Common Methods For Security Risk Analysis

Sylvie Malboeuf, William Sandberg-Maitland, William Dziadyk, Eugen Bacic
Cinnabar Networks Inc.

Cinnabar Networks Inc.
265 Carling Avenue, Suite 400, Ottawa, Ontario K1S 2E1

Project Manager: E. Bacic 613-371-3539

Contract Number: W7714-4-3009 & W7714-4-3010

Contract Scientific Authority: J. Gélinas 613-993-5188

Terms of release:

The scientific or technical validity of this contractor report is entirely the responsablility of the contractor and the contents do not necessarily have the approval or endorsement of Defence R&D Canada.

DEFENCE R&D CANADA - OTTAWA
Contractor Report
DRDC Ottawa CR 2004-247
December 2004

Common Methods

For

Security Risk Analysis

Cinnabar Document Number:	**DRD - 4 - 011**
Client File Number:	**W7714-4-3009-3010**
Document Version Number:	**Version 1.1**
Date:	**12 January 2005**

Cinnabar Networks Inc.

Revisions – Document History

Revision	Date	Description of Revision	Pages Affected
0.1	30 Sep 2004	First Draft Outline	All
0.2	6 Oct 2004	Comments from J. Gélinas	Highlighted
0.3	19 Oct 2004	Draft in progress	
0.32	10 Nov 2004	Incomplete draft for project status	All
0.33	30 Nov 2004	First Draft for review	All
1.0	20 Dec 2004	Final deliverable	All
1.1	12 Jan 2005	Typos, remove “Protected A” by J. Gélinas	All

Executive Summary

The Defence Research and Development Canada (DRDC) is an agency within the Department of National Defence. As the Canadian representative, DRDC provides an authoritative contribution to the NATO Working Group on "Improving Common Security Risk Analysis". Amongst the focused objectives, Canada's involvement is to gather information on national risk analysis methodologies and contribute to the Working Group Report (RTO IST-049 / RTG-021).

This document is the results of a study conducted to document the state of the Canadian risk management. The study provides a history of Canada' initiatives with respect to risk management and investigates how Canada can augment the Working Group with its experiences and its future initiatives and opportunities. In addition, the study presents a comparison between the prevalent Canadian threat and risk assessment methodology (ITSG-04) and the recommendations of the National Institute of Standards and Technology Risk Management Guide for Information Technology Systems (NIST 800-30).

Most governments mandate the requirement for risk management. A risk management program includes such activities as threat and risk assessments (TRA), periodic security audit and certification and accreditation for information systems. These activities permit Senior Management to be aware of the threats surrounding the government critical assets, the level of risk systems operate under and provide processes to maintain a sound security posture. Although most policies dictate the requirement to establish such program, the tools available are complex, often lead to inconsistency in the results, and lack of usefulness. Substantial evolution of risk management has occurred in the past few years, but the tools and documentation have been a significant impediment on further development. There is a definite need to standardize the TRA process and provide system owners with a useful and consistent tool to evaluate the risks to information and IT systems.

The approach to a common framework is emphasized by the need for a common language. The provision of a shared set of concepts and vocabulary can only help unify the disparate terminologies that variant TRA approaches and methodologies have engendered. Equally valuable is the prospective TRA automation or partial automation. Automated tools were premature in the early days when risk management was first introduced. Practitioners have gained expertise and experience in the conduct of TRA. It is recognized that human intervention will most likely be required in any automated TRA, however partial automation may be an initial step toward a common framework.

This study serves as inputs to the RTG-21 report and is used to establish DRDC involvement with the Working Group. Consideration of the recommendations and suggestions for future work will position Canada as a significant partaker to a common solution.

REPORT APPROVAL AND QUALITY ASSURANCE

Project Title: Department of National Defence – Common Methods
Prepared By: Cinnabar Networks Inc.

Cinnabar Networks Resources:
Sylvie Malboeuf, Senior IT Security Analyst, BEng, CISSP
William Sandberg-Maitland, Senior IT Security Analyst, M.S.C
William Dziadyk, Senior Management Technical Review and QA, P.Eng, MSc
Eugen Bacic, Project Manager, MCS

This document was produced in accordance with Cinnabar Networks Inc. Quality Assurance guidelines for documentation production and control in order to maintain a high standard for all client deliverables.

Consultants

Project Manager	Eugen Bacic		
Designation	**Name**	**Signature**	**Date**

QA Manager	William Dziadyk, PEng		
Designation	**Name**	**Signature**	**Date**

Client Acceptance

Scientific Authority	Jacques Gélinas		
Designation	**Name**	**Signature**	**Date**

Common Methods For Security Risk Analysis

TABLE OF CONTENTS

List of Tables

List of Figures

Annexes

1 INTRODUCTION

This document contains an overview of Canada's position with respect to risk management. The report covers a survey and research of risk management methodologies and practices applied by Information Technology (IT) managers. A suggestive examination of risk analysis techniques in terms of defining a common framework with a cumulative association to the Common Criteria (CC) is described for forum discussion.

1.1 PROJECT BACKGROUND

A NATO work group titled "Improving Common Security Risk Analysis" has the task to investigate risk analysis methodologies to decide on a feasibility of a common approach. Today all NATO nations use their own national risk analysis methodologies (for example EBIOS for France, CRAMM for UK and ITSG-04 for Canada). Although these methodologies are based on similar principles, each nation experiences different threats and threat agents, focuses on diverse vulnerabilities and safeguards and has distinctive approach in considering information classification. The increased requirement for interoperability between national and NATO systems suggests that there is value for a common risk analysis approach. A Canadian contribution, received in September 2001, outlined the need for a common NATO classification for threats and vulnerabilities.

This NATO initiative is bringing together experts as part of the Task Group to work towards satisfying the following focused objectives:

a. Identify existing national methodologies;
b. Define main steps for risk analysis with associated tools;
c. Identify security needs;
d. Provide a process to selecting and analysing threats;
e. Provide a process to selecting and analysing vulnerabilities;
f. Define security objectives and requirements; and
g. Study possible links with Common Criteria and related tools.

1.1.1 ROLE OF DRDC

Defence Research and Development Canada (DRDC) is an agency within the Department of National Defence. DRDC provides research and development leadership both nationally and internationally by providing the Canadian Forces with relevant and timely technologies, while at the same time offering attractive collaborative opportunities to other government departments, the private sector, academia and international allies. [1]

With respect to risk management and IT Security, DRDC attends the NATO Working Group on risk management representing Canada with the following tasks [2]:

a. Gather information on national risk analysis methodologies;
b. Identify existing support documentation;

[1] DRDC Web site: http://www.drdc-rddc.dnd.ca
[2] Attachment 2, RTG021 Action List, April 2004.

c. Review and contribute to the Working Group Report; and
d. Provide references for all documents referenced in the national presentation.

1.1.2 SCOPE OF THIS PROJECT

The scope for this project is to provide a history of Canada' initiatives with respect to risk management and investigate how Canada can augment the Working Group with its experiences and its future initiatives. The report presents conclusions and recommendations for future efforts in this area.

1.1.3 PUPOSE OF THE REPORT

The purpose of this report is to provide DRDC Scientific Authority with the information necessary to sustain discussions in the NATO Working Group with respect to the status of Canada initiatives and vision on risk management and to contribute to the RTG-21 report.

1.1.4 DOCUMENT AUTHORITY

This document was developed for DRDC to further research in risk management. The document is under configuration management with the Office of Primary Interest (OPI), the Canadian Scientific Authority for RTO IST-049/RTG-021, Information Operations Section, Defence Research and Development Canada, Tel: 613-993-5188. Any comments should be forwarded to the OPI.

1.2 INFORMATION GATHERING

Information for this project was gathered from a variety of sources including individual interviews, standard references and publications. The Scientific Authority provided a wide range of business and technical documents. An initial kick-off meeting was held in order to validate the project requirements, to gain an appreciation of the background of the project and to establish a project plan with assigned responsibilities. A list of the people interviewed and the documents used and reviewed for the analysis may be found in ***Annex A – Information Resources***.

1.2.1 ACKNOWLEDGEMENT

Cinnabar would like to acknowledge the contribution of representatives from Communications Security Establishment and Treasury Board Secretariat in the pursue of future Canadian initiatives in Risk Management.

2 HISTORICAL PERSPECTIVE ON RISK MANAGEMENT

In the early 1990s, the application of risk management within the Government of Canada was a new, ad hoc or perhaps obscure concept with most IT security and business managers. Globally, this was a turbulent period when the enterprise computer assets in all governments were quickly becoming more geographically and organizationally distributed, and more widely used by non-IT professionals within each of their departments and agencies. The pre-1990 “fortress” data centre security types with centrally mandated security controls could no longer be directly and cost effectively applied in this distributed environment. The “walls” of the “fortress” were “breached” to allow connectivity to external enclaves. With the introduction of many non-homogeneous distributed computing environments having different business and security requirements, it was recognized by the Government of Canada Treasury Board Secretariat (TBS) and the security central agencies (Communications Security Establishment (CSE) and the Royal Canadian Mounted Police (RCMP)) that:

a. Traditional prescriptive approach of mandating (i.e. “shall” implement) specific security controls could not be cost effective;

b. “Absolute security” was not achievable and that a risk management approach was needed; and

c. Many Security Managers were applying the logic behind risk management, however:

   (1) There was no common approach for identifying risk, evaluating risk and applying needed controls to mitigate risks to acceptable levels; and

   (2) There was not a common governance and accountability structure for IT security related risk management.

The “Security Volume” of the Treasury Board Manual, originally published in November 1990, did little to emphasise risk management but the policy had directives on safeguarding sensitive information. A new version of the Security Volume, better known as Government Security Policy (GSP), in June 1994 and a subsequent amendment in June 1995, identified specific requirements for management accountability and protection of information derived from the Access to Information Act and Privacy Act. Risk management became a crucial approach to integrating security in Information Technology projects.

Departments were required to manage security risks by confirming the appropriateness of minimum standards and supplementing these standards where necessary, and eliminating unnecessary expenditures and administrative barriers. Furthermore, the process of Certification and Accreditation was introduced adding pressure to managers for risk mitigation through evaluation and implementation of necessary safeguards. From then on, security in information technology system was no longer a barrier and managers had a means, through risk management, to deal with this “stone wall”. The need for TRA became evident:

a. Integrate security at the beginning of the lifecycle of a system;

b. Minimize cost;

c. Ensure adequate level of protection is provided, (not too much, not too little);

d. Provide Senior Management with options for managing risk; and

e. Ensure accountability through Certification and Accreditation.

Over the last decade, the main elements of the 1994 GSP have proven to be the requirements that Threat and Risk Assessments be performed and that the Deputy Minister within each department be responsible for accepting residual risk (i.e. security accreditation) of IT systems. A culture of IT security risk management has effectively been implemented across all Government of Canada departments and agencies.

2.1 GOVERNMENT SECURITY POLICY

In June 1995, the ultimate objective of the GSP was "to ensure the appropriate safeguarding of all sensitive information and assets of the Federal Government"[3]. The GSP consisted of seven chapters, one policy chapter, and six standards chapters with specific policy statements such as:

a. Materiel and IT assets are to be classified and designated according to their requirements for confidentiality, integrity, and availability, and their value;

b. Sensitive information and assets are to be safeguarded in accordance with minimum standards and an assessment of related threats and risks.

To meet the policy, specific guidelines were developed. The Communications Security Establishment (CSE), in collaboration with several departmental representatives, authored the first Canadian risk management framework for Information Technology (IT) systems. This document is part of the commonly known "MG Series" and was published in 1996.

The current version of the GSP, published February 1, 2002 has a slightly different objective. The policy objective is "to support the national interest and the Government of Canada's business objectives by safeguarding employees and assets and assuring the continued delivery of services". [4] The policy mandates safeguarding of information through continuous risk management and Deputy Head accountability. In addition, specific directives impart on the identification of assets, their corresponding sensitivity and the degree of potential injury to national interest (Classified Information) or private and other non-national interests (Protected Information).

2.2 TIMELINE ORIGINAL TRA METHODOLOGY

As introduced in the previous section, CSE has developed a series of risk management framework documents [5] to help government departments in meeting the GSP requirements. In addition, other departments had started initiatives in this area. In the mid 90, risk management documents were available to Threat and Risk Assessment (TRA) practitioners. These documents expanded on the standards set out in the GSP:

a. MG2 - Risk Management Framework for Information Technology (IT), 1996:

   (1) Provide specific guidance for risk management within an IT system environment and its life cycle;

   (2) The document is still used today.

[3] Introduction to Information Technology Security, Course Number: CSE-300 Version Oct 01, CSE

[4] Government Security Policy, February 1, 2002 – (http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg1_e.asp#eff)

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

b. MG3 - A Guide to Risk Assessment and Safeguard Selection for Information Technology Systems, January 1996;

   (1) Provide specific guidance for risk assessment and safeguard selection process throughout the IT system life cycle;

   (2) The document is still used today.

c. MG4 - A Guide to Certification and Accreditation for Information Technology Systems, January 1996:

   (1) Provide more specific guidance for the certification and accreditation of an IT system throughout its life cycle;

   (2) The document is still used today.

d. ITSG-04 - Threat and Risk Assessment Working Guide, October 1999:

   (1) Provides guidance to an individual (or a departmental team) carrying out a Threat and Risk Assessment (TRA) for an existing or proposed IT system;

   (2) The document is still used today by most practitioners.

The MG series provides a solid theory on risk management to managers but lack of methodology to assign a risk value. A working group was created to developed a corresponding working guide to assign value to assets, threats, vulnerabilities and safeguard effectiveness to obtain a suggestive risk rating with recommendations to reduce the risk to an acceptable level. The document produced was the ITSG-04.

In addition to CSE efforts in developing a TRA guideline, the Royal Canadian Mounted Police (RCMP) has been 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 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.

2.2.1 COMMON LANGUAGE – MAKING THE RELATIONSHIP

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 optimal cost[6]. Risk management is an iterative and cumulative process. The following figure outlines the overall risk management process which involves: planning; the TRA; selection of safeguards; system certification and accreditation; maintenance; and monitoring and adjustments to safeguard selections. Risk management is most effective when applied early and throughout the information technology planning process and in concert with project managers, information technology specialists and users.

[6] 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).

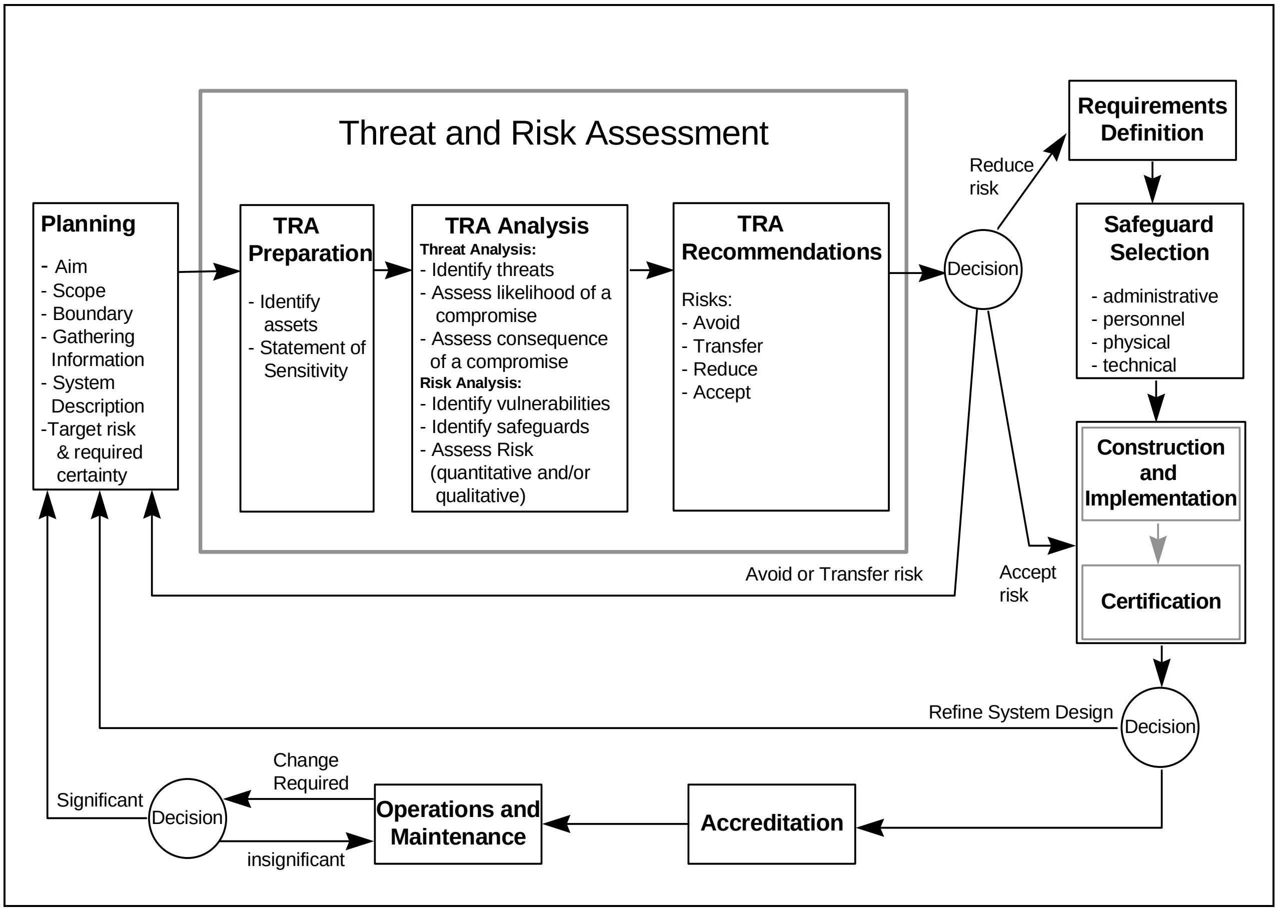

Figure 1. Risk Management Model [7]

Since one of the tools to risk management is TRA, the specific language or terminology used in this context is key to understanding the forthcoming result, the risk. The TRA is a proactive diagnostic tool in determining the current level of **R**isk caused by a **T**hreat Agent acting on a Critical **A**sset of an Information System given its **V**ulnerabilities, or $R = f\ (A_{Val}, T, V)$. Refer to the Glossary of Terms in Annex B for definitions.

