Harmonized Threat and Risk Assessment (TRA) Methodology

TRA-1

Date: October 23, 2007

This page intentionally left blank.

Foreword

The *Harmonized Threat and Risk Assessment (TRA) Methodology* is an unclassified publication, issued under the authority of the Chief, Communications Security Establishment (CSE) and the Commissioner, Royal Canadian Mounted Police (RCMP). It supersedes and replaces the following CSE and RCMP publications:

- ITSG-04, Threat and Risk Assessment Working Guide;
- G2-001 Guide to Threat and Risk Assessment for Information Technology;
- R1-001 Threat and Risk Assessment Involving On-site Physical Security Examination;
- R1-001a/b TRA Baselines;
- R1-001c TRA Statement of Sensitivity; and
- R1-003 Survey Notes/Form.

This initial version of the *Harmonized TRA Methodology* should be regarded as an interim release pending completion of the policy suite renewal project by the Treasury Board Secretariat. Of necessity, it will require updating once the Government Security Policy and supporting standards have been revised and replaced. That being said, the actual mechanics of the methodology are likely to remain the same, only references to the superior policies, directives and standards are expected to change significantly.

Suggestions for amendments and requests for clarification should be forwarded through departmental security channels to your Client Services Representative at CSE or the Technical Security Branch of the RCMP.

Further advice and guidance on the *Harmonized Threat and Risk Assessment (TRA) Methodology* is available from:

IT Security Client Services
Communications Security Establishment
P.O. Box 9703
Terminal
Ottawa, Ontario
K1G 3Z4
Telephone: (613) 991-7600
E-Mail: client.svcs@cse-cst.gc.ca

Royal Canadian Mounted Police
Technical Security Branch
E-Mail: traclientservices@rcmp-tsb.ca

Specific training options are described at the following web sites:

Communications Security Establishment
http://www.cse-cst.gc.ca/training/training-e.html

Royal Canadian Mounted Police
http://www.rcmp-grc.gc.ca/tsb/workshops/index_e.htm

Effective Date

This publication takes effect on 2007-08-28.

Gwen Beauchemin
Director, IT Security Mission Management Group
Communications Security Establishment

Guylaine Dansereau
Director, Technical Security Branch
Royal Canadian Mounted Police

Revision History

Document No.	Title	Release Date

This page intentionally left blank.

Table of Contents

Foreword i
Effective Date ii
Revision History iii
Table of Contents v
List of Tables vii
List of Figures ix
Introduction IN-1
Executive Overview E0-1
Management Summary MS-1
Annex A - Preparation Phase A-1
Appendix A-1 - TRAs in a Project Plan/System Development Life Cycle A1-1
Appendix A-2 - Security Standards versus Threat and Risk Assessments A2-1
Appendix A-3 - TRA Team Composition A3-1
Appendix A-4 - Use of TRA Consultants A4-1
Appendix A-5 - Sample Statement of Work for TRA Consulting Services A5-1
Appendix A-6 - Sample TRA Work Plan A6-1
Annex B - Asset Identification and Valuation Phase B-1
Appendix B-1 - Sources of Asset Data B1-1
Appendix B-2 - Asset Listing B2-1
Appendix B-3 - BIA, PIA and TRA B3-1
Appendix B-4 - Expanded Injury Table B4-1
Appendix B-5 - Asset Valuation Table / Statement of Sensitivity B5-1
Annex C - Threat Assessment Phase C-1
Appendix C-1 - Sources of Threat Data C1-1
Appendix C-2 - Threat Listing C2-1
Appendix C-3 - Threat Metrics C3-1
Appendix C-4 - Threat Assessment Table C4-1
Annex D - Vulnerability Assessment D-1
Appendix D-1 - Sources of Vulnerability Data D1-1
Appendix D-2 - Vulnerability Listing D2-1
Appendix D-3 - Vulnerability Metrics D3-1
Appendix D-4 - Vulnerability Assessment Table D4-1
Annex E - Calculation of Residual Risks E-1
Appendix E-1 - Residual Risk Tables E1-1
Appendix E-2 - List of Assessed Residual Risks E2-1

Annex F - Recommendations Phase F-1
Appendix F-1 - Sources of Safeguard Data F1-1
Appendix F-2 - Safeguard Listing F2-1
Appendix F-3 - Selection of Potential Safeguards F3-1
Appendix F-4 - Calculation of Safeguard Cost Effectiveness F4-1
Appendix F-5 - Recommendations Table F5-1
Appendix F-6 - Outline TRA Report F6-1
Appendix F-7 - Sample TRA Report F7-1

Annex G - Conclusion G-1
Appendix G-1 - TRA Worksheet G1-1
Appendix G-2 - Glossary and Acronyms G2-1
Appendix G-3 - References G3-1

List of Tables

Table A-1: Typical Length of a TRA Report A-8
Table A1-1: Relative Stages in a Project Plan and System Development Life Cycle A1-3
Table A6-1: TRA Team Composition List A6-3
Table A6-2: Simple TRA Activity List A6-5
Table B-1: Asset Categorization Injury Levels Specified by the GSP B-7
Table B-2: Comparative Asset Values B-8
Table B-3: Abbreviated Injury Table and Asset Values B-9
Table B-4: Sample Asset Valuation Table/Statement of Sensitivity B-16
Table B3-1: Comparative Mapping of BIA, PIA and TRA Processes B3-5
Table C-1: Threat Likelihood Table C-12
Table C-2: Threat Gravity Table C-14
Table C-3: Threat Levels Table C-15
Table C-4: Sample Threat Assessment Table C-17
Table C3-1: Threat Likelihood Table C3-1
Table C3-2: Threat Gravity Table C3-2
Table C3-3: Threat Levels Table C3-2
Table D-1: Safeguard Impact Table D-5
Table D-2: Vulnerability Impact on Probability of Compromise (Prevention) D-14
Table D-3: Vulnerability Impact on Severity of Outcome (Detection, Response, Recovery) . D-16
Table D-4: Basic Vulnerability Assessment D-17
Table D-5: Sample Vulnerability Assessment Table D-20
Table D3-1: Vulnerability Impact on Probability of Compromise (Prevention) D3-1
Table D3-2: Vulnerability Impact on Severity of Outcome (Detection, Response, Recovery) D3-2
Table D3-3: Basic Vulnerability Assessment D3-2
Table E-1: Numeric Scores for Asset Value, Threat and Vulnerability Levels E-2
Table E-2: Risk Levels and Ranges E-3
Table E-3: List of Assessed Residual Risks E-4
Table E1-1: Numeric Scores for Asset Value, Threat and Vulnerability Levels E-1

