform a threat analysis Identify potential threat agents Analyse the threat agents in terms of capability and motivation Analyse the likelihood of each potential threat event occurring Record the potential threat events by domain and highest-level asset categories	Threats identification	

CRAMM	EBIOS	RISKAN	TRA	MAGERIT	Comments
Assessing threats and vulnerabilities	Step 3.2: Vulnerabilities For each selected attack method, identification of the system vulnerabilities which could allow their realization	Evaluation of vulnerability of assets to the threats	Perform a vulnerability analysis Identify the vulnerabilities Assign a vulnerability severity and exposure ratings Determine the overall vulnerability ratings For each domain, record the vulnerabilities with the highest exposure [or] severity rating, and the vulnerabilities with the highest overall ratings Record safeguards that already protect assets from recorded vulnerabilities	There are no vulnerabilities identified in the MAGERIT method	

CRAMM	EBIOS	RISKAN	TRA	MAGERIT	Comments
	Step 3.3: Threat formulation A threat results from the combination of: • A threatening agent (with a capacity) • An attack method • A set of vulnerabilities • The entities which present those vulnerabilities		Perform a risk analysis Identify possible threat scenarios		

CRAMM	EBIOS	RISKAN	TRA	MAGERIT	Comments
Calculating measures of risks	Step 4.1: Risks formulation A risk results from the combination of: • A threatening agent (with a capacity) • An attack method • A set of vulnerabilities • The entities which present those vulnerabilities • The threat capacity • The security needs • The impacts	Calculating of risk value for every asset and threat pair	Perform a risk analysis Estimate the likelihood of each logical threat scenario occurring. Base the estimate on the likelihood the threat agent acting or the natural phenomenon occurring Analyse the potential impact of each logical threat scenario Assess the level of risk from each logical threat scenario. Likelihood of occurrence and potential impacts are considered	Risk analysis	
Calculating measures of risks	Step 4.2: Security objectives				
Risk management	Step 5.1: Functional requirements		Assess system risks for acceptability	Comparative analysis can be displayed (with /without security measures)	

This table shows that the different methods have a very similar structure with the following main steps:

- Background information;
- System modelling;
- Assets identification;
- Assets valuation;
- Threats analysis;
- Risk analysis; and
- Selection of counter measures.

3.3 ALTERNATIVE METHODS

All the above mentioned methodologies could be considered as exhaustive as they try to analyse all the threats on all assets of a given system. If we consider a very large system with many assets and a lot of potentials threats, themselves based on the existence of numbers of potential vulnerabilities, we arrive to a huge number of combinations. This result in a huge amount of tables and values which oversteps the human analysis capabilities and which are of little help to those in charge of the risk management part of the process. The use of tools are not a solution to this problem, as, on the contrary, they facilitate the possibility to combine automatically the items without any added value on the synthesis of the results.

To go round these reef methods based on attack trees tend to emerge for the analysis of large or complex systems. These methods are derived from the fault tree analysis used for reliability analysis (more information to be found in [W4]).

When using attack tree methods, the analysis is focused on a limited list of feared events which for NATO systems are generally easy to identify (loss of command / control capability, system destruction, …). Then an attack scenario is built with a level of detail increasing as the project moves from definition phase to realization or security evaluation.

The main drawback of this method is that it is not exhaustive. However, if the feared events are chosen carefully, the coverage can be large enough. Among the other drawbacks we can mention the lack of tools and the lack of experience on real systems.

The advantages are the facility to interpret the results due to the graphical representation and also the possible link with the methods and tools used by “red teams” people.

At this moment these methods are still in exploratory phases and it is then difficult to consider them as eligible as common NATO tools. However, we consider that they could be of real help in the future.