The approach to risk management could also be driven by assurance, and the security context by wish one may implement the driving force behind security concerns. The manager should be concerned with the protection of assets from threats, where threats are categorised as the potential for abuse and misuse of protected assets, as shown in figure 2.

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

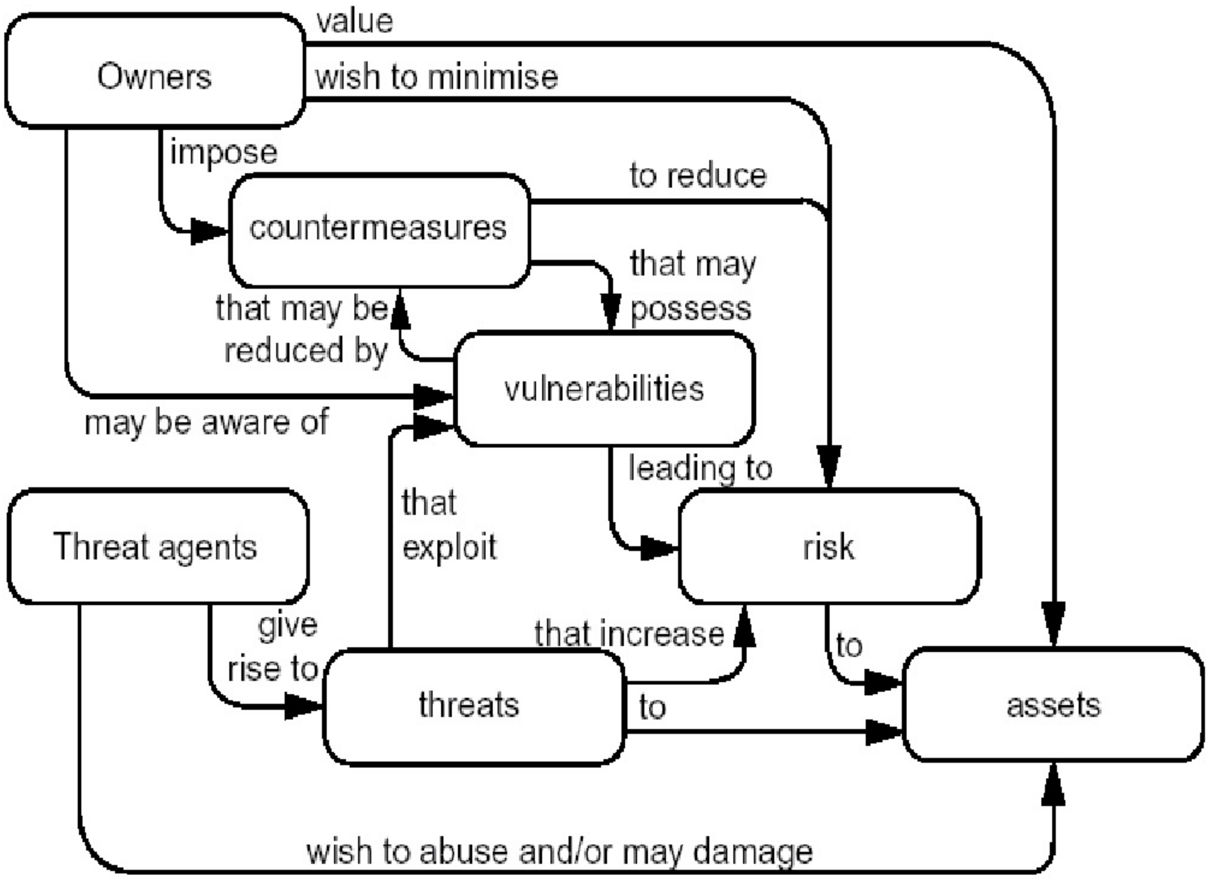

Figure 2. Security Concept and Relationships [8]

The relationship between these two diagrams is genuine although they come from different security methodologies, one being the risk management framework of ITSG-04 and the other being the Common Criteria Part 1. This relationship is presented at this point in the report to emphasize the lack of correlation perceived by the two practitioners' domains and the fact that in Canada, in the early years of risk management, very little work had been done in associating and using the two distinctive but related approaches to risk management. In section 6, discussion with respect to possible common framework is introduced.

2.3 PERCEPTION ON RISK MANAGEMENT TODAY

The risk management directives outlined in the latest GSP (Feb 2002) are emphasised by a second set of documentation known as the Operational Security Standards. Each stated policy is amplified in such documents. The three tiers approach of government security publications, as depicted in figure 3, remains valid but as it relates to risk management a more

[8] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, January 2004 Version 2.2, Revision 256 CCIMB-2004-01-001.

closely unity to baseline security and a view of corporate risk management profile is promoted. Most of the Operational Security Standards will, to a great extent, influence the way risk management is conducted. The reader may refer to Section 3 "Initiatives in this Field" for additional information.

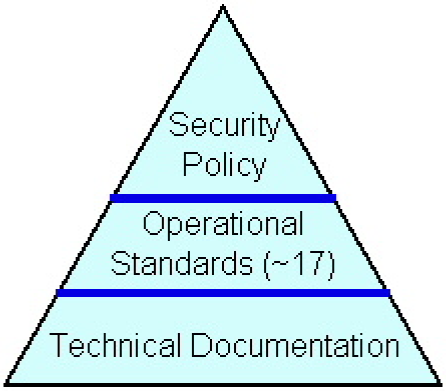

Figure 3. Security Documentation Architecture [9]

2.3.1 OPERATIONAL SECURITY STANDARDS

The development and publication of the operational standards to fit the existing security policy has been a long process. Many of the standards are still being written. Currently available on the TBS web site are:

a. Operational Standard for the Security of Information Act (SOIA), last modified March 17, 2003;

b. Operational Security Standard - Business Continuity Planning (BCP) Program, last modified March, 23, 2004;

c. Operational Security Standard: Management of Information Technology Security (MITS), last modified May 31, 2004;

d. Operational Security Standard - Readiness Levels for Federal Government Facilities, last modified January 11, 2002;

e. Personnel Security Standard - 2-04, last modified October 17, 2002;

f. Physical Security Standard - 2-02, November 15, 1994;

g. Security and Contracting Management Standard - 2-05, last modified June 9, 1996; and

h. Security Organization and Administration Standard - 2-01, last modified June 1, 1995.

2.4 WHAT IS PUSHING RISK MANAGEMENT

Most system and information owners realized the importance of risk management and the fact that a TRA is the basis for many life cycle phases of an IT system. The TRA relation with life cycle phases and other risk management activities can be summarized as follows:

[9] Introduction to Information Technology Security, Course Number: CSE-300 Version Oct 01, CSE

a. Certification and Accreditation activities where the implementation of existing and recommended safeguards derived from the TRA are validated within the system security architecture;

b. Critical deliverable to support the conduct of a Privacy Impact Assessment;

c. Addition of an assurance component when selecting safeguards to link the CC evaluated products to TRA recommended safeguards;

d. Basis for Department Heads' accountability in the safeguarding of government assets;

e. Notion of self assessment to evaluate an organization security posture against an established baseline outlined in policy and operational standards; and

f. Evidence for IT security audit and a means to assess compliance.

2.5 RISK MANAGEMENT IS HERE TO STAY

As introduced in this section, risk management is a relatively new approach to managing IT systems. The security community has adopted frameworks developed in the early stage of decision-making based on risk level. In the next sections, the report offers a comparative approach, where growing expertise has allowed substantial evolution of risk management but where the tools and documentation have been a significant impediment on the evolution of risk management.

3 RISK MANAGEMENT TOOLS

This section expands on current risk management tools available to managers and practitioners. Strength and weakness are outlined and the recognition of problematic within the risk management approach is examined. In the light of such limitation with existing tools, many initiatives are taking place within the Government of Canada (GoC) suggesting a compelling business forefront to risk management.

3.1 METHODOLOGY AVAILABLE IN CANADA

The current GoC information technology risk management is supported by two basics methodologies, the ITSG-04 and the RCMP TRA guidelines. It must be noted that many government departments have developed their own methodology to suit their environment but the root to those remains the formal two basic methods with the occasional insight derived from the NIST [10].

3.1.1 RCMP METHODOLOGY

The RCMP developed two TRA methodologies:

a. The Guide to Threat and Risk Assessment For Information Technology, published in 1994; and

b. 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 of the first publication. Many practitioners use this methodology because it is relatively easy to work with. The analysis is recorded in a table format where the reader can view the overall analysis 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 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 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 implementation.

The RCMP TRA Guide is available to general public on the RCMP – Technical Security Branch (http://www.rcmp-grc.gc.ca/tsb/pubs/it_sec/g2-001_e.pdf). Also, it is available through the government intranet. RCMP provides training sessions on TRA to government employees.

3.1.2 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

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

government employees. This TRA methodology is very comprehensive with ratings for threat 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 threat centric and can be applied to complex networks and systems.

The drawbacks with the ITSG-04 reveal 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 to understand the results. Finally, there is no provision for a remedial or follow-up plan.

The ITSG-04 TRA Guide is available to general public on the CSE web site. CSE provides training sessions on TRA to government employees and security consultants of the private sector.

3.1.3 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 only the emphasis on the TRA components is 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 drawback is with the vulnerability assessment. This step of the TRA can be dealt with at a very high level or a particularly in depth analysis. It was proven at more than once that the TRA results are more consistent. Nevertheless, the depth of the analysis rest with the TRA practitioners and their experience in that field.

3.2 METHODOLOGY AUTOMATION

At present the use of specialized automated risk analysis tools in Canada is probably confined largely to the commercially available tools currently accessible internationally. In this regard the Canadian experience is similar to other countries where no one specific standard or toolset has been mandated or preferred for government use. This lack of perspective does not mean that research and development of risk assessment tools has been historically neglected in Canada.

3.2.1 A SHORT HISTORY ON RISK METHODOLOGY AUTOMATION

There have been many attempts to capture an adequate level of broad abstraction and technology-specific applicability in a general-purpose risk analysis tool. Predominantly, these attempts have taken place within those government agencies whose mandate it is to enforce or assess IT security practice within the government as a whole. The research phase has either been largely initiated within the government, or contracted out to capable commercial firms. Similarly, development has been largely contracted out. The ultimate user base of these tools has been within the government organizations that commissioned them, with a very small distribution and use of certain packages in the private sector.

The use of government-based risk tools has not been large or widespread, even within those government organizations that have initiated their development. A variety of reasons for this drawback can be explained by:

a. The sheer force of new technology in the IT marketplace has obviated older approaches to vulnerability analysis; and
b. The change in security policy models and their enforcing architectures that has been witnessed in the 1990's.

3.2.1.1 The Qualitative Versus Quantitative Approach

To further understand the lack of success with automation, one can first examine developments in the decade that preceded this era. In the 1980's, forward-thinking initiatives such as the NIST Risk Management Workshops evidenced the need for a systematic approach to risk analysis. Much of the early work in this vein was mathematically sophisticated and great attention was given to the models and calculations required to consistently assess risk in a complex computing environment. The Ali Mosleh model from the Risk Management Workshops was particularly influential among Canadian tool-designers in the late 1980's. These models generally favour a software tool solution simply because the complexity of calculation required prohibits a more human-dependent approach. Another feature of this quantitative approach is the need for detailed statistical information. Often, this type of information is not consistently gathered by the client organization and is effectively impossible to reconstruct. In spite of these considerations, a number of commercial risk assessment tools soon appeared on the international scene, some of which have survived to the present.

The initial years of the 1990's saw a steady decline in interest in the formerly pervasive multi-level secure (MLS) operating system with its roots in the risk-mitigating solutions of the cold war era. This critical period was accompanied by a rise in new safeguard technology such as Public Key Infrastructure (PKI), cryptographic tokens, and intrusion detection systems. The Trusted Computer System Evaluation Criteria (TCSEC) Rainbow Series Red Book, which stressed strong network architectural constraints and limited connectivity, proved inadequate to apply in a more open network environment. These parallel developments created a moving target for tool developers and favoured a more adaptive qualitative approach to risk assessment. The increased participation of accounting firms and security auditing requirements in the financial sector favoured, as well, a more procedural and methodology-based approach to risk assessment.

The use of commercial tools in risk analysis was quickly adopted in progressive organizations during the early 1990's, but with mixed results in the Canadian government. Early tools were often not designed with the government perspective in mind, and could only be applied with some difficulty. One such tool, which accepted only monetary valuations of information assets, was adopted as a departmental TRA standard by DND during this period, only to be dropped within a year. In the reaction that followed, more work was put into finding methodological and procedural standards that did not require specific applications other than the optional use of generic spreadsheets, checklists and databases. The latter technologies have proven more than enough to address any computational shortcoming inherent in the qualitative approach, and to further provide sophisticated report generating functionality.

While the importance of risk analysis has remained invariant within Canada over this time period, the automated approaches lost ground to methodological advances in the qualitative risk assessment field. Perhaps another important Canadian factor has been the tendency for lead government organizations in the security field to create and maintain variant models of the risk assessment process. This may have provided too little incentive for the commercial sector to create tools that have too small a market to justify extensive software development. Also, most of the risk management standards that came out at this time seemed to favour a procedural methodological approach. The exception was perhaps the CIS-01-6 standard of DND that included funding of at least one tool built on a database core.

The qualitative approach has dominated the commercial field of risk assessment consulting and government practice in Canada. The Threat Risk Assessment in Canada now tends to be a study by a specialist in the field that documents in a report the findings of the asset sensitivity analysis, IT system vulnerabilities and assumed threat model, and concludes with an overall risk assessment for the system in question. In most cases a recommended set of risk-mitigating safeguards is prepared and a final residual risk assessment is given. A three-point or five-point scale is common for evaluations of vulnerability, threat capability and motivation, and risk.

While many simple tools are capable of providing this kind of outputs, there are few tools that have the current knowledge base or inference engine to correctly reason with the fine points of contemporary IT network architectures and their security technology, as efficiently and as well as a competent human expert. Thus the need for an expert human analyst is currently still strong even in the tool-rich environment. No one has convincingly seen the much hoped-for tool that is strong enough to aid a non-specialist user through a complex risk analysis. Part of the problem is that non-specialists can only afford limited time from their job-related duties for training in a tool technology. At the same time, the advanced technological subject matter of vulnerability analysis, in particular, seems to necessitate a requisite level of knowledge on the part of the analyst. On the other hand, information asset classification is often successfully performed by a non-specialist who has in-depth work experience with organizational assets.