Table E1-2: Risk Levels and Ranges E1-2
Table E1-3: Risk Table for Very Low Asset Values E1-2
Table E1-4: Risk Table for Low Asset Values E1-3
Table E1-5: Risk Table for Medium Asset Values E1-3
Table E1-6: Risk Table for High Asset Values E1-3
Table E1-7: Risk Table for Very High Asset Values E1-3
Table F-1: Acceptability of Assessed Residual Risks F-2
Table F3-1: Abbreviated List of Assessed Residual Risks F3-1
Table F3-2: List of Unacceptable Assessed Residual Risks F3-3
Table F3-3: List of Potential Safeguards F3-5
Table F3-4: Projected Residual Risks with a Locked Entrance and Escorted Access F3-8
Table F3-5: Projected Residual Risks Adding a Duress Alarm and Security Guard on Call F3-8
Table F3-6: Projected Residual Risks with Security Guard, etc. F3-9
Table F4-1: Initial and Recurring Direct and Indirect Costs F4-3
Table F4-2: Calculation of Safeguard Cost Effectiveness F4-4
Table F7-1: Calculation of Assessed Residual Risk F7-3

List of Figures

Figure IN-1: Modular Structure of the Harmonized TRA Methodology IN-4
Figure EO-1: Integrated Risk Management Process EO-1
Figure EO-2: Management Accountability Framework EO-2
Figure EO-3: A Harmonized TRA Methodology in Support of Modern Comptrollership EO-3
Figure MS-1: Contextual Framework for the Harmonized TRA Methodology MS-2
Figure MS-2: Phases and Processes within a TRA Project MS-3
Figure MS-3: (Very) Simplified Risk Management Model MS-9
Figure A1-1: TRA Information Flows in a Project Environment A1-4
Figure A2-1: Risk Management Methodologies A2-3
Figure A2-2: Hierarchy of Security Documentation A2-4
Figure A4-1: Engaging Consultants to Augment Dedicated TRA Staff A4-3
Figure A6-1: Diagram Illustrating Linked TRA Projects for a Single Facility A6-2
Figure B-1: Asset Identification Model B-4
Figure B-2: Sample Segment of the Asset Listing Hierarchical Structure B-5
Figure B-3: Selecting Assets within the Scope of a TRA Project B-6
Figure B-4: Asset Values Based on Complete Compromise B-10
Figure B3-1: Scope of a TRA B3-2
Figure B3-2: Scope of a BIA B3-3
Figure B3-3: Scope of a PIA B3-3
Figure C-1: General Threat Model C-3
Figure C-2: Sample Segment of the Threat Listing Hierarchical Structure C-4
Figure C-3: Direct and Indirect Threats C-10
Figure D-2: Vulnerability Listing Hierarchical Structure D-12
Figure E-1: Calculation of Residual Risk E-2
Figure F-1: Active Security Strategy F-6
Figure F-2: Calculation of Amortized Annual Cost F-11
Figure F-3: Calculation of Safeguard Cost-Effectiveness F-12

This page intentionally left blank.

Introduction

1 Background

When the *Government Security Policy (GSP)* was first promulgated in June 1986, it introduced several important concepts, including the safeguarding of sensitive information and assets on the basis of minimum security standards and an assessment of related threats and risks. Shortly thereafter, the threat and risk assessment (TRA) process was described in more detail in section 9 of the *Security Organization and Administration Standard*. Nevertheless, it was recognized that government institutions would require even more specific direction and guidance on the conduct of TRAs before they could be implemented in practice. Therefore, over the next fifteen years, two lead agencies assigned specific responsibilities in Appendix A to the policy for providing advice on TRAs, namely the Communications Security Establishment (CSE) and the Royal Canadian Mounted Police (RCMP), published an array of technical documentation, including:

> "Departments must . . .
> – Apply physical and information technology safeguards to sensitive information and assets in accordance with standards and threat and risk assessment."
>
> *Government Security Policy*, June 1986

- *Preparation of Physical Security Briefs* (G1-005);
- *Guide to Threat and Risk Assessment Involving On-Site Physical Security Examination*;
- *Guide to Threat and Risk Assessment for Information Technology (IT)* (G2-001);
- *A Guide to Security Risk Management for Information Technology Systems* (MG-2);
- *A Guide to Risk Assessment and Safeguard Selection for IT Systems* (MG-3);
- *A Guide to Certification and Accreditation for IT Systems* (MG-4); and
- *Threat and Risk Assessment Working Guide* (ITSG-04).

2 Issues

Despite these ongoing efforts to develop explicit instructions on the preparation of TRAs, many government institutions experienced considerable difficulties with the process, which was often viewed as needlessly complex and inflexible. These problems were compounded because the responsible lead agencies actually fielded three different TRA methodologies, one for physical security and two more for IT systems. Although the fundamental principles remained the same, many detailed differences amongst the varied guidelines and related training caused some confusion and inconsistencies in their application. In fact, the Auditor General noted these discrepancies and a widespread reluctance to conduct TRAs in the February 2005 audit of IT Security.