3.2.1.2 THE TOOLS – A FIRST STEP

Given the above perspective, the recognized tools that have been developed during the past two decades within the Canadian government can be considered. One of the early tools that was developed by CSE in partnership with AIT and other commercial consultants is the ExScript tool (1991). This tool runs within a frame-based expert system shell called ExESS (Extensible Expert System Shell). At the time that the project began no commercially available expert system was found that was suitable for the specific risk management criteria that CSE sought. Among those criteria was a flexible support for analysis of highly dynamic environments. A risk management tool called IPSATA (I.P. Sharp Associates Threat Analysis) was an earlier attempt that influenced the design of ExScript / ExESS.

An unusual feature of ExScript is its ability to perform intelligent dynamic safeguard analysis in trusted computing base (TCB) network environments in addition to risk derivation based on a draft Canadian standard similar to the TCSEC Yellow Book. It demonstrated the power of using rule-based reasoning to minimize risk by correct introduction and placement of cryptographic devices in a network. While use of ExScript was not widespread, it provided an exemplar within the Canadian government for a knowledge-based approach to risk management functions. As late as 1996, ExScript was seen as a component of a more ambitious framework of tools named the SERAPE project.

SERAPE included a purely knowledge-based component called TENSAR, based on the Knowledge Interface Format (KIF) developed at Stanford University. Other components such as ExScript, CLIPS, ANSSR and the New Zealand government tool CATALYST were seen as a toolbox for the modeling and analysis of risk in IT systems. Work on SERAPE ceased in the late 1990's, although CSE and DND continued to enter into research and development joint ventures with companies developing specialized risk analysis tools, such as the Vulcanizer project of DOMUS Software Inc. The latter incorporated fuzzy logic to enable security policy / risk analysis in a network setting and presented outputs in 2-D visual format. Some later developments in DND saw greater development of real time risk environments using 3-D data visualization techniques as the presentation layer. The IRONMAN project, which involved commercial intrusion detection tools and interfaced with a specialized module of Vulcanizer, spanned the late 1990's and came to termination in 2001.

3.2.2 AUTOMATION IN RISK MANAGEMENT – A REALITY OR ELSE

One of the main difficulties in the area of risk analysis tool development in Canada has been the viability of various initial versions of tools in the face of changing policies, technologies, risk standards and the knowledge representation required to keep up with time. User interface has proven to be a deciding factor in user acceptance. Some of the tools were found to be difficult to understand or "program". Some had a simple interface but were plagued by intolerably slow performance. User expectation, particularly in visual presentation tools, added to the problem. All of these issues indicate that continued support and funding might be needed to overcome the inertia that too often sets in after an initial success.

On the positive side, the Canadian experience has been strongly oriented towards forward thinking solutions in risk management. The research and development of rule-based tools in the early 1990's showed that, properly configured, these tools can solve much more than just the basic risk determination problem. They can hypothesize solutions to risk problems and suggest variant architectures that may have been overlooked by an expert human analyst.

3.3 OTHER PLAYERS – GOVERNMENT DEPARTMENTS

The minimum expertise in threat and risk assessment within departments and agencies has brought forward the need for simpler methodologies. Many departments tried to resolve the complexity of TRA with the development of an abridged approach to suit their own environment. Regardless of the method instigated, the assessment is most often based either on threat events or vulnerabilities, and sometime a combination of both. Some significant examples are:

a. DND has adopted a checklist type approach as part of their Certification and Accreditation Guideline;

b. Canadian Revenue Agency (CRA) has developed a questionnaire where the system owner has to describe the IT system under assessment and the IT security section review the supporting document with the baseline security model in mind;

c. RCMP has developed, for its internal risk mitigation strategy, a web based TRA framework which builds on threat and vulnerability databases and generates a corresponding report for management review; and

d. Other departments have tried to replicate the ITSG-04 resulting in more complicated methods with additional steps to the analysis.

On the provincial scene, the provincial government or sectors of are promoting their own approach. Some provincial examples are:

a. The government of Ontario has developed a vulnerability assessment methodology to be used as a proactive diagnostic tool in determining, in an effective manner, the various areas of weakness within an information system and implementing mitigation strategies based on industry best standards;

b. The government of Ontario Health sector is promoting a threat and risk assessment methodology with a unique safeguards / risk tracking tool to ensure risk mitigation through implementation of recommended safeguards;

c. Many provinces are adopting a comparable policy to the GSP with similar components (personnel security, classification of data, risk management) to establishing mutual trust and allow for connectivity and interoperability.

3.4 PERHAPS AN ERRONEOUS PROCESS

The methodologies available today are lacking consistency when implemented by the TRA practitioners. There is a definite requirement for uniformity, reusability, traceability and standard format in risk assessment.

3.4.1 MANUAL PROCESS

The problem with manual processes is their potential lack of consistency and variability of output. The insights and experience of a human analyst and those of the interviewees, as well as the soundness of the information sources used in the TRA all contribute towards the reliability of the findings. These facts can revealed to be a strong point as well as a weak point. However, as the sheer volume of risk analysis increases, it does tend to tax the resources of established practitioners in the field and erode quality. Tools can be aimed at the complete process or to specific stages or technology-specific components of the analysis. In Canada, the manual approach is widespread, because the standardization of risk analysis has not been achieved and the various risk assessment methodologies that exist either assume, or favour, a manual sequence of information gathering and documentation tasks.

3.4.2 COMPLEXITY

The complexity of the risk assessment process also varies over different risk standards and frameworks. In some cases, an ad hoc checklist approach is advocated in the interest of obtaining a quick, inexpensive result. On the other extreme, detailed studies involving person-years of work and multi-staged review are sometimes commissioned in the interest of obtaining a sound basis before designing, implementing or releasing a new system. It is difficult to rule out either approach. Either may have economic or assurance constraints and requirements that rationalize their deployment in a given case.

3.4.3 OFTEN LEAD TO INCONSISTENCY IN THE RESULTS

The granularity in the assessment is a key factor to consistent results. The methodologies offer a rating scale of three variables. A much-simplified methodology may provide for high-level analysis and trivial results. A more granular assessment, where the TRA components are rated to a five-variable scheme with detailed rating definition, allows for finer more accurate results and lessens the potential of inflated risk valuation. The result reveals to be more consistent from one TRA analyst to another.

Inconsistency is evident in the depth of the analysis. A more policy-oriented analyst will have the tendency of keeping the analysis at a high level; unlike a hands-on technical consultant will be inclined to provide more in depth technical details especially in the area of vulnerability and safeguards.

3.4.4 LACK OF USEFULNESS

The TRA report including findings, risk rating and recommendations to be considered by the system owner has a place in the life cycle of the system. A TRA report stored on a shelf does little to fulfil the purpose of the exercise except for meeting one specific policy requirement. The fact that a TRA has been conducted does not in itself provide for a sound secured system. System owners tend to be more aware of the importance of a good TRA and its usefulness to manage and implement an IT system. The TRA must be integral to the system implementation and operation. The lack of remedial plan precludes the application of security best practices within the system operation. The capability to direct the TRA recommendations to specific responsibility within an organization, with defined timeframe, priority, and resources put emphasis on accountability and final risk mitigation strategy. A well-conducted, well-managed TRA will accentuate the report usefulness and its reusability.

3.4.5 LACK OF REUSABILITY

Given the large fluctuations of scale and depth of knowledge that a typical risk analysis must deal with, it is clear that the degree to which a risk assessment is reusable or reliable over time is open to debate. Any change in the assets, architecture, threat motivation or capability, or the relative vulnerability of IT components and safeguards can trigger a change in the overall risk assessment of the system. Unfortunately, there is little in the way of methodology or tool base to cope with the dynamic modeling of risk. Another important source of risk change over time is the degree to which connectivity and interfaces may change, either within the boundary of assessment or with external systems.

In all of these situations we know little about the general sensitivity of risk to changes in the underlying IT system and its environment. A large or small change in the architecture or environment does not necessarily imply a large, or respectively, small change in overall risk. This false sense of security is a major area of concern as it determines to a great extent how often a TRA should be repeated on a given system.

3.4.6 DOES NOT MATCH CURRENT POLICY

As outlined in the previous section, the methodologies are outdated compared to the Government Security Policy and its applicable Operational Security Standards. Although the basis of risk management and the conduct of a TRA are fairly static, new security principles may be implicit within a policy and be overlooked by the methodologies. Such a concept exists with the injury test with respect to confidentiality, integrity and availability and the information classification schema of national interest and private or public interest. The last few years have brought significant changes in national policies due to the security events. The methodologies need to be adapted to capture the nuance in interpretation and application of security policy.

3.4.7 NO DEFINITE FRAMEWORK / COMMON APPROACH

To further facilitate the above objectives, it is imperative to work towards a common understanding and acceptance of risk concepts and models in the form of common standards and methodologies. The risk management terminology needs to be unified. The reader may refer to Annex B, Glossary of Terms, and discover the numerous risk management definitions and meanings adopted from different standards.

There is a current need to harmonize risk management standards in Canada. Any cooperation or development in this direction will lead to greater acceptance of risk assessments across large, disparate, yet connected systems that increasingly occur in the Canadian government and business domains. The use of global harmonized security standards such as the Common Criteria and ISO 17799 may further increase the applicability of TRA approach.

3.4.8 MOST AUTOMATION INITIATIVES FAILED

Risk assessment is properly applicable to existing systems of any size and scope, as well as those that are anticipated or planned for future deployment. The latter type of analysis may have inputs that include varying degrees of completeness of life-cycle information on the target system. Trying to find a generic tool that fits all scope and depth of knowledge constraints is not easy. Thus there is bound to be a balance in the field between a tool-driven approach and the completely manual approach of the human analyst.

Perhaps the ultimate expectation in the automation of risk assessment is the paradigm of instant automated TRA assessments based on agent and expert system technology with access to all potential system resources and data-collection tools. This approach is clearly dynamic and may provide a more current and accurate analysis of system assets and threat agents. Some aspects of non-invasive penetration testing may also be integrated into this approach. The Canadian IRONMAN project was an early exemple of what can be done in this area. However, there has been little advance towards this ultimate goal in the past few years.

In view of the above considerations, it is understandable why automation of the risk assessment and management process has had mixed results. One of the key virtues of a well-executed manual study is that rationales are included for all major decisions and analyses within the report. Often in the case of commercial tools, the risk analysis process is entirely black-box in nature, with no convincing trace or rationale for why a specific result was found. This drawback is partly due to the proprietary nature of the algorithms in a given tool, to the complexity of logic that must be rendered during the automated analysis, and the issue of human readability or comprehension in general. A similar situation exists within the formal methods domain, where the actual full mechanical proofs are not generally presented to, or desired by, the user.

There is clearly a role for increased automation of risk analysis. The durability of the current international commercial software in this sector is a testament, at the very least, to their perceived utility and effectiveness. The need for increased automation on the Canadian scene is motivated by requirements for increased efficiency, lower cost per TRA, increased degree of reusability or component-wise composability, and the ability to forecast future risk dynamically.

Not all of these desiderata are achievable in the short run. Some are difficult theoretical problems that have not been solved, or even attempted, in many years. In summary, it is clear that the increased demand in objectivity and reusability can partially be met by further development and use of tools that both avoid the mistakes of the past and draw on past successes.

4 CANADIAN INITIATIVES IN RISK MANAGEMENT

Considering the many security events and the related change requirements 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. Canada recent implementation and operations of Government-on-line (GOL) and Government of Canada (GoC) Electronic Service Delivery (ESD) reaffirm the commitment to provide electronic service delivery to employees and citizens. Furthermore, in the recent years, government departments were introduced to the “conduct of business” within their environment, which lead to new approach to risk management.

4.1 NATIONAL SECURITY POLICY

Risk management encompasses more than just information technology. In the light of recent events in the world, the Canadian Government considered the importance to identify and protect Canada’s critical infrastructure. A new policy was created which governs all other Canadian policies including the GSP.

On April 27, 2004, the Government released "Securing an Open Society: Canada's National Security Policy," a strategic framework and action plan. The National Security Policy focuses on addressing three core national security interests:

a. Protecting Canada and Canadians at home and abroad;

b. Ensuring Canada is not a base for threats to allies; and

c. Contributing to international security.

The Policy includes six key strategic issue areas: intelligence; emergency planning and management; public health emergencies; transport security; border security; and international security. Work on the National Security Policy involves several federal government departments from the areas of intelligence, emergency planning, public health emergencies, transportation security, border security and international security. [11]

The implementation of such policy has ramification in the way government departments and agencies set priority in risk management. Although this policy does not directly address IT, the identification of critical systems and critical assets is a key component to emergency preparedness and critical infrastructure. The introduction, at this point, of the National Security Policy is a leading effort to the contribution and initiatives in risk management by the different departments and agencies.

4.1.1 TREASURY BOARD SECRETARIAT

As the central agency for security and service delivery issues for the Government of Canada, the Treasury Board of Canada Secretariat (TBS) is responsible to develop and update the Government Security Policy and provides strategic direction, leadership, advice and assistance on security and service delivery issues to federal departments and agencies. The current TBS initiatives with respect to risk management are:

[11] Paraphrased from PSEPS Web site: http://www.psepc.gc.ca/publications/news/20041008-2_e.asp#PSEPC

a. The provision of clear direction on grouping of assets (assets profiles), safeguards, vulnerabilities, and threat. The benefit of such approach is to standardized asset profiles to provide departments and agencies with a common baseline to identify GoC critical assets. The cataloguing scheme for safeguards and vulnerabilities will organize the recommended controls in a more logical means to support consideration by senior management and remediation by technical and operations staff. A significant advantage in cataloguing is to promote standard definitions for safeguards and vulnerabilities and encourage TRA reusability;

b. The foundation for a residual risk language that will minimize the inadequacies of the statement of residual risk and in particular how injury is not adequately expressed. This initiative is related to senior executive residual risk acceptance as a management decision. The underlying concepts that lead to a residual risk should be expressed in a business language;

c. The development of a TRA template with a business focus and language, typical to government departments. A standard TRA template will provide for consistency, ease of use and readability, reusability, and added efficiency to the risk management process. A common template will focus the TRA practitioners in meeting the needs of the system owners and departmental IT Security staff. As introduction to departments, the TRA template should be limited to government service delivery with tier level architecture and connectivity to the Internet (application type TRA or system update). This initiative is in line with GOL and GoC ESD and fits many new applications associated with GOL and those legacy applications that are being upgraded to web interface (portal);

d. The development of Operational Security Standards on asset identification and risk management to complement the GSP. This initiative identifies risk management as belonging to three areas: the conduct of TRA, the process of Certification and Accreditation and continuous monitoring through such activities as internal audit, self-assessment and vulnerability analysis. The Operational Standards will ensure the TRA is leverage to other risk management activities such as ITS Self Assessment Methodology, Privacy Impact Assessment (PIA), and Business Impact Assessment (BIA) which is an integral part of the Business Continuity Planning (BCP) and critical system identification;

e. The dissemination the recently published Management of Information Technology Security (MITS) Operational Security Standard. The MITS has replaced the well-known and accepted RCMP standard, Technical Security Standard for Information Technology, (TSSIT) which was obsolete for today's technology environment;

f. The completion of the ITS Self-Assessment Methodology. The trial version of the document has been used by a number of departments in a pilot. The rollup reports from this trial are being used by TBS and the Auditor General for assessing general degree of compliance of departments to the GSP. The methodology is currently being revised in order to update the question set for all five maturity levels to be more consistent with the new MITS, and to develop a web front end for the application; and

g. The update of the GSP to reflect the new language used in the National Security Policy[12] produced by Public Safety and Emergency Preparedness Canada (PSEPC). Security statement and language become key features in understanding Canadian security as a whole.

4.1.2 CSE

As the cryptology and information technology security (ITS) technical authority, the Communications Security Establishment (CSE) is responsible to develop operational standards and technical documentation as it relates to ITS in terms of system certification and accreditation, risk and vulnerability analysis, product evaluation, system and network security analysis. In addition, CSE develops and provides specialized ITS training, especially with respect to network vulnerabilities and relevant technical safeguards. The current CSE initiatives with respect to risk management are:

a. 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;

b. The service offering of an Active Network Security Testing exercise to evaluate departments' network security status provided by the Active Network Security Testing Team (ANST Team). The ANST Team assists management in determining if an ANST Program is appropriate for their organization, positions the exercise within a standard system development lifecycle, and imparts threat information in support of informed risk management decision-making. An ANST exercise provides the system owner with an assessment of the effectiveness of the existing safeguards, countermeasures and controls implemented on the IT system and a means to assess the protection necessary to counter outside threat agents;

c. The revision of all Risk Management reference documents (MG series and ITSG-04) to fit the GSP vision on risk management;

d. The active promotion of the Common Criteria with innovative ideas such as the development of a baseline mapping of TRA safeguard areas to the Common Criteria assurance and functionality classes and families. The approach is to use the qualitative descriptions and structured terminology of controls and safeguards available in the CC framework as guidance within Risk Management. This comprehensive analysis demonstrated that the security assurances and functional requirement classes (SARs and SFRs), and the environmental and security policy components of the CC can be used to enhance and corroborate the TRA findings;

e. The service offering in the area of training. The ITS Learning Centre (ITSLC) offers courses in three areas of IT security: Management Safeguards; Technical Safeguards;

[12] Canada's National Security Policy Securing an Open Society, April 2004.

and Operational Safeguards. Related to risk management, the following courses are offered:

(1) Threat and Risk Assessment (TRA) - Risk Management in a Hostile Environment;

(2) Certification and Accreditation (C&A) - Achieving Confidence and Accountability;

(3) System Security Policies - Capturing IT Security Requirements;

(4) Security Testing and Evaluation - Practical Approaches for System Certification;

(5) Information Infrastructure Protection (IIP) - Technical Framework;

(6) Selecting the Right Security Technologies - Mapping Threat and Risk Assessment to Common Criteria;

(7) Understanding and Applying Product Evaluation - Common Criteria Protection Profiles and Security Targets.

4.1.3 RCMP

As lead department for federal law enforcement, with a crime prevention mission, the Royal Canadian Mounted Police (RCMP) is responsible for providing advice to departments on the process of threat and risk assessments, the conduct of IT system security reviews, inspections and audits, and for providing technical assistance to investigations related to IT. In addition, the RCMP has a lead role in the development and provision of ITS training and awareness. The current RCMP initiatives with respect to risk management are:

a. The provision of risk-based audit services to senior management on the soundness of risk management strategies and practices, management control frameworks, systems and practices, and information used for decision-making and reporting; and

b. The conduct of workshop to assist the security practitioner in conducting a threat and risk assessments in the IT environment, using practical exercises throughout the process.

4.1.4 CSE AND RCMP

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). Presently, this working group is not formalized that is, there is no Memorandum of Understanding in place, but the project has an aggressive time frame of April 2005. The intent is to develop a common TRA framework that can be used uniformly by all departments. The ultimate goal (beyond April 2005) 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.

4.1.5 PSEPC

The creation of Public Safety and Emergency Preparedness Canada (PSEPC) in December 12, 2003, fulfills the fundamental role of government to secure the public's safety and security. PSEPC is dedicated to minimizing a variety of risks to Canadians, from risks to personal safety to crime or naturally occurring events, to threats to national security from terrorist activity.[13] PSEPC provides valuable information on threat and vulnerabilities and is a significant resource for TRA practitioners. With respect to risk management, PSEPC provides such services as:

a. Operational notices via alerts, advisories and information notes as well as analytical products that include threat and incident analyses and infrastructure mapping products.

   (1) Alerts are issued to communicate information about potential, imminent or actual threats, vulnerabilities or incidents affecting the Government of Canada or other sectors of Canada’s critical infrastructure;

   (2) Advisories are used to communicate information about potential, imminent or actual threats, vulnerabilities or incidents assessed as limited in scope but having possible impact on the Government of Canada or other sectors of Canada’s critical infrastructure; and

   (3) Information Notes are used to draw attention to information relating to significant threats and vulnerabilities.

b. The Canadian Disaster Database that contains historical information on disasters. References to all types of Canadian disasters, including those triggered by natural hazards or technological hazards can be found in this database. The database describes where and when a disaster occurred, who was affected, and provides a rough estimate of the direct costs.

4.1.6 NCSIP

The National CIO Council Subcommittee for Information Protection (NCSIP) is a committee with the mandate to develop means to facilitate the sharing of electronic information between provincial, territorial, municipal, and Government of Canada jurisdictions. The NCSIP has recently published a Public Sector Security Classification Guideline to serve as a common reference point for governments wishing to share electronic information and may cross-reference their own information classification rating to this guideline. This document provides an initial first step in the risk management of the sharing of electronic information.

The document is not a mandatory standard but is rather a guideline approved by the Public Sector CIO Council (PSCIOC) to be applied by governments on a voluntary basis to facilitate the sharing of electronic information between government jurisdictions. This schema is not intended to impinge upon the classification schemas or security approaches of individual governments. However, governments may adopt this particular classification schema if they wish. The establishment of a commonly understood and accepted Public Sector Security Classification Guideline is required to protect sensitive electronic information that participating

[13] Role of PSEPC taken from PSEPC Web site: http://www.psepc-sppcc.gc.ca/index_e.asp

jurisdictions wish to exchange. This guideline is primarily intended for information that is not of the national interest.[14]

4.1.7 FASO

The Federal Association of Security Officials is an association that works closely with government security organizations and the security industry to organize training seminars, workshops, and conferences, and provide briefings in such areas as new developments and new technologies.[15] With respect to risk management, FASO offers:

a. Training and awareness initiatives with training courses on the GSP, identification of assets and the conduct of TRA;

b. Developing Policy and Standards with the collaboration of TBS, RCMP and CSE to develop policy and standards within the scope of the GSP, including:

    (1) Physical security;

    (2) Information security;

    (3) Information technology security;

    (4) Personnel security; and

    (5) Security administration.

4.1.8 DEPARTMENTS APPROACH

As mentioned previously in this document, many departments have developed TRA templates to suit their own environment, which proved to be more or less valuable, expertise being the driven factor. In spite of this, large departments have furthered their risk management program with a leading edge approach to TRA. This approach, discovered during a survey conducted on behalf of TBS,[16] reveals significant advantages and cost saving in the conduct of TRA. Since the critical assets and the threat associated with a particular department or agency, are relatively static, the Departmental Security Officer opted to conduct an enterprise-wide Statement of Sensitivity (SoS). The critical assets, mostly information, are presented in the form of asset profiles grouping together information of similar nature, sensitivity and business purposes. The owner of a new application only needs to ensure the information fits one of the profiles, or else, identify any particular, and can rely on this SoS to implement the new application.

Further to the enterprise-wide SoS, a number of departments have conducted TRA on their network environment and infrastructure to define a baseline security model. The threats are identified, labelled and rated as such, appropriate safeguards are put in place to secure the network infrastructure and the residual risk is identified and signed off by Senior Management. A set of minimum-security requirements is conveyed to a system owner who wishes to add a new application or system. A short TRA is necessary to prove the new system / application does not degrade the current network security posture. This simplified TRA may radically

[14] Public Sector Security Classification Guideline, September 2004

[15] FASO Web site: http://www.faso-afrs.ca/about-e.html

[16] Report on the Feasibility of Developing a Threat and Risk Assessment Template for Treasury Board Secretariat, Cinnabar Document Number TBS-4-017, Client File Number 24052-6004286, Version Number Version 1.0, 15 October 2004

overlooked the network infrastructure and assume the appropriate safeguards are in place. This approach benefits in time, money and acceptability regarding certification and accreditation.

One may recognize the benefit of department-wide SoS and network TRA and the distinct relation with TBS initiative with respect to the development of a TRA template for common business process.

4.2 AUTOMATED TOOLS AVAILABLE IN CANADA

As mentioned earlier in the document, a number of risk analysis tools have been prototyped in Canada and supported during the research stage by the Canadian government. In the Canadian commercial section a number of risk analysis and control products have been developed, although the majority deal with financial, corporate or environmental risk, or else, are applicable only in specific business sectors such as oil and gas resource.

An example of a product that has more general capabilities is the CARD®*map* software by Paisley Consulting, from Toronto. This product is designed to help organizations meet risk and control governance responsibilities including operational risk requirements. It is described as a “Web-enabled software program that charts and monitors any facet of an organization's operation”. It allows users to create a survey of objectives, risks, controls, and residual risk status by identifying problems, monitoring process performance, assigning responsibility and prioritizing action items. A database of loss history, risk exposures, controls, residual risk status, action plans and quality assurance work for an entire organization is built. As such, tools such as this and RiskCommander (by TruSecure, Hearndon, Virginia) are effective in demonstrating compliance in a security audit.

Another commercial product that has been used in the past in Canadian government applications is RiskWatch. This tool was more approachable but it did not fit in with the business processes.

4.2.1 ARE THEY USEFUL?

It is not clear that such tools meet the government standards currently in force within Canada, although they may be a component in meeting these requirements. The main challenge in using automated tools is ensuring that the tool reflects the business process of the system under analysis. For example, if valuation of assets is only offered in monetary terms such as in the Annual Loss Expectancy approaches, the national interest based sensitivity values and injury test used in Canadian Government applications is difficult to model or translate properly.

Another difficulty is the dependence on subjective assessments that many qualitative tools have. While subjectivity is a potential in any data collection process, the quality of an analysis using only subjective inputs is more open to question than an analytical model based on architectural inputs and frequencies of security incidents. Again the black-box nature of many commercial tools does not permit a complete judgement of their relative strengths and weaknesses, or anything approaching a comparative analysis.

The expertise in risk management, gained from all those years of trials, success and failures, is a positive aspect in automation of risk management tools. Extensive discussion is provided in Section 6.

4.3 EXPERTS IN THE FIELD

Although risk management is accountable to department 's Head, the expertise in the conduct of TRA is sparse in many departments. The cost of developing inside expertise and the assignment of personnel resources to this demanding task are prohibitive. The conduct of TRA remains with security consultants.

4.3.1 ADVANTAGE / DISADVANTAGES OF USING THIRD PARTY

During a survey conducted for TBS, on the usability of TRAs, the IT security officer was asked to comment on the use of third party to conduct TRAs. The following observations were recorded:

a. **Advantages**: The security consultant provides for a different viewpoint has an outsider to the organization. He/She is able to perceive the overall vision, from the security rules advocate by the security section to the system and information owners operational requirements to the users convenience. Most consultants have gained a great deal of expertise over time with specialization in the area of threat analysis, vulnerabilities and safeguard recommendations. Consulting companies have the resources even in rush of the end of the fiscal year. The security consultant can provide for an independent assessment with unbiased solutions and recommendations.

b. **Disadvantages**: Notwithstanding the cost associated with the security services, it is common for departments to fund projects over and over for the same analysis portion. Consultants do not know the existing baseline such as the network infrastructure, common threats to the organization and common departmental practices like personnel security clearance. Although not unique to security practitioners, it has been acknowledged that the government contracting process is overwhelming, time consuming and often results in unsatisfactory outcome.

A solution to the contracting process was to set master standing offers in the area of security consulting to ease the process, provide for genuine expertise, and ensure competitive prices.

4.3.2 ITISPS

The Information Technology Infrastructure Security and Protection Services (ITISPS) is a National Master Supply Arrangement, which became effective on August 1 2002. CSE[17] has established the ITISPS Supply Arrangements with four firms, (refer to Table1), through Public Works and Government Services Canada to provide Federal Government Departments and Agencies with a contractual vehicle that can be used to provide Information Technology Security (ITS) and Information Infrastructure Protection (IIP) Professional Services. The supply arrangement is divided in three Tiers of services:

a. Tier One - Risk Management Services;

b. Tier Two - Information Infrastructure Protection Services; and

c. Tier Three - Research and Development Services.

[17] http://www.cse-cst.gc.ca/en/services/industrial_services/itisps_program.html

Table 1. ITISPS Selected Firms

ITISPS Selected Firms – All located in Ottawa	
AEPOS Technologies Corporation Contact: John Detombe Director, Information Security Tel: (819) 772-8522 Fax: (819) 772-0449 E-mail: jdetombe@adga.ca Web site: www.aepos.com	CGI Information Systems and Management Consultants, Inc. Contact: Andrew Pridham Director, Consulting Services InfoSec Centre of Expertise Telephone: (613) 566-4680 Fax: (613) 234-6934 E-mail: andrew.pridham@cgi.ca Web site: www.infosec.cgi.com
Cinnabar Networks Inc. Contact: R.D.(Bob) Henry Principal Cell: (613)371-3539 Fax: (613)236-2506 E-Mail: bhenry@cinnabar.ca Web site: www.cinnabar.ca	TRM Technologies Inc. Contact: Gareth Hughes Telephone: (613) 722-8843, ext 103 E-mail: ghughes@trm.ca Web site: www.trm.ca

All four Companies can provide Tier One services under the ITISPS Supply Arrangements. Tier One deals with Risk Management Services including such activities as:

a. Requirements analysis and studies;
b. Security architecture design and engineering support;
c. Development methodologies, policies, procedures, standards and guidelines related to Information Technology Security;
d. Evaluation of IT security products;
e. Threat Risk Assessment, Network Certification and Accreditation and Business Continuity Planning activities;
f. Project Management support to IT Security related projects;
g. Security audits and security awareness training;
h. Independent Verification and Validation (IV & V) support to ITS related projects;
i. ITS systems installation and operation support; and
j. Network Vulnerability analysis.

Only Cinnabar, AEPOS and CGI can provide Tier Two services under the ITISPS Supply Arrangements. Tier Two deals with Information Infrastructure Protection Services including such activities and services as:

a. Network vulnerability assessments;
b. Analysis of threat agents;

c. Development of methodologies, policies, procedures, standards and guidelines related to Information Infrastructure protection;
d. Analysis of tools or techniques;
e. Analysis of technical trends;
f. Incident analysis support; and
g. Training and awareness.

Only Cinnabar, AEPOS and TRM can provide Tier Three services under the ITISPS Supply Arrangements. Tier Three deals with Research and Development Services including such activities and services as:

a. R&D activities related to IT software and hardware security products;
b. R&D related to IT security protocols at all layers of the OSI and TCP/IP stacks;
c. Analysis of R&D reports;
d. Development of policies, procedures, standards and guidelines development related to R&D; and
e. Participation in National/International R&D forums.

4.3.3 IPS

The Informatics Professional Services (IPS)[18] is available to IT security firms to provide services to Government Departments. The IPS is an electronic procurement tool that assists federal departments in the procurement of informatics services in the National Capital Region, below the NAFTA threshold. The client department can complete a search through the database on predetermined criteria. The search results will provide a list of potential consultants with comprehensive information about the consultants' skills sets, areas of experience, years of experience and per diem ceiling rates. Cinnabar offers his services through IPS.

4.3.4 COMMON CRITERIA EXPERTS

The Canadian Common Criteria Evaluation and Certification Scheme (Canadian CCS)[19] is an independent third party evaluation and certification service for measuring the trustworthiness of IT security products and systems. In order to speed the approval of IT security products and to maximize opportunity for their vendors, the Governments in Canada, the United States, United Kingdom, Netherlands, Germany, and France are part of the Mutual Recognition Arrangement (MRA) based on the Common Criteria (CC). Under the MRA, the results of a product evaluation conducted in one of these countries are automatically recognized in the others. In Canada, three firms have been accredited as IT Security Evaluation and Testing (ITSET) Facility, under ISO/IEC 17025-1999, and are approved to perform CC evaluations by CSE. Additional, several IT security firms are recognized by CC experts as having expertise in CC consulting, including research, document productions and document review.

[18] http://www.pwgsc.gc.ca/sipss/pspd/ips/home-e.htm
[19] http://www.cse-cst.gc.ca/en/services/common_criteria/ccs_overview.html

Table 2. Common Criteria Expertise

Common Criteria Laboratories	
CGI Information Systems and Management Consultants Inc. 275 Slater Street, 14th floor Ottawa, Ontario, K1P 5H9 Contact: Cal Clupp (613) 234-2155	DOMUS IT Security Laboratory 2220 Walkley Road Ottawa, Ontario, K1G 5L2 Contact: Greg Scorsone (613) 247-5509
EWA - Canada 55 Metcalfe Street, Suite 1600 Ottawa, Ontario, K1P 6L5 Contact: Paul Zatychec (613) 230-6067 ext. 1227	
Common Criteria Consulting	
Cinnabar Network Inc 265 Carling Avenue, Suite 200 Ottawa, Ontario, K1S 2E1 Contact: Eugen Bacic (613) 724-9577	AEPOS Technologies Corporation 200-200 rue Montcalm Hull, Quebec, J8Y 3B5 Contact: John Detombe (819) 772-8522
Mantricon Consulting Inc. 1269 Maitland Avenue Ottawa, Ontario K2C 2C4 Contact: William Sandberg-Maitland (613) 298-3416	Armacode Inc. #252 – 99 Bank Street Ottawa, Ontario K1S 5P4 Contact: William Pase (613) 237-5590

4.4 A SHORT COMPARISON – ITSG VERSUS NIST

This section presents a short comparison between the Canadian most popular TRA methodologies, “Threat and Risk Assessment Working Guide” (ITSG-04) published by Communications Security Establishment and the “Risk Management Guide for Information Technology Systems” (800-30) from the National Institute of Standards and Technology (NIST). The purpose of this comparison is to reaffirm the need for a common TRA methodology with common terminology, common business goals and common framework in the light of interoperability among NATO participating nations.