> "Out of 82 departments and agencies we surveyed, only 37 (45 percent) had performed threat and risk assessments of their programs, systems, or services".
>
> *Audit of Information Technology Security*, February 2005

3 Objectives

In order to address these legitimate concerns and promote the use of TRAs, CSE and the RCMP initiated a joint project in December 2004 to develop a single *Harmonized Threat and Risk Assessment Methodology* for the Government of Canada with the following goals or objectives:

- **Flexibility -** The new methodology must be **scalable** to handle all assets, physical and IT, both large and small, at an appropriate level of detail to satisfy business objectives. It must support different levels of **granularity** with a roll-up capability, from finely detailed or tightly focused analyses to more broad overviews, depending upon the risk environment and the purpose of the assessment.
- **Modularity -** To permit the breakdown of larger more complex TRAs into smaller, more manageable components, the new methodology must support modular analysis with suitable linkages between related elements.
- **Simplicity -** The underlying logic of the methodology must be intuitively satisfying and simply stated to permit easy application by program and project managers, as well as security practitioners. To enhance user-friendliness, the fundamental principles and processes of the harmonized methodology must be well illustrated with extensive charts, diagrams, examples, tables and templates.
- **Consistency** - To achieve greater consistency amongst TRAs performed by different agencies, the new methodology must establish a common vocabulary with straightforward definitions for all aspects of risk management. Solid metrics for risk variables, specifically asset values, threats and vulnerabilities, are essential for comparative analysis and replicable results, both of which are crucial to informed risk communications, improved interoperability and cost-effective security solutions.
- **Generality** - The methodology must apply equally to physical and IT assets, as well as the protection of employees and service delivery.
- **Automation -** Although the *Harmonized Threat and Risk Assessment Methodology* is a manual tool, it has been developed with a view to automation to further simplify and support the TRA process.

4 Principles

Some important principles have governed development of the *Harmonized Threat and Risk Assessment Methodology*, including:

- **Compatibility -** The new methodology must build upon and support the GSP and relevant Operational Security Standards, particularly those regarding the Identification of Assets, Security Risk Management, Management of Information Technology Security, Physical Security and Business Continuity Planning. It must be tightly integrated with other related policies, especially those concerning Risk Management, Access to Information and Privacy, as well as the Integrated Risk Management and Management Accountability Frameworks.

- **Transparency -** To best meet the needs of government managers who will ultimately use the new methodology, extensive interdepartmental consultation with regular briefings and an active user focus group was essential during the development process.
- **Evolutionary Change -** Over the past twenty years, security lead agencies have invested significant time and effort to develop various TRA methodologies with the associated guidelines and training packages. Many departments have made considerable efforts to adopt and employ these tools. Therefore, to take advantage of this knowledge and experience, the *Harmonized Threat and Risk Assessment Methodology* has been developed as an incremental improvement rather than a radical departure from established practices.

5 Structure and Use

In order to meet the dual objectives of simplicity and flexibility in a comprehensive, general purpose tool, the *Harmonized Threat and Risk Assessment Methodology* has been structured in a highly modular format at several levels of detail, ranging from high level summaries to increasingly focused descriptions of specific processes and metrics. Most segments are limited to a few pages in length, so users may concentrate quickly on those aspects of immediate interest or concern without having to search through a lengthy narrative. This format also facilitates cross-referencing for easy accessibility.

Major modules of the *Harmonized Threat and Risk Assessment Methodology* include:

- a **Foreword** to identify the authority for issuing the document and provide a point of contact for questions and suggested improvements, as well as the usual Table of Contents and Lists of Figures and Tables;
- an **Executive Overview** to explain the importance of TRAs as a tool to help senior executives meet their responsibilities and accountabilities for Modern Comptrollership, and the Integrated Risk Management and Management Accountability Frameworks;
- an **Introduction** to review some background, the rationale for a new methodology, the objectives and principles that governed its development, and the structure adopted to achieve these goals;
- a **Management Summary** to describe the entire TRA process at a high level for program and project managers with risk management responsibilities;
- a series of six **Annexes** to present each step of the TRA process in greater detail for program, project and security staff who must apply the methodology in practice;
- an array of **Appendices** with even more detailed material in the form of diagrams, technical descriptions, checklists, flowcharts, tables, and templates to illustrate every aspect of the TRA process and facilitate easy application; and
- a seventh **Annex** containing additional supporting material, such as a comprehensive Glossary, List of Acronyms and References.

This format is illustrated in Figure IN-1.
Anyone approaching the document for the first time should browse the Introduction (4 pages) and read the Management Summary (9 pages) very carefully to understand the overall process.

The more detailed annexes and appendices are intended to help program or project personnel and security practitioners who are actually tasked with the preparation of a TRA report. Each should be studied thoroughly before commencing the successive phases of a TRA project. Many of the normal questions and concerns will be answered specifically in the body of these segments, often with practical examples to illustrate different solutions.