The selection criteria for the comparison were influenced by the fact that the NIST 800-30 is sometime used in the conduct of TRA in Canada. A comparison table is available in ***Annex C. Comparison Table ITSG-04 Versus NIST 800-30***. This table provides observations on both methodologies and interpretation on the difference between the 800-30 and the ITSG-04. It must be noted that the observations provided in this report are based on the analyst experience and expertise and should not be taken as judgmental. The following observations are derived from the comparison table:

a. Both methodologies have very similar approach to risk management;

b. Both introduce the principle of TRA throughout a system development life cycle;

c. ITSG-04 is used for classified and protected information assets, it has a more government security minded principles and terminology. The 800-30 stresses the privacy of sensitive unclassified information for federal computer systems. This methodology has a more business oriented terminology, for examples:

   (1) ITSG-04: Threat agent - Threat event - Threat scenario – Threat analysis - Vulnerability analysis - Risk analysis - Safeguards.

   (2) 800-30: Threat source - Threat action - Threat statement – Threat identification – Vulnerability identification –- Risk determination - Controls.

d. The Canadian method is more asset and threat centric with an emphasis on the SoS as being an integral part of the TRA. The US counterpart is more vulnerability centric and offers little insight on confidentiality, integrity and availability and SoS. However, it suggests associating the asset criticality to the Business Impact Assessment (BIA). The concept of assets is introduced after the threat and vulnerability identification tasks;

e. Emphasis is put on the use of tools to help identifying vulnerabilities. Such tools are the use of self-assessment guide to develop security checklist (SP 800-26) (http://csrc.nist.gov/publications/nistpubs/index.html) and the NIST I-CAT Vulnerability database (http://icat.nist.gov/icat.cfm). The ITSG-04 offers a limited list of potential vulnerabilities as an annex.

f. ITSG-04 provides grouping of safeguards in accordance with their functions such as Safeguard functional categories: Correction / Detection / Deterrence / Prevention (Avoidance) / Containment / Recovery / Monitoring / Awareness. NIST 800-30 categorizes security area into Management Security / Operational Security / Technical Security and further categorized controls into a similar approach to the Canadian method: Management Security Controls: Preventive / Detection / Recovery; Operational Security Controls: Prevention / Detection; Technical Security Controls: Support / Prevention / Detection and Recovery;

g. The NIST approach offers a discussion on implementation plan and stresses the importance of a follow-up process to the TRA. A good example is provided as an annex. The lack of remedial plan is noticeable in the CSE approach.

h. The risk mitigation options for ITSG-04 are Transfer / Avoidance / Acceptance / Reduction. The 800-30 extents the choice to Assumption / Avoidance / Limitation / Planning / Research and Acknowledgement / Transference.

Both methodologies have associated guidance documents to explain the general concepts of risk management. They both offer very useful insights to the TRA components. A melding of the two methodologies would likely result in a more complete, useful and reusable TRA.

5 LINKING THE COMMON CRITERIA

As previously discussed in section 2, the GSP requires that TRA be conducted on Information Technology systems to identify security controls needed to mitigate risks to an acceptable level in the context of certification and accreditation decisions. Numerous TRA practitioners and departmental security officers agree that the TRA guidance does not provide detailed direction on how the results of the analysis could be used as input to other system assurance processes or provide for a consistent framework that would allow results of one TRA to be consistent, effectively reused, and traceable. The Common Criteria (CC), on the other hand, provides a formal framework for defining technical, procedural and policy security controls for a system. Within the Common Criteria framework, significant work has been accomplished to identify applicable safeguards and controls to meet a certain level of assurance. Therefore, it would be beneficial if such approaches can be related to the TRA methodology to help system owners in using the CC as part of their TRA findings. Such study was sponsored by CSE[20].

5.1 OVERVIEW - COMMON CRITERIA

The Common Criteria (CC) is a catalogue of criteria and a set of tools for construction of requirements. These requirements serve as a guide for the development of products with IT security features, for the procurement of products with IT security features and a basis for the evaluation of IT security products. The Common Criteria approach to security evaluation draws from the strengths of:

a. Trusted Computer System Evaluation Criteria (TCSEC) designed in 1983/85 by the United States;

b. Information Technology Security Evaluation Criteria (ITSEC) from UK, France, and Germany in 1991;

c. Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) produced by Canada in 1993; and

d. US Federal Criteria (FC) which was produced, in early 1993, by the United States with the assistance of Canada.

With the dawn of an international market, it was soon realized that there were unnecessary and expensive constraints on a vendor for recognition of a product certification to be recognized in other countries. Therefore, the three main schemes came together to create something more suitable, the Common Criteria with Mutual Recognition Agreement (MRA) signed in October 1998. The CC became an ISO standard 15408 in 1999.

[20] CSE - Threat and Risk Assessment Controls and Safeguards in Relation to The Common Criteria Report and Recommendations, Version 1.1, 27 March 2002, Conducted by: Cinnabar Networks Inc

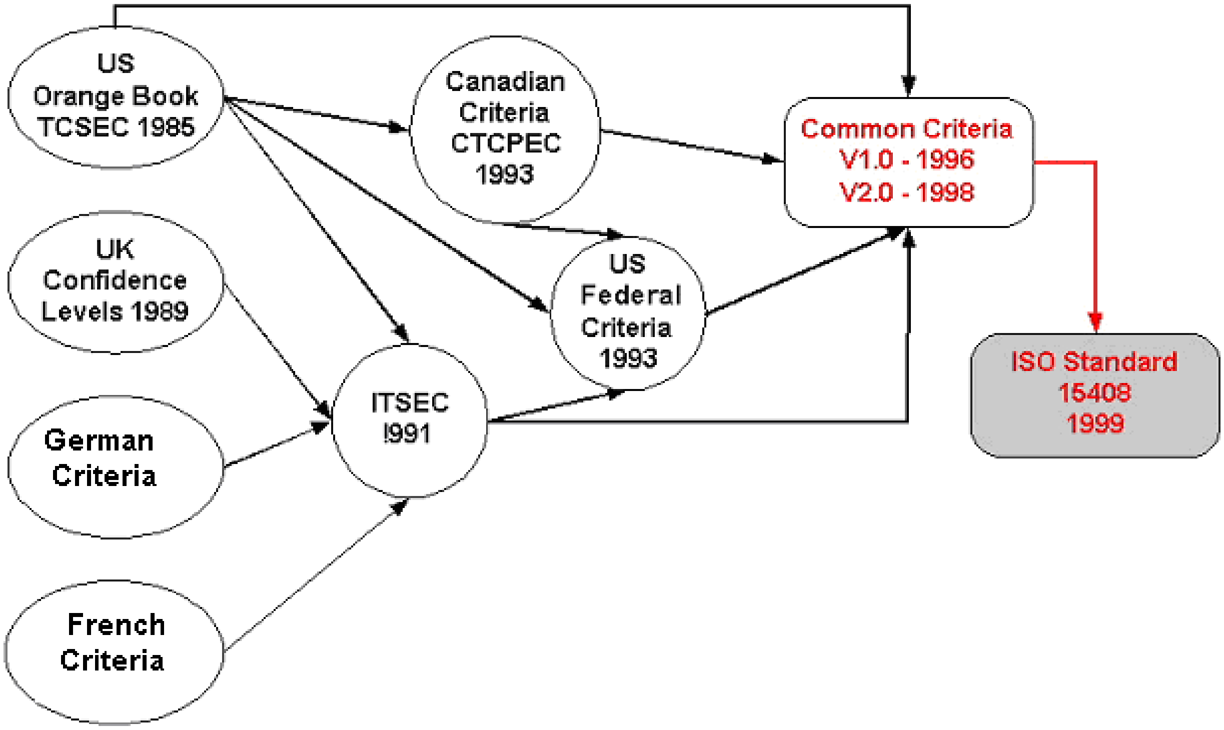
US Orange Book TCSEC 1985
UK Confidence Levels 1989
German Criteria
French Criteria
Canadian Criteria CTCPEC 1993
ITSEC I991
US Federal Criteria 1993
Common Criteria V1.0 - 1996 V2.0 - 1998
ISO Standard 15408 1999

Figure 4. Common Criteria Source Documents Development[21]

5.1.1 *ROLE OF SECURITY EVALUATION*

The CC is a cooperatively developed and widely adopted international Information Technology Security product evaluation standard. The CC contains a highly developed taxonomy of security functional requirements and features a hierarchical structure that organizes a broad range of security functionality. Developers and consumers can select a rational set of security functionality in products by expressing requirements from functionality classes, families and components that address specific needs in a policy-directed manner. Security management and audit requirements are included and form central components in deriving a compliant set of requirements.

The CC assurance model comprises seven assurance packages or evaluation assurance levels (EAL's). These assurance levels provide a graduated scale that appropriately grades the product's developmental process, documentation and testing. Use of these assurance levels provides an accepted security-engineering standard for developers and informs consumers on the level of trusted development that a product has undergone.

[21] Common Criteria and Protection Profiles: How to Evaluate Information Technology Security, by Kathryn Wallace, Practical Version 1.4b (© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights)

5.2 WHERE IS THE CORRELATION

There are many different approaches to the problem of deriving a risk analysis and a solution that mitigates the identified risks to an acceptable level. A common feature to virtually all these approaches is the collection of existing and new safeguards that effect this mitigation. Much of the work of the risk analyst in IT security is to identify the appropriate safeguards for a specific threat scenario. The collection of these controls provides a basis for the TRA recommendations, and in some methodologies, provides the basis for a separate document that identifies an action plan for implementation. Examples are the Statement of Applicability in ISO 17799 or the Safeguard Implementation Plan in NIST 800-30. If one could extend the TRA findings to include an assurance component, the resulting analysis would add a valuable criterion in the system owner risk acceptance phase.

5.3 SECURITY CONTEXT MODEL

The link between TRA and CC can make both the common criteria and the TRA methodology more dynamic rather than the current static fashion they are. The extension of the TRA to security assurance requirements is an important and often poorly rationalized step in the design and integration of secure architectures. The mapping of TRA findings to the CC assurance levels is a fundamentally distinct process that would delineate a requirement for a specific safeguard assurance level, or an overall assurance level for a system. The CC can relates to TRA in many aspects:

a. Structured terminology of controls;
b. Qualitative description of safeguards;
c. System architecture model;
d. Applicable threat model, including threat attributes (motivation, capability, opportunity … etc) and threat scenarios;
e. Taxonomy of relevant vulnerabilities;
f. Classification scheme / sensitivity analysis of information assets;
g. Impact analysis of information assets, with respect to confidentiality, integrity and availability scenarios, and possibly mode of access;
h. Risk derivation model, the functional relation between risk and any of the above parameters;
i. Risk mitigation model linking safeguards and controls to threat scenarios.

Risk acceptance of system operations is assessed based on CC evaluation results of security components of a system. This leading edge approach provides the missing assurance component to the TRA methodology. Further studies are required to influence future risk management practices.

6 RESEARCH INTO A COMMON FRAMEWORK

The traditional risk analysis framework is well established, although this is a field where considerable variation exists in terms of interpretation of the basic terms and the general process model as seen in the previous sections. In this section, the analysts attempt to present some of the standard ways in which risk analysis is conducted either using an automated tool or a manual methodological. These approaches use qualitative and / or quantitative descriptors. A short discussion is provided with observations, which set the ground rule for the common framework.

Since many of the commercial packages are proprietary, and not openly documented in terms of design, it is not possible to achieve anything near completeness in this goal. Even among the well-documented sources, access to automated designs is difficult to obtain. The best sources of documentation are invariably the standards that model manual procedures. The treatment provided here is based on experience in the Canadian governmental sphere, and tend to reflect the specific needs of that community.

6.1 QUANTITATIVE RATINGS

Qualitative versus quantitative rating values for TRA components was preliminary introduced in section 3. The following discussion relates to automated tools for risk management and why the difficult task of quantitative rating is so challenging.

Quantitative risk management involves the use of a mathematical model to manage risk. In particular, quantitative risk management uses precise mathematical terms to perform risk assessment. Thus the cumulative risk of a system is a mathematical function of a system risk model. A model of this type has components such as assets, threat agents, environmental threats, vulnerabilities, safeguards, and possibly other auxiliary components such as system states. Functional notion of likelihood, or similar concepts, is present in all these models. The relationships that exist between these components are mathematically defined and are used to determine derived functions such as initial risk and residual risk in a system.

The quantitative ratings allow the analyst to model the system to a desired degree of granularity and scope. In many cases, the mathematical model may incorporate underlying theories such as probability theory, bayesian statistics, fuzzy logic, decision theory, graph theory, tree theory, and conventional arithmetic and algebraic functions. Some quantitative tools are formally modeled and proven using formal methods tools (e.g., the Electronic Security Inspector (eSI) tool created by the German government). Many of these models are strictly intended for automated tool implementation, as attempted human calculation could lead to undetected error.

The validation of the generic risk model is usually left as a self-evident truth, or may be documented by the developer of the model. It is necessary for the user to understand the model, its terminology, semantics and the process of gathering relevant information and employing the tool. Quantitative risk management that uses probability or statistical approaches generally depends on some historical statistical information on the system. If these data cannot be supplied, an estimate must be made, based on qualitative or anecdotal data. This approach can in turn be a source of error.

It is clear that probabilistic models have a natural connection with the notion of risk through the interpretation of the likelihood function. There may also be related notions of causality employing Bayesian techniques. Thus a threat agent may have a probabilistic tendency (i.e., capability) to effect a certain attack scenario, or a safeguard may mitigate such an attack with a given probability. More complex scenarios can be modelled with conditional probabilities, decision trees, fuzzy distributions, causal nets or other mathematical structures.

6.1.1 QUANTIFICATION OF ASSETS

Quantification of asset value and impact analysis is an important function that is generally independent of probabilistic or statistical relationships. The measurement of impact can be qualified by fuzzy measures of loss scenarios or quantified by exact monetary measures of damage. Often the impact carried by a given asset varies by scenario. If an asset is disclosed in an unauthorized manner, the impact will be different than if its integrity is degraded or it is destroyed entirely. This characteristic may or may not be supported in the risk model.

6.1.1.1 WHAT CAN BE MEASURED

Perhaps the oldest theory of asset impact valuation is Annualized Loss Expectancy (ALE), which is based on the mean annual loss to an organization involving a certain asset, broken down by attacks of applicable types. This concept is a direct carry-over from the original definition of risk analysis developed in the insurance industry. The main innovation in the IT security application is the introduction of mitigating safeguards that are likewise assessed in terms of their cost and monetary benefit to the loss of specific assets. The greatest value of this analysis is in systems where a definite monetary loss can be placed on compromise of information assets.

If the system asset model is basically not measurable in terms of dollar figures, then usually some finite ordered set of impact values is substituted. There is, of course, no reason why impact could not be modelled as a partially ordered set or lattice, but this is rarely done. In the Canadian government context, impact is generally tied to asset valuations based on the Government of Canada Security Policy (GSP) and the sensitivity of the information being of national interest or not. Some attention has been given to mapping the GSP to a mathematical lattice model in the mid-1990's, but to date no official recognition has been given to these attempts. The main obstacle to consensus is the ordering relationship between the Top Secret, Secret and Protected C sensitivity levels, if any. Although not recognized, the attempt to map information sensitivity and the impact (injury test) resulted in the following diagram, which has been used in training sessions and conference[22]:

Top Secret	**Protected C**
Secret	
Confidential	**Protected B**
Restricted	**Protected A**
Unclassified / Undesignated	

Figure 5. Injury Test - Confidentiality

[22] The Metrics of Risk – Measuring and Managing Uncertainty, by John Clayton, Tutorial given at the 14th Annual Canadian Information technology Security Symposium 2002 sponsored by Communications Security Establishment.

6.1.1.2 PROBABILITY AND STATISTICS

Probability / Statistical models (and Fuzzy logic) also apply to threat analysis and vulnerability analysis. In most cases, the probabilistic weight is usually attached to the threat agent and a specific threat scenario, with capability, motivation and possibly opportunity measures. Vulnerability analysis can be a separate engineering study in itself, and is not often fully developed in a TRA methodology or tool. The Common Criteria has a detailed methodology for vulnerability analysis that goes somewhat beyond what is found in TRA tools. Both threat and vulnerability analysis are dynamic in the sense that over time the technology base accessible to a threat agent tends to add to their capability rating, and new vulnerabilities of a system are generally discovered and documented. Much of threat and vulnerability analysis has been more susceptible to expert system modelling than to a static mathematical structure.

6.1.2 QUANTITATIVE RATING - SUMMARY

The previous research and development projects have significantly advance the concept of quantitative ratings. One methodology that has emerged in the late 1990’s, and has featured the structure as opposed to expert system, is Schneier’s Attack Tree method. This method uses a tree structure to capture all the potential attack steps that terminate in the compromise of a specific asset or set of related assets. It can be performed in a graphical paper-and-pencil analysis, or could potentially be encapsulated in a tool. Earlier versions of this approach are the fault logic and hazard logic trees that appeared in the General Risk Assessment Model (GRAM) of the 1980’s, and other similar approaches.

From the 1980’s, when various fundamental tools such as CCTA Risk Analysis and Management Methodology (CRAMM), Livermore Risk Analysis Methodology (LRAM) and Aerospace Risk Evaluation System (ARiES) were developed on mathematical principles, there has been a gradual development in the mathematical modeling of risk. While a quantitative approach is favoured in many mathematical risk tools, there are often ways of softening the valuation of input elements so that probabilistic or fuzzy-valued measures are accepted.

In many cases, the purely quantitative methods and tools have presented challenges to users in terms of gathering the right kind of data. This negative aspect has created a market for streamlined and simple tools that provide a greater ease of use. A possible future application of the hard-core quantitative approach may be in the approach of the IRONMAN project at DND, which pushes data gathering onto the automated services of the network rather than onto the human analyst. In such a context, the mathematical risk models described above can carry through a precise and dependable risk analysis using mathematical theories, structures, knowledge bases and inference engines.

6.2 TWO APPROACHES

At the risk of overt generalization, there are two main approaches to the process of risk analysis in either the manual methodologies and automated tools. These will be referred to as the functional, and the relational approaches. This nomenclature is by no means standard, but will be useful in the present context to delineate the high level taxonomy of risk analysis process models.

6.2.1 THE FUNCTIONAL APPROACH

The functional approach describes the framework as a system of functions that have defined inputs and outputs. Inputs are either explicitly formatted data collected by the analyst from on-site interviews, observations and organizational documentation, or are the interim outputs of other functions in the framework. The functional approach therefore provides the analyst with a rigorous process model for obtaining well-defined results. An example of the functional approach is the natural evaluation of risk in the ALE model, where risk is the product of likelihood of a threat scenario and impact due to the assets compromised by the scenario. Thus likelihood and impact function outputs feed as inputs into the risk function. In an automated context, functional systems are likewise structured from a basic input model that generates interim and final results that match what a human analyst would have computed.

6.2.2 THE RELATIONAL APPROACH

The relational approach is more often found in automated tools that employ rule-based or other forms of automated reasoning. An example would be the EXess tool that employs the semantic net AI model to obtain results that are normally obtainable only by expert human cognition. In this approach, it is possible to employ non-functional relations that may naturally exist between elements of the analysis. Very often, security policy, threat agent behaviour, human resources or legal requirements of an organization can be more effectively modeled as a system of relational rules among risk model elements. Once mastered, this approach can closely model the cognitive process that an expert human analyst might employ in a manual analysis. Analytically, these systems are goal-based and often depend on sophisticated backtracking and unification techniques to achieve their results.

6.2.3 HYBRID ANALYSIS

Hybrid systems that employ aspects of both functional and relational analysis are possible and may exhibit the best of both worlds. Also, it is important to recall that each approach can, and does, include the other. A function is just a special type of relation, and any relation can be mathematically expressed as a characteristic function. So the difference between the approaches is more apparent than actual. The terms functional and relational are more useful to describe the philosophical approach of methodologies or automated tools than any canonical difference between them.

6.3 A FUNCTIONAL FRAMEWORK

The main components of functional risk analysis are often best described as components of a manual methodology, although there is no requirement for an automated tool to follow the human-based reasoning that is favoured in the methodologies. These components make up a framework of tasks that the analyst is obliged to complete and document. Very often, a rationale is provided by the analyst to support the conclusions of the assessment. This information is generally textual in nature, but may also be graphical. One example that has been used in some Canadian government departments is the application of specialized diagrams to document attack architectures. Automated tools, particularly those based on expert systems, may also provide a trace that records reasoning employed in the analysis. Vulnerability assessment tools and penetration testing provide great insight in the technical analysis of a system. These provide the reader with valuable documentation on the thought process that produced the conclusions of the analysis.

6.3.1 LIMITATIONS AND NEEDS

It is practically inconceivable to model an entire TRA process in an automated tool. The fact remains that no matter which methodology are being used, a TRA practitioner is required as subject matter expert, to segregate, validate and input the proper information, to draw conclusions, to recommend the appropriate course of actions, either technical, procedural or operational controls, and to merge all findings in a report addressed to Senior Management. Another shortcoming with TRA is the static nature of the process. The TRA is based upon a snapshot of the current representation and expectation of the system, which is inevitably going to change over time requiring continuous risk management effort. Likewise, the TRA report should be considered a living document, preferably under configuration management, and be updated as required to manage the risks as the system design evolves over its lifecycle. From these two limitations, it is important to realize which component(s) of a TRA can be automated and which one(s) likely will fail automation.

Like any good practice, the identification of the needs is a crucial success factor. Actually, understanding what is success for the system owner provides a much better insight to any assessment. In an attempt to derive a general functional framework, the following desirable inputs or needs / requirements can be mapped to the elements of a TRA:

a. Behaviour versus reactive approach;

b. Phase approach, predictive or dynamic security posture;

c. Assets, information or commodity;

d. Modelling of network enclave;

e. Knowledge base, more than just a database; and

f. Assurance.

A general functional framework for either manual or automated risk assessment would comprise the following elements and potential needs:

Table 3. Generic Functional Framework

Function	Description	Inputs	Outputs
Business Model	The organization business model is defined and understood	• Mission Statement • Interviews • Observations	• Business requirements
Corresponding Mapping of Needs: a, b, c			
System Architecture Analysis	System Architecture is analyzed and assessed as a basis for Asset location analysis and Vulnerability analysis	• Interviews • Documentation • Observations	• Architecture
Corresponding Mapping of Needs: a, b, c, d, e, f			
Asset Classification and Impact Analysis	Information assets are identified, described, classified by sensitivity	• Interviews • Documentation • Observations	• Statement of Sensitivity
Corresponding Mapping of Needs: c, d, e			

Function	Description	Inputs	Outputs
Threat Analysis	Threat agents are identified by class characteristics and behavioural analysis; Threat Scenarios are constructed using simple tabular or more complex, e.g., attack tree-based, Bayesian, or causal net-based representations.	• Interviews • Documentation • Observations • Architecture • Expert Knowledge	• Threat agents Table • Threat scenarios Table
Corresponding Mapping of Needs: b, d, e			
Vulnerability Analysis	System vulnerabilities are identified and assessed; relationship to threat scenarios identified using simple tabular or tree-based representations.	• Interviews • Documentation • Observations • Architecture • Expert Knowledge	• Vulnerability Table
Corresponding Mapping of Needs: a, d, e, f			
Safeguard Analysis	Existing safeguards are identified and assessed for strength; relationship to vulnerabilities identified	• Interviews • Documentation • Observations • Architecture • Vulnerability table • Expert Knowledge	• Initial Safeguard Tables
Corresponding Mapping of Needs: a, d, e, f			
Risk Assessment	Existing risk is assessed by threat scenario: associated vulnerabilities, safeguards and threat agent characteristics functionally determine an effective threat level that reflects current mitigation; Statement of Sensitivity and threat levels provide inputs of risk level determination.	• Statement of Sensitivity • Threat agents table • Threat scenarios table • Vulnerability table • Safeguard tables	• Initial Risk Assessment
Corresponding Mapping of Needs: d			
Additional Safeguard Recommendations	New Safeguards are identified and assessed for strength; relationship to vulnerabilities and threat scenarios identified, indicating effective risk mitigation rationale; strategic deployment of new safeguards indicated.	• Initial Safeguard tables • Architecture • Vulnerability table • Expert Knowledge	• Enhanced Safeguard tables
Corresponding Mapping of Needs: d, e, f			

Function	Description	Inputs	Outputs
Residual Risk Assessment	As in Risk Analysis above, but with the Enhanced Safeguard Tables, to show the effect of the mitigation strategy of adding new safeguards.	• Statement of Sensitivity • Threat agents table • Threat scenarios table • Vulnerability table • Enhanced Safeguard tables	• Residual Risk Assessment • Recommendations
Corresponding Mapping of Needs: a, b, c, d, e, f			

The initial phases of Business Model and System Architecture analysis are often not included in the scope of a threat risk assessment, but some work in this area is generally required as a foundation for the purely risk-oriented analysis that must follow. Likewise, security policy analysis is generally a component of risk management standards such as ISO 17799, but is omitted above. While the above table is strongly suggestive of a purely functional implementation, it is equally capable of being represented relationally and processed in a rule-based system that captures all or some of the expert knowledge components required. In a more sophisticated tool, the so-called 'tables' that are output by the analysis may indeed be more complex knowledge structures and report-generating mechanisms. Otherwise, the entire analysis can be performed, and often is, using simple spreadsheet and word processor tools.

6.4 ENRICHMENT OF THE FRAMEWORK

The strong points of the functional framework are its generality of application and methodical realization using simple tools. The relational approach is stronger in modeling risk in specialized knowledge domains and system ontology within the automated tool setting. Other specialized structures such as attack trees and fault analysis, can be inserted in either scheme.

The framework described above has at least two important defects:

a. It is a static present-value oriented representation of risk; and

b. It uses simplistic point estimators of what are essentially random variables.

To be a truly general framework, it would be desirable to generate output that dynamically forecasts future risk behaviour. Even if limited in scope, a time-functional as opposed to a static-valued output would be of greater value to decision makers. The dynamic model of risk takes into account the time value of threat agent technology and projects near-future risk analyses based on the dynamic nature of threat and safeguard technologies.

The dependency on crisp point estimation of impact, threat and vulnerability levels and risk precludes the use of advanced statistical or fuzzy modeling of the system. A great deal of research and application of these techniques has shown that a higher quality of reasoning can be carried out when the representation of knowledge includes with it the degree of accuracy it represents. All of this is lost when one collapses essentially uncertain, opinionated or blended data into simplistic point representations.

Fortunately, the above criticisms of the framework can be remedied without affecting the general structure. It is possible to manipulate functional or fuzzy representations in the same way that one reasons with numerical values. The only functions that change are the low-level functions that calculate arithmetic point estimate values. These are converted to handlers of ambiguity structures such as distributions or fuzzy sets. Final “de-fuzzification” is performed in the output or reporting functions.

The framework above provides a foundation that incorporates correct reasoning with ambiguous information inputs and dynamic modeling of risk. The use of variant modeling representations such as causal nets, fault- or attack- trees, or Bayesian net representations create the potential for finer automated analysis. It should always be general enough so that simple functional and relational structures are also supported in situations where uncertainty or cost constraints preclude a detailed analysis.

7 CONCLUSION AND RECOMMENDATIONS

This section presents conclusions and recommendations that have been derived from the study of the Canadian risk management, the goal to a common framework as part of the NATO Working Group vision and the options for automation of TRA methodology.

7.1 OBSERVATIONS AND CONCLUSIONS

The following conclusions were drawn from the analysis of the risk management posture in the context of the NATO common framework:

a. Most system and information owners realized the importance of risk management and the fact that a TRA is the driving force for many life cycle phases of a system;

b. The requirement for TRAs in evident in other risk management activities such as Certification and Accreditation, Privacy Impact Assessment, self-assessment, IT security audit, and departmental accountability;

c. Substantial evolution of risk management has occurred in the past few years, but the tools and documentation have been a significant impediment on further development;

d. The methodologies available today are lacking uniformity, consistency, traceability, and reusability;

e. Common language between methodologies is lacking, a limitation in the development of a common framework;

f. Most tool automation initiatives were premature and did not adjust well to scope and depth of knowledge. A significant shortcoming with TRA is the static nature of the process;

g. Regardless of the methodology being used, automated or not, a TRA practitioner is required as a subject matter expert to segregate, validate and input the proper information; and

h. Canada is currently involved in numerous IT risk management projects to meet the evolving policies. The Canadian expertise is growing and becoming more specialized. Some initiatives are unique and innovative.

7.2 RECOMMENDATIONS

The following recommendations should be considered in providing the NATO Working Group with a Canadian perspective and contribution to a common risk management framework:

a. The Common Criteria terminology provides a shared set of concepts and vocabulary that can only help unify the disparate terminologies that variant TRA approaches and methodologies have engendered. Further research should be conducted to link the CC to TRA methodologies;

b. Automation is possible, it was premature in the early days when risk management was introduced, but practitioners have gained expertise and experience in the conduct of TRA. The functional approach provides the rational behind the vision. Requirements should be gathered and resources commitment strongly encouraged;

c. Partial automation may be an initial step toward common framework. It is recognized that human intervention will most likely be required in any automated TRA. The concept of grouping or profiling common TRA elements such as critical assets may indeed allow automation of the statement of sensitivity. Canada should pursue this unique initiative and leverage the work initiated by the leading agencies and policy authority;

d. NATO Working Group should develop common “standard” asset profiles, sensitivity ratings, and limited injury test for ultimately automate the SoS;

e. A number of departments have practiced the concept of baseline security. There is an opportunity for the NATO Working Group to promote the model of enterprise wide statement of sensitivity and enterprise wide threat and risk assessment. This approach allows for improved risk management and ease of understanding and acceptance by the risk owners;

f. Canada should pursue the work on a national threat database and vulnerability database. Further initiatives should be encouraged such as linking the data based on dependencies (identification of safeguards that are required to ensure adequate control); relationships (Identification of safeguards that may be complementary but not necessary) and related vulnerabilities; and

g. Further considerations should be given to future work (section 8) to promote the Canadian vision in risk management as a contribution to the NATO Working Group.

8 FUTURE WORK

Given current shortcomings with the risk management process, namely it's increasing out datedness due to system changes and the passage of time, and the expense of redoing book ended TRAs to update security baselines, future research should be directed towards the development of more maintainable, dynamic, and automated risk management processes. These revised processes will obviously commence with a conventional TRA but will model those results to form the baseline for a dynamic risk management system. This approach will ensure that what is defined in the initial TRA can be maintained throughout the risk management lifecycle thereby reducing cost while increasing length of validity. The following sections outline areas of future work that DRDC may be interested in pursuing that advance the nature and usefulness of the risk management process.

8.1 TRA AND RISK MANAGEMENT PROCESSES

There is a requirement for research into existing risk management processes in terms of their shortcomings. Areas of study could include:

a. Threat, Risk, and Vulnerability in the presence of evolving Local Area Networks;

b. The effects of change over time on established TRAs;

c. The Risk Management Process and the associated Vulnerability Assessment and how a more unified approach can be created to model the security posture of a network or system; and

d. A detailed examination of how to better interleave the actual risk management process into various system lifecycle processes currently in use within industry and government.

8.2 RISK MANAGEMENT DYNAMISM

There is a requirement for research into how the risk management process can be more dynamic. Areas of study could include:

a. An examination of how a Dynamic Risk Management Process can evolve from and fit into the current Risk Management Process;

b. A determination of how a dynamic risk management system will look and how it will be utilized to adequately define the security posture of a network or system; and

c. A determination of what elements of a system or network are dynamic by nature and how those elements can be automated to provide input to a dynamic model.