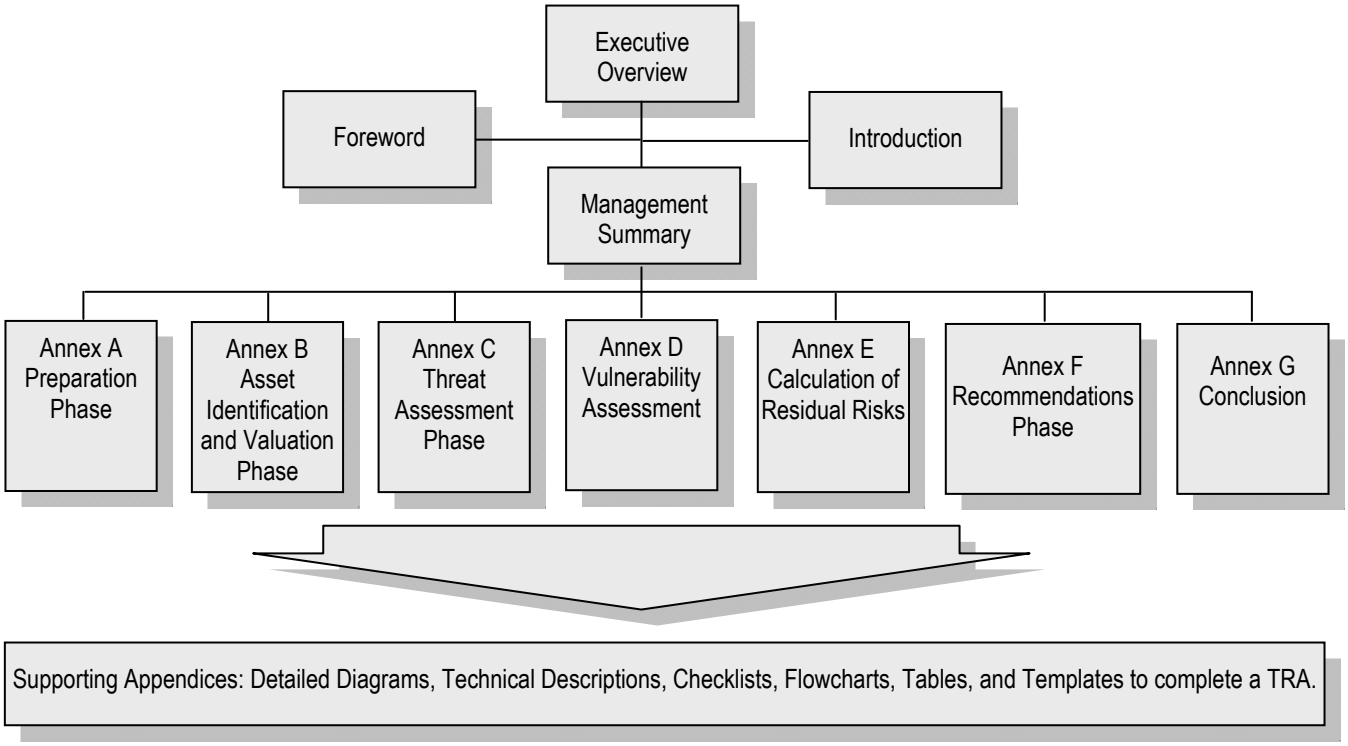

Figure IN-1: Modular Structure of the Harmonized TRA Methodology

In addition to this comprehensive toolkit, the *Harmonized Threat and Risk Assessment Methodology* also comprises structured training and awareness products to ensure easy accessibility and greater utility for departmental risk managers. These include:

- a formal training package with practical exercises to explain the user guide and reinforce the learning experience; and
- complementary briefings for senior program and project managers to situate the methodology within the overall Integrated Risk Management Framework and Modern Comptrollership generally.

As indicated in the Foreword, departmental program and project managers may obtain advice and guidance on the *Harmonized Threat and Risk Assessment Methodology* and its application from their Departmental Security Officer and IT Security Coordinator, and the responsible lead security departments, namely the Communications Security Establishment and the Royal Canadian Mounted Police.

Executive Overview

As part of the **Modern Comptrollership** initiative, *Results for Canadians: A Management Framework for the Government of Canada* identified four major commitments to improve management practices and enhance service delivery: (1) sharper **citizen focus**; (2) a clear set of **values**; (3) strong emphasis on **results**; and (4) **responsible spending** of limited public funds.

Clearly, new technologies offer many opportunities for innovative solutions to meet these important challenges, albeit with attendant risks arising from the rapid rate of change, the inherent complexity of many service lines, and a variety of hazards ranging from system failures through deliberate misuse to natural disasters. To balance both risks and opportunities more effectively, **Mature Risk Management** is one of the four pillars of Modern Comptrollership.

The **Integrated Risk Management Framework,** developed in response to the *Report of the ADM Working Group on Risk Management: Risk Management for Canada and Canadians*, amplifies the earlier *Risk Management Policy* which requires departments to: (1) identify potential perils; (2) analyze and assess risks; and (3) implement cost-effective risk prevention, reduction or avoidance control mechanisms. The more elaborate nine-step model of the Integrated Risk Management Framework is illustrated in Figure EO-1.