8.3 BASELINE MODELS

In order to evolve the existing risk management processes an investigation into necessary baseline models consistent with and outgrowths of the TRA process are necessary:

a. Determine how and what is necessary in the creation of an automated model of the security posture of a network or system;

b. Determine the feasibility of developing a revised Dynamic Risk Management process that can define an ongoing, computed security posture; and

c. Determine what constitutes an acceptable baseline and how that baseline will be used within any newly evolved risk management process.

8.4 FEASIBLE AUTOMATION

In order to utilize any new risk framework or automated risk management process, it is necessary to determine how much of a framework can be automated and in what form that automation will take. There is naturally a requirement then to determine how much of an automated framework can be delivered using existing technology and how well it will perform.

In order to effectively automate the existing risk management processes an investigation into necessary baseline models consistent with and outgrowths of the TRA process are necessary.

a. Determine how and what is necessary in the creation of an automated model of the security posture of a network or system; and
b. Determine the feasibility of developing a revised Dynamic Risk Management process that can define an ongoing, computed security posture.

Annex A. Information Resources

The following chart provides an overview of the key individuals who were directly involved in providing input to this project.

Information Gathering Resources - Interviews	
Name	**Title / Area of Responsibility**
Jacques Gélinas	Defence Research and Development Canada Defence Scientist, Network Information Operations Section
John Clayton	Communications Security Establishment Senior Information Technology
Alain Sylvestre	Communications Security Establishment Senior Information Technology
Hugh Gillis	Treasury Board of Canada, Secretariat Senior Policy Analyst - Security Policy
Linda Hunter	Treasury Board of Canada, Secretariat Coordinator - Architecture, Standards and Engineering

The following documents were used as input to this study.

Information Gathering Resources - Documents	
Policies / Standards / Guidelines	
1.	French TRA Methodology, EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), published by Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI), version 1.02, February 1997. www.ssi.gouv.fr/fr/confiance/ebios.html
2.	United Kingdom TRA Methodology, CRAMM. http://www.cramm.com
3.	Canada TRA Methodology, ITSG-04 - Threat and Risk Assessment Working Guide, October 1999 http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg1_e.asp#eff
4.	Treasury Board of Canada Secretariat, Government Security Policy, February 2002. http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg1_e.asp#eff
5.	MG2 - Risk Management Framework for Information Technology (IT), 1996 http://www.cse-cst.gc.ca/en/knowledge_centre/gov_publications/itsg/itsg.html

Information Gathering Resources - Documents	
6.	MG3 - A Guide to Risk Assessment and Safeguard Selection for Information Technology Systems, January 1996
7.	MG4 - A Guide to Certification and Accreditation for Information Technology Systems, January 1996
8.	Royal Canadian Mounted Police, Security Information Publication - Guide to Threat and Risk Assessment For Information Technology, November 1994 http://www.rcmp-grc.gc.ca/tsb/pubs/it_sec
9.	Royal Canadian Mounted Police, Guide to Threat and Risk Assessment Involving On-Site Physical Security Examination, published in 2002 http://www.rcmp-grc.gc.ca/tsb/pubs/phys_sec
10.	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, January 2004 Version 2.2, Revision 256 CCIMB-2004-01-001 www.commoncriteriaportal.org
11.	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, August 1999, Version 2.1, CCIMB-99-032
12.	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, August 1999, Version 2.1, CCIMB-99-033
13.	Operational Standard for the Security of Information Act (SOIA), last modified March 17, 2003 http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/siglist_e.asp
14.	Operational Security Standard - Business Continuity Planning (BCP) Program, last modified March, 23, 2004
15.	Operational Security Standard: Management of Information Technology Security (MITS), last modified May 31, 2004
16.	Operational Security Standard - Readiness Levels for Federal Government Facilities, last modified January 11, 2002
17.	Personnel Security Standard - 2-04, last modified October 17, 2002
18.	Physical Security Standard - 2-02, November 15, 1994
19.	Security and Contracting Management Standard - 2-05, last modified June 9, 1996
20.	Security Organization and Administration Standard - 2-01, last modified June 1, 1995
21.	CIS/01/6, IT Systems Security Architecture Handbook
22.	A-IM-100-000/AG-001, Guideline for Certification and Accreditation of Information Systems, Revision 3, Version 1, 30 June 2000
23.	Canada Customs Agency, IT Security Evaluation Guide (SOS / TRA) and associated TRA template.
24.	RCMP Technical Security Standard for Information Technology, (TSSIT), August 1997
25.	ITS Self Assessment Methodology, (a TBS initiative in pilot phase)
26.	Technical Security Standards for Information Technology (TSSIT), RCMP, 1997
27.	Canada's National Security Policy Securing an Open Society, April 2004, produced by Public Safety and Emergency Preparedness Canada http://www.psepc-sppcc.gc.ca/national_security/publications_e.asp

Information Gathering Resources - Documents	
28.	Public Sector Security Classification Guideline, September 2004, Prepared for the Public Sector CIO Council by the National CIO Council Subcommittee for Information Protection (NCSIP)
29.	International Standard ISO 17799, Information Technology - Code of Practice for Information Security Management, First edition 2000-12-01
30.	NIST SP800-30 - Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology, July 2002
31.	NIST SP800-37 - Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004
32.	NIST SP800-60 - Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004
References	
33.	NATO AC/323 Information Systems Technology Panel, Task Group on Improving Common Security Risk Analysis, (IST-049/RTG-021), Terms of Reference
34.	DRDC Web site: http://www.drdc-rddc.dnd.ca
35.	Attachment 2, RTG021 Action List, April 2004
36.	Introduction to Information Technology Security, Course Number: CSE-300 Version Oct 01, Communications Security Establishment.
37.	Bonyun, D. A., “A proposal concerning a new approach to the problem of risk analysis methodologies DRAFT”, TTCP XTP1 Workshop on Next Generation Security Risk Management, Wellington, New Zealand, November 14 – 17, 1995, pp. 26 – 31
38.	Bonyun, D. A., & Jones, G., “An expert systems approach to the modelling of risks in dynamic environments”, Proceedings, Computer Security Risk Management Model Builders Workshop, Denver, Colorado, May 24-26 1988, pp.203 - 223
39.	Bonyun, D. A., & Kerr, S. W., EXESS an extensible expert system shell, User Manual. March, 1991
40.	Guarro, S. B., “Analytical and decision models of the Livermore Risk Analysis Methodology”, Proceedings, Computer Security Risk Management Model Builders Workshop, Denver, Colorado, May 24-26 1988, pp.49 - 71
41.	Mosleh, A., “A matrix/bayesian approach to risk management of information systems”, Proceedings, Computer Security Risk Management Model Builders Workshop, Denver, Colorado, May 24-26 1988, pp.103 - 116
42.	RiskWatch Inc. “RiskWatch Information systems and ISO 17799”, RiskWatch white paper www.riskwatch.com
43.	Sandberg-Maitland, W., “TENSAR semantics and ontology”, Communications Security Establishment, research report. March 31 1995.
44.	TruSecure Inc., RiskCommander 2.0 http://www.trusecure.com/solutions/products/risk_commander.shtml
45.	Report on the Feasibility of Developing a Threat and Risk Assessment Template for Treasury Board Secretariat, Cinnabar Document Number TBS-4-017, Client File Number 24052-6004286, Version Number Version 1.0, 15 October 2004
46.	CSE ITS Program Key Messages: Threat & Vulnerability Analysis System (TVAS) Release 0.

Information Gathering Resources - Documents	
47.	CSE - A Guide to Active Network Security Testing Within the Government of Canada, Version 1.3, 27 January 2003.
48.	CSE and Canadian Forces Information Operations Group – A Client Guide for Active Network Security Testing, Version 1.0, 29 January 2003
49.	CSE - Threat and Risk Assessment Controls and Safeguards in Relation to The Common Criteria Report and Recommendations, Version 1.1, 27 March 2002, Conducted by: Cinnabar Networks Inc.
50.	Cinnabar Vulnerability methodology for Province of Ontario
51.	CORPORATE SECURITY, Information Classification Policy, Version 0.9, September 2003, developed by Cinnabar Networks Inc.
52.	The Metrics of Risk – Measuring and Managing Uncertainty by John Clayton, Communication Security Establishment, Tutorials 2002, 14th Annual Canadian Information Technology Security Symposium.

Annex B. Glossary of Terms

This glossary of terms was produced using Information Technology Security Standards well known by Canadian risk management practitioners. Some terms have more than one definition to demonstrate to the reader to difference in the language from one methodology to another. This fact is crucial if a common approach to risk management is envisioned, (common language, business language, structured terminology, taxonomy).

Term	Definition	Source
Acceptable Risk	A concern that is acceptable to responsible management, due to the cost and magnitude of implementing security controls	NIST SP800-37
Acceptable Risk	A judicious and carefully considered assessment by the appropriate Designated Approving Authority (DAA) that an information technology (IT) activity or network meets the minimum requirements of applicable security directives. The assessment should take into account the value of IT assets; threats and vulnerabilities; countermeasures and their efficiency in compensating for vulnerabilities; and operational requirements.	CSE ITSG-04
Accountability	Property that allows the ability to identify, verify, and trace system entities as well as changes in their status. Accountability is considered to include authenticity and non-repudiation.	NIST SP800-37
Accountability	The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This support non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.	NIST SP800-30
Accountability	The property that ensures that the actions of an entity may be traced uniquely to that entity. (Based on ISO 7498-2)	CSE ITSG-04
Accreditation	The authorization of an IT system to process, store, or transmit information, granted by a management official. Accreditation, which is required under OMB Circular A-130, is based on an assessment of the management, operational, and technical controls associated with an IT system.	NIST SP800-37
Accreditation	Formal declaration by the responsible management authority 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.	CSE ITSG-04
Accreditation	The official authorization by management for the operation of an IT system, and acceptance by that management of the associated residual risk. Accreditation is based on the certification process as well as other management considerations	GSP

Term	Definition	Source
Asset	A component or part of the total system or network 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, services and organizational image.	CSE ITSG-04
Asset	Information or resources to be protected by the countermeasures of a Target Of Evaluation (TOE).	Common Criteria
Asset	Tangible or intangible things of the Government of Canada. Assets include but are not limited to information in all forms and media, networks, systems, materiel, real property, financial resources, employee trust, public confidence and international reputation. (The inclusion of information in this definition is for the purposes of this policy only and should not be interpreted as importing any legal consequences applicable for assets to information.)	GSP
Asset Value	A measure of asset worth in terms of replacement cost, confidentiality, integrity and availability.	CSE ITSG-04
Assets, Classified	Assets whose unauthorized disclosure would reasonably be expected to cause injury to the national interest.	GSP
Asset, Critical	Assets supporting a critical service.	GSP
Asset, Intangible	The attitude, value or perception impacting the organization, e.g., public confidence, goodwill, competitive advantage, morale, ethics, productivity or loyalty.	CSE ITSG-04
Asset, Protected	Assets whose unauthorized disclosure would reasonably be expected to cause injury to a non-national interest.	GSP
Assurance	Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. “Adequately met” includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or bypass.	NIST SP800-30
Assurance	The degree of confidence that the implemented security functions of an IT system or product adequately enforce the system security policy. Alternatively, the degree of confidence that the implemented system meets its stated security requirements.	CSE ITSG-04
Assurance	Ground for confidence that an entity meets its security objectives.	Common Criteria

Term	Definition	Source
Attack	The act of aggressively trying to bypass security controls on an IT system or network. The fact that the attack is made does not mean it will succeed. The success depends on the vulnerability of the system, network or activity and the effectiveness of the safeguards in place.	CSE ITSG-04
Attack potential	The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.	Common Criteria
Audit	The process of conducting an independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.	CSE ITSG-04
Audit, Security	An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established security policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, security policy and procedures.	CSE ITSG-04
Availability	Assurance that information, services, and IT system resources are accessible to authorized users and/or system-related processes on a timely and reliable basis and are protected from denial of service.	NIST SP800-37
Availability	The security goal that generates the requirement for protection against – intentional or accidental attempts to perform unauthorized deletion of data or otherwise cause a denial of service or data, and/ or unauthorized use of system resources.	NIST SP800-30
Availability	The accessibility of systems, programs, services and information to authorized users when needed and without undue delay.	CSE ITSG-04
Availability	The condition of being usable on demand to support operations, programs and services.	GSP
Certification	The comprehensive evaluation of the technical and non-technical security controls of an IT system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.	NIST SP800-37
Certification	A comprehensive evaluation of the technical and non-technical security features of an IT system and other related safeguards to establish the extent to which a particular design and implementation meets a specific set of security requirements, made in support of the accreditation process.	GSP

Term	Definition	Source
Classified information	Information related to the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act, and the compromise of which would reasonably be expected to cause injury to the national interest.	GSP
Confidentiality	Assurance that information in an IT system is not disclosed to unauthorized persons, processes or devices.	NIST SP800-37
Confidentiality	The security goal that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and in transit.	NIST SP800-30
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. (ISO 7498-2)	CSE ITSG-04
Confidentiality	The attribute that information must not be disclosed to unauthorized individuals, because of the resulting injury to national or other interests, with reference to specific provisions of the Access to Information Act and the Privacy Act	GSP
Confidentiality	The sensitivity of information or assets to unauthorized disclosure, recorded as classification or designation, each of which implies a degree of injury should unauthorized disclosure occur.	RCMP Appendix A
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. Synonymous with Impact and Injury	CSE ITSG-04
Controls, Management	Controls that address the security management aspect of security and IT security, and the management of risk for the department and IT environment. Examples: Threat and Risk Assessment, Privacy Impact Assessment, IT security governance structure. "Subject matter areas" in this "control category" are: General IT Security; IT Operations; Physical and Personnel Security; Contracts; Business Area; and Other.	ITSSAP
Controls, Operational	Controls that address the security mechanisms primarily implemented and executed by people (as opposed to systems). Examples: Emergency and Business/system Continuity Plans (BCP) and procedures, Physical security, Logs review, Backups. "Subject matter areas" in this "control category" are: General IT Security; IT Operations; Physical and Personnel Security; Contracts; Business Area; and Other.	ITSSAP
Controls, Personnel	Controls that address the human element of using system. Examples: Security screening, security training, Acceptable Use policies. "Subject matter areas" in this "control category" are: General IT Security; IT Operations; Physical and Personnel Security; Contracts; Business Area; and Other.	ITSSAP

Term	Definition	Source
Controls, Technical	Controls that address security mechanisms contained in and executed by hardware or software. Examples: Alarms systems, Intrusion detection, Anti-virus protection, Logical access controls. "Subject matter areas" in this "control category" are: General IT Security; IT Operations; Physical and Personnel Security; Contracts; Business Area; and Other.	ITSSAP
Criticality/sensitivity	A measure of the importance and nature of the information processed, stored, and transmitted by the IT system to the organization's mission and day-to-day operations.	NIST SP800-37
Exposure	A measure of the potential risk to an IT system from both external and internal threats.	NIST SP800-37
Exposure	The state of being vulnerable to criticism or attack.	RCMP Appendix A
Impact	A measure of the degree of damage or other change caused by a threat event. See Consequence	CSE ITSG-04
Information, Personal	Any form of recorded information about an identifiable individual. See Section 3 of the Privacy Act for examples. The Act also includes some exceptions to the definition. Personal information, a subset of other sensitive information, deserves enhanced protection and may carry the marking "PROTECTED personal information".	CSE ITSG-04
Injury	See Consequence	CSE ITSG-04
Integrity	Assurance that information in an IT system is protected from unauthorized, unanticipated, or unintentional modification or destruction. System integrity also addresses the quality of an IT system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data.	NIST SP800-37
Integrity	The security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has it has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).	NIST SP800-30
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	NIST SP 800- 60
Integrity	The property that data is being handled as intended and has not been exposed to accidental or intentional modification or destruction.	CSE ITSG-04
Integrity	The accuracy and completeness of assets, and the authenticity of transactions	GSP

Term	Definition	Source
Integrity	The accuracy and completeness of information and assets and the authenticity of transactions.	RCMP Appendix A
Levels of Concern	An expression of the criticality/sensitivity of an IT system in the areas of confidentiality, integrity, availability, and exposure, expressed qualitatively as high, moderate or low. The level of concern indicates the extent to which security controls must be applied to an IT system based on risk, threat, vulnerability, system interconnectivity considerations, and information assurance needs.	NIST SP800-37
Likelihood	The probability of a given event occurring.	CSE ITSG-04
Likelihood	The state or quality of being probable, probability.	RCMP Appendix A
Non-repudiation	Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.	NIST SP800-37
Privacy	The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. Note: Because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security. (ISO 7498-2)	CSE ITSG-04
Reliability	The property of an IT system to maintain consistent, intended and trustworthy operation over a given period of time.	CSE ITSG-04
Replacement Cost	The actual expenditure required to replace the asset(s). Some of the elements that contribute to the overall costs are, time to operation, direct purchase costs, installation and training costs. See Value.	CSE ITSG-04
Residual Risk	Portion of risk remaining after security controls have been applied.	NIST SP800-37
Residual Risk	The risk that remains after risk treatment.	ISO 17799
Residual Risk	The risk that remains after safeguards have been selected and implemented.	CSE ITSG-04
Residual Risk, Target	The risk to the system which can be accepted and managed by the system operational authority. Based upon risks identified by the risk assessment, it categorizes risks as those which can be accepted as manageable by the system operational authority, and those risks which must be reduced in order to be accepted. In the latter case the level to which risk must be reduced is identified.	CSE ITSG-04

Term	Definition	Source
Risk	The net mission impact considering: (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular IT system vulnerability and (2) the resulting impact if this should occur. IT system-related risks arise from legal liability or mission loss due to: (1) unauthorized (malicious or accidental) disclosure, modification, or destruction of information, (2) unintentional errors and omissions, (3) IT disruptions due to natural or man-made disasters, and (4) failure to exercise due care and diligence in the implementation and operation of the IT system.	NIST SP800-37
Risk	A combination of: (i) the likelihood that a particular vulnerability in an agency information system will be either intentionally or unintentionally exploited by a particular threat resulting in a loss of confidentiality, integrity, or availability, and (ii) the potential impact or magnitude of harm that a loss of confidentiality, integrity, or availability will have on agency operations (including mission, functions, and public confidence in the agency), an agency's assets, or individuals (including privacy) should there be a threat exploitation of information system vulnerabilities.	NIST SP800-60
Risk	The net mission impact considering (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and (2) the resulting impact if this should occur. IT-related risks arise from legal liability or mission loss due to: a. Unauthorized (malicious or accidental) disclosure, modification or destruction on information; b. B. Unintentional errors and omissions c. 3. IT disruptions due to natural or man-made disasters d. 4. Failure to exercise due care and diligence in the implementation and operation of the IT system.	NIST SP800-30
Risk	The combination of the probability of an event and its consequence.	ISO 17799
Risk	Intuitively, the adverse effects that can result if a vulnerability is exploited or if a threat is actualized. In some contexts, a risk is a measure of the likelihood of adverse effects or the product of the likelihood and the quantified consequences.	CSE ITSG-04
Risk	The chance of a vulnerability being exploited	GSP
Risk, High	Requiring immediate attention and safeguard implementation.	RCMP p23
Risk, Low	Requiring some attention and consideration for safeguard implementation as good business practice.	RCMP p23
Risk, Medium	Requiring attention and safeguard implementation in the near future.	RCMP p23

Term	Definition	Source
Risk Acceptance	An action taken by the responsible manager to declare and be held accountable for acceptance of the remaining or residual risks attributed to an IT system after the performance of a threat and risk assessment. Generally, the acceptance of the residual risk is made because any further addition of safeguards does not justify the effort in terms of cost or functionality.	CSE ITSG-04
Risk Analysis	The systematic approach of estimating the magnitude of risks.	ISO 17799
Risk Assessment	The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of risk management and synonymous with risk analysis.	NIST SP800-37
Risk Assessment	The process of identifying the risk to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of risk management and synonymous with risk analysis.	NIST SP800-30
Risk Assessment	The assessment of threats to, vulnerabilities of and impacts on information and information processing facilities and the likelihood of their occurrence. Risk assessment is overall process of risk identification, risk analysis and risk evaluation.	ISO 17799
Risk Assessment	An evaluation of risk based on threat assessment information, the effectiveness of existing and proposed security safeguards, the likelihood of system vulnerabilities being exploited and the consequences of the associated compromise to system assets.	CSE ITSG-04
Risk Assessment	An evaluation of the chance of vulnerabilities being exploited, based on the effectiveness of existing or proposed safeguards.	RCMP Appendix A
Risk Evaluation	The process of comparing the estimated risk against risk criteria to determine the significance of the risk.	ISO 17799
Risk Identification	The process of identifying risks considering business objectives, threats and vulnerabilities.	ISO 17799
Risk Management	A family of security controls in the management class dealing with the process of identifying and applying controls commensurate with the value of the assets protected based on a risk assessment. The total process of identifying, controlling, and mitigating IT system-related risks. It includes risk assessment; cost benefit analysis; and the selection, implementation, test and security evaluation of security controls. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws.	NIST SP800-37

Term	Definition	Source
Risk Management	The total process of identifying, controlling, and mitigating information system – related risks. It includes risk assessment, cost benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws.	NIST SP800-30
Risk Management	Coordinated activities to direct and control an organization with regard to risk. NOTE: Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication (exchange or sharing of information about risk between the decision-maker and other stakeholders).	ISO 17799
Risk Management	The process by which resources are planned, organized, directed, and controlled to ensure the risk of operating a system remains within acceptable bounds at optimal cost.	CSE ITSG-04
Risk Management	A systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk issues.	MITS
Safeguards	The approved minimum security measure(s) and controls which, when correctly employed, will prevent or reduce the risk of exploitation of specific vulnerability(ies) which would compromise an IT system.	CSE ITSG-04
Safeguards	Actions or measures taken to offset a particular security concern or threat.	RCMP Appendix A
Scenario Analysis	An IT system vulnerability assessment technique in which various possible attack methods are identified and the existing safeguards are examined in light of their ability to counter such attack methods.	CSE ITSG-04
Security Controls	Management, operational, and technical measures prescribed for an IT system which, taken together, satisfy the specified security requirements and protect the confidentiality, integrity, and availability of the system and its information. Security controls can be selected from a variety of families including risk management, system development and acquisition, configuration management, system interconnection, personnel security, media protection, physical and environmental protection, contingency planning, incident response capability, hardware and system software maintenance, system and data integrity, security awareness, training, and education, documentation, identification and authentication, logical access, audit, and communications.	NIST SP800-37
Security Goals	The five security goals are integrity, availability, confidentiality, accountability, and assurance.	NIST SP800-30
Security Requirements Baseline	A description of minimum-security requirements necessary for an IT system to maintain an acceptable level of security.	CSE ITSG-04

Term	Definition	Source
Sensitivity	Used in this guideline to mean a measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.	NIST SP800-60
Sensitivity	The characteristic of a resource which implies its value or importance to an organization, or the injury or harm that could result from its deliberate or inadvertent disclosure, modification, loss or denial.	CSE ITSG-04
Severity	A measure of the degree of damage suffered as the result of an event. May be expressed as a percentage of the impacted assets or as a time interval.	CSE ITSG-04
Statement of Sensitivity (SoS)	A description of the confidentiality, integrity and/or availability requirements associated with the information or assets stored or processed in or transmitted by an IT system.	CSE ITSG-04
Target	The objective of a hostile threat agent.	CSE ITSG-04
Threat	The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability; or Any circumstance or even with the potential to harm an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.	NIST SP800-37
Threat	The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.	NIST SP800-30
Threat	Any circumstance or event with the potential to intentionally or unintentionally exploit a specific vulnerability in an information system resulting in a loss of confidentiality, integrity, or availability.	NIST SP 800-60
Threat	A potential cause of an unwanted incident, which may result in harm to a system or organization.	ISO 17799
Threat	Any potential event or act that could cause one or more of the following to occur: unauthorized disclosure, destruction, removal, modification or interruption of sensitive or critical information, assets or services. A threat can be natural, deliberate or accidental.	CSE ITSG-04
Threat	Any potential event or act, deliberate or accidental, that could cause injury to employees or assets	GSP
Threat	Any potential event or act that could cause one or more of the following to occur: unauthorized disclosure, destruction, removal, modification or interruption of sensitive information, assets or services, or injury to people. A threat may be deliberate or accidental.	RCMP Appendix A
Threat Agent	An entity that may act to cause a threat event to occur by exploiting the vulnerability(ies) in an IT system.	CSE ITSG-04
Threat Analysis	The examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.	NIST SP800-30

Term	Definition	Source
Threat Analysis	The examination of all actions and events for determining the areas of vulnerability and the result of countermeasures to counteract perceived threats to assets that might adversely effect an IT system.	CSE ITSG-04
Threat and Risk Assessment (TRA)	A process in which the objective is to identify system assets, to identify how these assets can be compromised by threat agents, to assess the level of risk that the threat agents pose to the assets and recommend the necessary safeguards in order to mitigate effects of the threat agents.	CSE ITSG-04
Threat Assessment	An evaluation of threat agent characteristics including resources, motivation, intent, capability, opportunity, likelihood and consequence of acts that could place sensitive information and assets at risk.	CSE ITSG-04
Threat Assessment	An evaluation of the nature, likelihood and consequence of acts or events that could place sensitive information and assets as risk.	RCMP Appendix A
Threat Capability	The ability of a threat agent to act, or to be effective.	CSE ITSG-04
Threat Consequence	The adverse outcome or effect of a threat event on an asset.	CSE ITSG-04
Threat Event	An event whose occurrence would cause harm to an IT system in the form of disclosure, modification of data, destruction and/or denial of service. See Threat Scenario	CSE ITSG-04
Threat Source	Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability.	NIST SP800-37 and 30
Threat Scenario	A postulated set of circumstances in which a specific threat agent can mount a specific type of attack in an attempt to compromise (in one or more ways) one or more system assets.	CSE ITSG-04
Value	A measure or statement of the utility (usefulness) 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. See Replacement Cost.	CSE ITSG-04
Vulnerability	A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the systems security policy.	NIST SP800-37 and 30

Term	Definition	Source
Vulnerability	A flaw or weakness in the design or implementation of an information system (including security procedures and security controls associated with the system) that could be intentionally or unintentionally exploited to adversely affect an agency's operations (including missions, functions, and public confidence in the agency), an agency's assets, or individuals (including privacy) through a loss of confidentiality, integrity, or availability.	NIST SP800-60
Vulnerability	A weakness of an asset or group of assets which can be exploited by a threat.	ISO 17799
Vulnerability	A quantifiable, threat-independent characteristic or attribute of any asset within a system boundary or environment in which it operates and which increases the probability of a threat event occurring and causing harm in terms of confidentiality, availability and/or integrity, or increases the severity of the effects of a threat event if it occurs.	CSE ITSG-04
Vulnerability	An inadequacy related to security that could permit a threat to cause injury.	GSP
Vulnerability Assessment	An evaluation of the vulnerabilities of an IT component, program or system to determine if the controls in place or the proposed controls are sufficient to address security issues that could impact the confidentiality, integrity, or availability of the component(s) , program(s) or system(s) assets.	CSE ITSG-04
Vulnerability Assessment	A determination of the existence of system vulnerabilities	MITS

Annex C. Comparison Table ITSG-04 Versus NIST 800-30

The following table provides observations on both methodologies and interpretation on the differences between the NIST 800-30 and the ITSG-04.

Criteria	ITSG-04	NIST 800-30
Date Published	October 1999	October 2001
Published by	CSE	NIST
Number of Pages	36 (without annexes)	41 (without annexes)
Risk Management activities	Planning, organizing, directing and controlling	Risk Assessment, risk mitigation, and evaluation and assessment
Managing Risk Options	Transfer / Avoidance / Acceptance / Reduction	Assumption / Avoidance / limitation / Planning / Research and Acknowledgement / Transference
SDLC Integration	Yes	Yes
TRA steps or tasks	9	9
Critical Assets identification	Integral part of the SoS based on CIA	Much less emphasis on identification of critical assets and CIA
Sensitivity Schema	National Interest and Non-National Interest Classified and Protected information	Sensitive unclassified information in federal computer systems
Statement of Sensitivity (SoS)	Integral part of a TRA CIA and replacement value Qualitative Example SoS in an Annex	Less emphasis on assets, more on threat and vulnerability. Introduce assets after threat and vulnerability sections Associate asset criticality to BIA CIA with qualitative
Threat language	Threat agent Threat event Threat scenario	Threat source Threat action Threat statement
Threat Analysis	Capability and Motivation Numerical value of 1 to 5 Likelihood of threat event occurring (very limited guidance) Does not take into consideration vulnerabilities and existing safeguards at this stage. Qualitative or quantitative List of threat agents and threat events in Annexes	Capability and Motivation Likelihood determination is based on threat source motivation and capability, nature of vulnerability, existence of controls Qualitative

Criteria	ITSG-04	NIST 800-30
Vulnerability Analysis	Exposure and severity Vulnerability rating (quantitative) List of vulnerability in an Annex	List of vulnerability (NIST I-CAT Vulnerability database) http://icat.nist.gov/icat.cfm Security requirement checklist in three security area: Management security / Operational Security / Technical Security Use self assessment guide to develop checklist ITS 800-26
Risk Analysis	Combination of threat scenarios likelihood and impact Vulnerability and existing safeguards Risk rating Terminology: Safeguards	Likelihood the threat source exercise a vulnerability Magnitude of impact should the threat source exercise vulnerability Adequacy of planned or existing controls Explanation of risk value Terminology: Controls
Recommendations	Safeguard functional categories: Correction / Detection / Deterrence / Prevention (Avoidance) / Containment / Recovery / Monitoring / Awareness	Technical Security Controls: Support / Prevention / Detection & Recovery Management Security Controls: Preventive / Detection / Recovery Operational Security Controls: Prevention / Detection
Implementation Plan	No	Yes
Observations	ITSG-04 is an asset and threat centric methodology.	NIST 800-30 is a vulnerability centric methodology

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Establishment sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Cinnabar Networks Inc.
265 Carling Avenue, Suite 400,
Ottawa, Ontario K1S 2E1

2. SECURITY CLASSIFICATION (overall security classification of the document, including special warning terms if applicable)

UNCLASSIFIED

3. TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C or U) in parentheses after the title.)

Common Methods for Security Risk Analysis (U)

4. AUTHORS (Last name, first name, middle initial)

Sylvie Malboeuf, William Sandberg-Maitland, William Dziadyk, Eugen Bacic

5. DATE OF PUBLICATION (month and year of publication of document)

December 2004

6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc.)

80

6b. NO. OF REFS (total cited in document)

52

7. DESCRIPTIVE NOTES (the category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Final Contractor Report

8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include the address.)

Defence R&D Canada, Ottawa

9a. PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant)

15bf26

9b. CONTRACT NO. (if appropriate, the applicable number under which the document was written)

W7714-4-3009 & W7714-4-3010

10a. ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the originating activity. This number must be unique to this document.)

10b. OTHER DOCUMENT NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor)

DRDC Ottawa CR 2004-247

11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification)

(x) Unlimited distribution
( ) Distribution limited to defence departments and defence contractors; further distribution only as approved
( ) Distribution limited to defence departments and Canadian defence contractors; further distribution only as approved
( ) Distribution limited to government departments and agencies; further distribution only as approved
( ) Distribution limited to defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in 11) is possible, a wider announcement audience may be selected.)

13. ABSTRACT (a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual).

This document is the results of a study conducted to document the state of the Canadian risk management. The study provides a history of Canada' initiatives with respect to risk management and investigates how Canada can augment the Working Group with its experiences and its future initiatives and opportunities. In addition, the study presents a comparison between the prevalent Canadian threat and risk assessment methodology (ITSG 04) and the recommendations of the National Institute of Standards and Technology Risk Management Guide for Information Technology Systems (NIST 800-30). Substantial evolution of risk management has occurred in the past few years, but the tools and documentation have been a significant impediment on further development. There is a definite need to standardize the TRA process and provide system owners with a useful and consistent tool to evaluate the risks to information and IT systems.

The approach to a common framework is emphasized by the need for a common language. The provision of a shared set of concepts and vocabulary can only help unify the disparate terminologies that variant TRA approaches and methodologies have engendered. Equally valuable is the prospective TRA automation or partial automation. Automated tools were premature in the early days when risk management was first introduced. Practitioners have gained expertise and experience in the conduct of TRA. It is recognized that human intervention will most likely be required in any automated TRA, however partial automation may be an initial step toward a common framework.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Computer Security
Risk Assessment
Threat and Risk Analysis