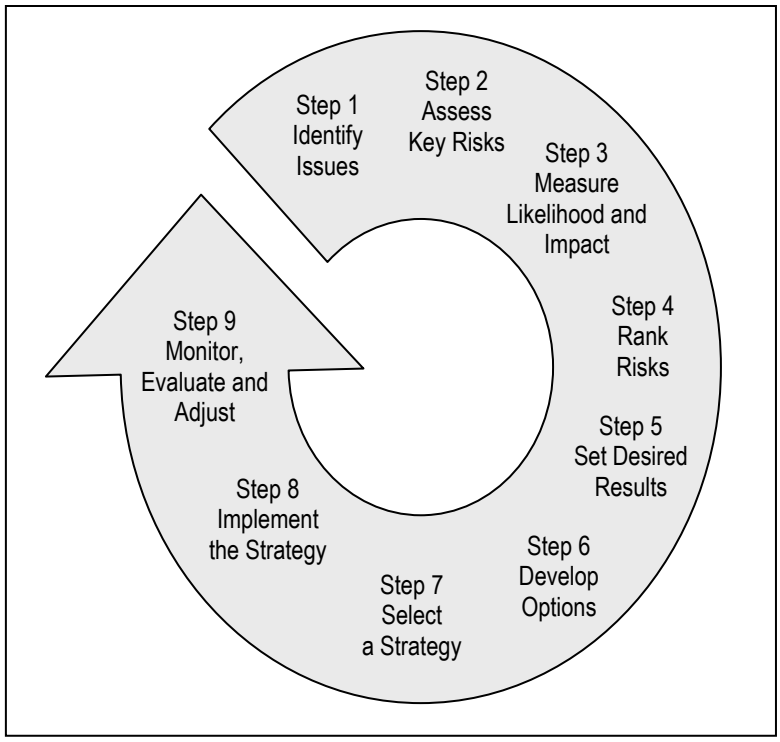

Figure EO-1: Integrated Risk Management Process

To help deputy heads and all public service managers assess organizational performance and identify priorities for management improvement, the Treasury Board Secretariat developed a *Management Accountability Framework* comprising 10 essential elements of sound management, illustrated in Figure EO-2, with a series of indicators and associated measures of effectiveness. While all ten factors are tightly integrated and completely interdependent, the ultimate goals of **Results and Performance** in the provision of **Citizen-focused Service** cannot be achieved transparently with full **Accountability** for sound **Stewardship** in the absence of effective **Risk Management**. It is equally important to balance the opportunities and risks inherent to **Innovation and Change Management** within a solid **Governance Framework** in support of **Strategic Directions** consistent with approved **Policies and Programs**. In short, informed risk management is crucial to responsible decision making.

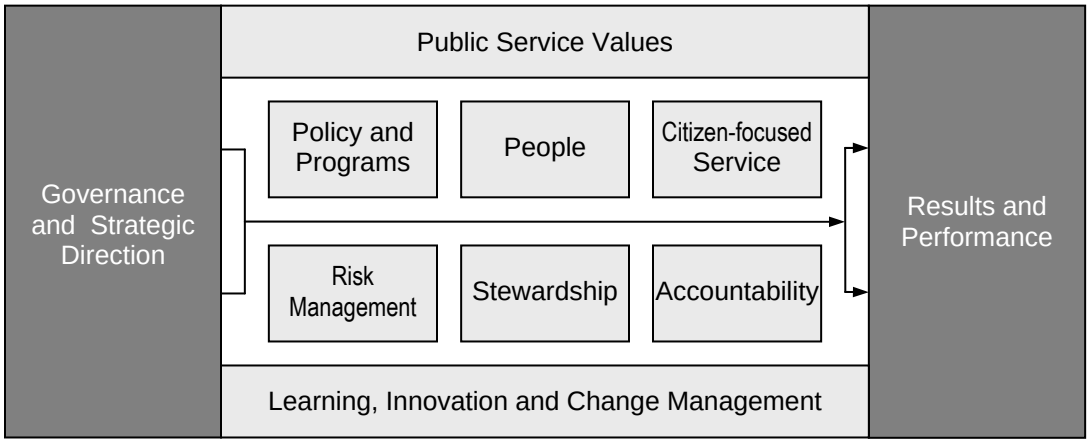

Figure EO-2: Management Accountability Framework

The stated objectives of the *Government Security Policy (GSP)* are very similar: "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." From a practical perspective, the GSP prescribes two complementary mechanisms, baseline security requirements and continuous risk management based upon the Threat and Risk Assessment (TRA), to achieve adequate protection for employees, assets and services at risk.

The latter approach, the TRA, is a particularly powerful tool to help program and project managers meet their responsibilities for due diligence and sound stewardship while seeking innovative solutions to enhance service delivery results and performance. More specifically, the *Harmonized Threat and Risk Assessment Methodology for the Government of Canada* provides:

- a **common vocabulary** to promote better understanding, more informed discussion and, therefore, improved communications regarding risk dynamics;
- a **flexible toolkit** to help managers identify important assets and services, as well as the vulnerabilities that expose them to potential hazards, all at an appropriate level of detail;
- **explicit metrics** for comparative analysis to prioritize relative risks;
- a **clear rationale** for cost-effective risk mitigation strategies and safeguards to meet business requirements; and

- a **transparent audit trail** and **record of risk management decisions** to demonstrate due diligence and accountability, thereby satisfying statutory obligations and policy requirements.

The *Harmonized Threat and Risk Assessment Methodology* is designed to address all employees, assets and services at risk. Furthermore, it is easily integrated with project management methodologies and system development life cycles. Analysis may be performed at any level of granularity, from broadly based departmental risk profiles to more tightly focused examinations of specific issues, to meet management needs for responsive solutions at both strategic and operational levels. Use of common tools can promote interoperability when managing risks across shared facilities and interconnected information technology systems, an increasingly important consideration when service delivery responsibilities transcend organizational boundaries. Finally, in the spirit of Modern Comptrollership, objective metrics and analytical reports support the Management Accountability Framework to assess results and performance, especially with respect to risk management, stewardship and accountability. The relationships amongst these important elements of Modern Comptrollership are illustrated in Figure EO-3.

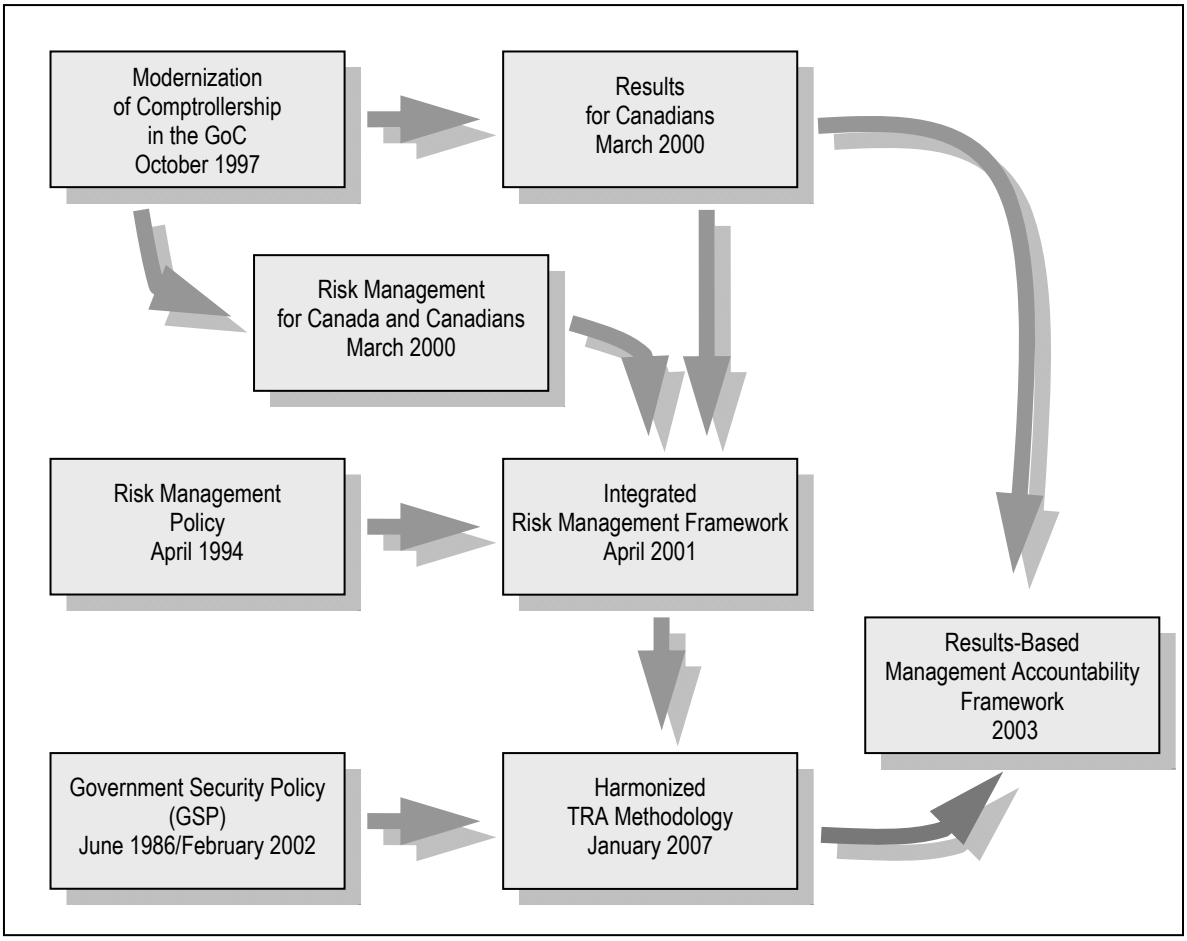

Figure EO-3: A Harmonized TRA Methodology in Support of Modern Comptrollership

This page intentionally left blank.

Management Summary

1 Introduction

> "Assets must be safeguarded according to baseline security requirements and continuous security risk management."
>
> *Government Security Policy*, February 2002

At the highest level, the Government Security Policy (GSP) prescribes two complementary approaches to security risk management.

The first is the application of baseline security requirements, or minimum security standards, specified in the policy itself and other supporting documentation, specifically the operational security standards and technical documentation described in section 9 of the GSP. Baseline security standards offer many advantages including ease of use, increased uniformity and, therefore, improved interoperability, amongst others. However, given the time required to develop effective standards, many become outdated by rapidly changing technologies. Furthermore, the choice of countermeasures may be limited and, as minimum standards, they may not be sufficient for more valuable assets faced with more serious threats.

To address these issues, the GSP provides for continuous risk management in the form of a threat and risk assessment (TRA) as an effective supplement.

While baseline security standards and TRAs differ considerably, the two approaches to risk management are entirely complementary.[1] Thus, a manager may conduct an informal TRA or cursory scan of the risk environment to determine the adequacy of baseline security standards. Then, if necessary, conduct a comprehensive TRA to address any gaps.

Where a comprehensive assessment is required, section 10.7 of the policy, Security Risk Management, describes a four-step TRA process:

- Establish the **scope of assessment** and **identify employees and assets** to be safeguarded.
- Determine the **threats to employees and assets** in Canada and abroad, and assess the likelihood and impact of their occurrence.
- Assess **vulnerabilities** based on the adequacy of **safeguards** and compute the **risk**.
- Implement **additional safeguards**, if necessary, to reduce risk to an acceptable level.

Other policy requirements amplify certain steps of the process and indicate where TRAs must be applied to achieve cost-effective security solutions for the protection of employees, assets and service delivery. Although operational security standards dealing with Identification of Assets, Security Risk Management, Physical Security, and the Management of IT Security and Business Continuity Planning expand upon these policy requirements, even more explicit details are necessary to actually complete a formal TRA project that will provide meaningful results.

[1] See Appendix A-2 for a fuller discussion of the relationship between security standards, TRAs, both formal and informal, and other approaches to risk management.

Therefore, the *Harmonized Threat and Risk Assessment (TRA) Methodology* has been developed as a practical tool elaborating on the policy and supporting standards, as illustrated in Figure MS-1, to help government managers meet both the objectives and the requirements of the GSP.

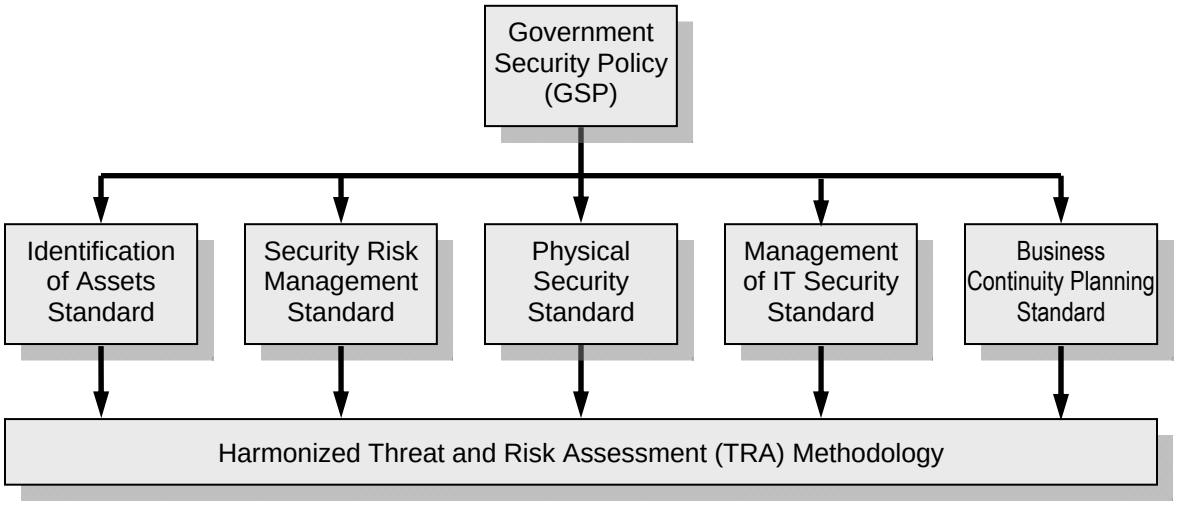

Figure MS-1: Contextual Framework for the Harmonized TRA Methodology

The *Harmonized TRA Methodology* presents the TRA as a project conducted in five distinct phases, each of which comprises three or more processes, as depicted in Figure MS-2. The first phase establishes both the mandate and scope of the project. The next three ascertain the risk environment with an examination of assets and their values, as well as threats and vulnerabilities within the scope of the assessment. The last phase provides recommendations regarding the acceptability of residual risks and, if necessary, identifies mitigation strategies and safeguards. Thus, the TRA is simply a formal project to collect and analyze relevant data to determine risk levels and recommend efficient, cost-effective safeguards where required.

Each TRA phase and the related processes are explained briefly in the balance of the Management Summary, and amplified considerably in the subordinate Annexes and Appendices.

2 Preparation

2.1 General

Careful planning and forethought are crucial to achieve effective results with any TRA project.

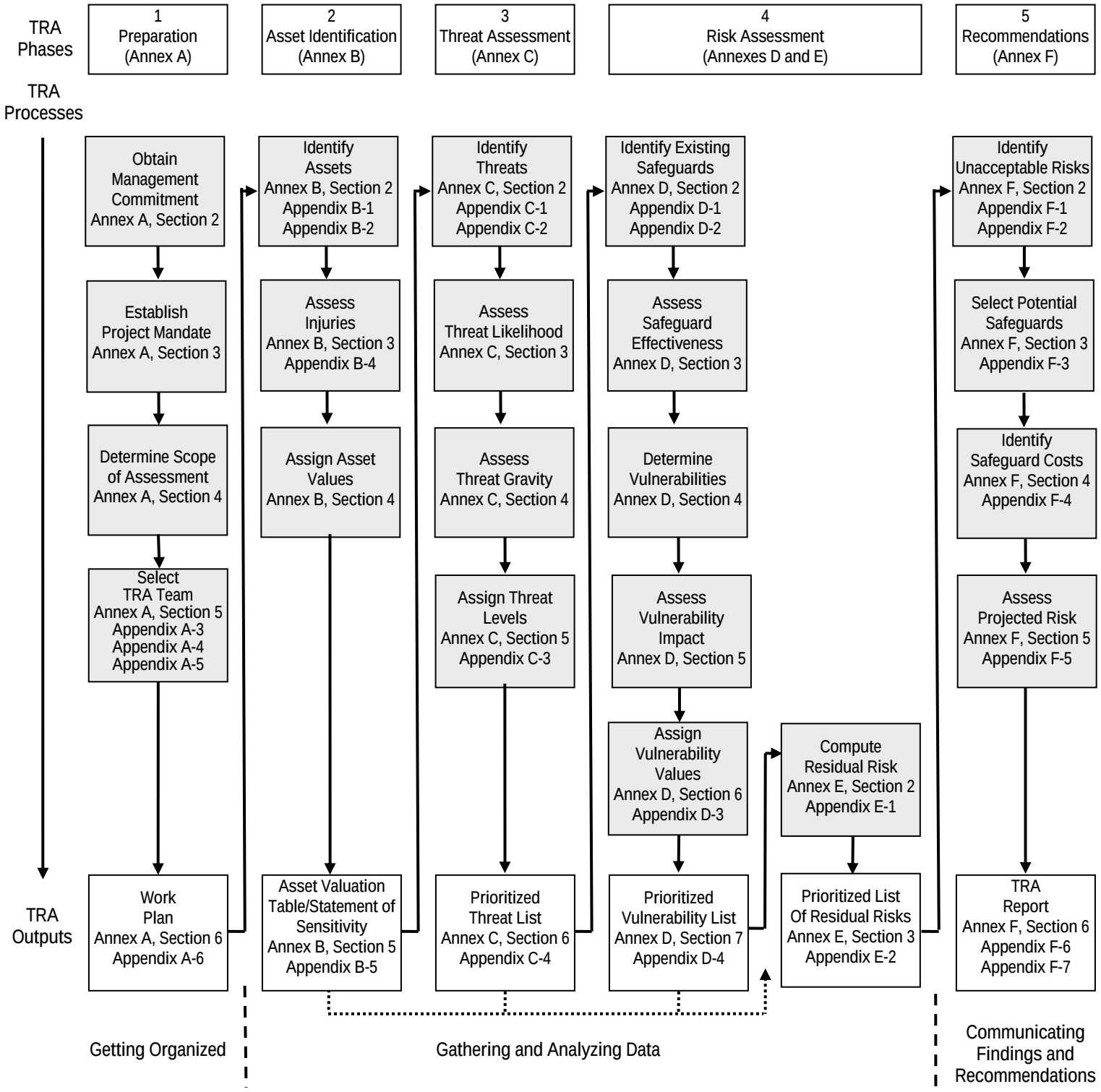

Figure MS-2: Phases and Processes within a TRA Project

2.2 Management Commitment

In order to make informed decisions regarding the acceptability of any residual risk, departmental executives require a sound understanding of TRAs and their role within an overall risk management program. Management commitment and support are also necessary to establish a clear mandate, mobilize necessary resources and facilitate the collection of data required for a balanced assessment.

2.3 Mandate of a TRA Project

Senior managers normally assign the responsibility for conducting a TRA to a single office or official with sufficient knowledge of both the business at hand and the selected TRA methodology. The designated official should first clarify the purpose of the TRA project in order to confirm both the feasibility of the exercise and the necessity for an assessment. Once these have been reviewed and accepted, relative roles and responsibilities should be specified, especially for the risk acceptance authority. Other issues to consider include project priorities, management expectations and reporting, all of which should be recorded in the TRA project Work Plan, as indicated in Section 2.7 below.

2.4 Scope of a TRA Project

Many TRAs fail because the scope of the assessment is not clearly defined at the beginning of the project. Almost inevitably this can lead to wasted effort and needless delays so it is important to determine the purpose of the assessment, the level of detail required and the boundaries of the exercise right at the start. As a general rule, the most effective TRAs are as short as possible consistent with the need for informed decision making. To achieve this ideal with larger projects or complex assets, it is often preferable to conduct several smaller, more modular assessments rather than one massive project. Of course, a project may be re-scoped at any time to meet changing circumstances, such as the discovery of previously unknown threats or vulnerabilities. With this in mind, some factors to consider when determining the scope of the TRA include:

- the **stage in the project plan** or **system development life cycle** – greater precision will be required as projects evolve from initial requirements definition through detailed design and development to final implementation;
- the **risk environment** – more extensive, in-depth analysis is generally required for the employees, assets and services at greatest risk, so a cursory scan may be necessary at first to characterize the risk environment;
- the **purpose of the TRA project** – departmental assessments are typically high level and broadly based, while those for major Crown projects are often quite detailed; conversely, very short, highly focused TRAs are ideally suited to address specific security concerns; and
- **cost and time constraints** – of necessity, practical considerations may limit the scope for legitimate reasons, but even a higher level TRA may serve management purposes.

2.5 Team Composition

Although smaller TRAs may be completed by a single individual, most will require a team effort to muster the necessary information and expertise for an effective assessment. In general, more team members are required for larger, complex projects, but even simpler, focused projects will require access to personnel with different knowledge and skill sets. To ensure adequate information for evaluation, the following authorities normally participate directly as team member, or at least provide input to a TRA:

- **program or business managers** understand the operational importance of employees, assets and the services they deliver, as well as the injuries that could arise in the event of a compromise, so their input is crucial to the Asset Identification and Valuation phases of the assessment;
- **project managers** and their staff translate functional or business requirements into technical solutions, so they can contribute significantly to both the asset identification process and the subsequent Vulnerability Assessment;
- **facility managers**, **Chief Information Officers** and their staff can provide valuable information regarding shared accommodations and technical infrastructures for both the asset identification process and the Vulnerability Assessment; and
- **departmental security authorities**, namely the Departmental Security Officer (DSO), IT Security Coordinator (ITSC) and Business Continuity Planning Coordinator (BCPC), can offer advice and guidance regarding the threat environment and safeguard options.

2.6 Other Resources

Depending upon the scope and purpose of a TRA project, other departmental resources, ranging from privacy coordinators through occupational health and safety staff to financial and materiel managers, as well as internal auditors and legal counsel may provide useful details to supplement material gathered by core team members. External resources available to the TRA team may include Lead Security Departments defined in Appendix A to the GSP and a variety of private consultants with relevant technical or professional qualifications.

2.7 TRA Work Plan

To ensure a coordinated effort that meets the operational needs of program managers and departmental executives, the TRA team should prepare a comprehensive Work Plan as their first major task. This plan should be approved by the risk acceptance authority who will ultimately review the recommendations and accept or reject the projected residual risk identified in the TRA report. While the actual level of detail will vary according to the scope and magnitude of the assessment, the plan should record as a minimum:

- the established mandate, purpose, scope and terms of reference for the TRA;
- the core team and other resources at their disposal, with short terms of reference for each;
- relevant inputs to the project, such as earlier TRA records, Privacy Impact Assessments (PIAs), Business Impact Analysis (BIAs), design documentation, facility floor plans,

inventory lists and any relevant memoranda of understanding (MOUs) for the sharing of information or other assets;
- a schedule with target dates for each deliverable from the Asset Identification Phase to the final recommendations in the TRA Report; and
- relevant logistic arrangements, such as security screening, administrative support and resource requirements, including the source of funds for any related expenditures, such as consulting contracts.

3 Asset Identification and Valuation

Once the Preparation Phase is complete, the TRA team may commence asset identification and valuation. This phase of a TRA project actually involves three different but closely related processes. Firstly, all employees, assets and services within the scope of the assessment must be identified at an appropriate level of detail to determine who and what might require protection. Next, the level of injury that could reasonably be expected to arise in the event of compromise to their confidentiality, availability or integrity must be assessed in accordance with the Identification of Assets Operational Security Standard. Then, based on this assessment, relative values are assigned to categorize assets and services in particular. All assets have one or more values related to their confidentiality, availability or integrity.

To facilitate the identification of assets at an appropriate level of detail, the *Harmonized TRA Methodology* introduces a comprehensive, hierarchical Asset Listing. To promote uniform asset valuation and permit comparative analysis amongst different assets or different values for the same asset, the guide also contains a complementary Injury Table with values ranging from Very Low to Very High.

The final output from the asset identification and valuation phase of a TRA project, also known as the Statement of Sensitivity, is simply a list of employees, assets and services with relative values assigned according to the injuries or operational impact arising from compromise.

4 Threat Assessment

Upon completion of the Asset Identification and Valuation Phase, the TRA team must identify any threats that could reasonably be expected to cause injury to employees, assets or service delivery identified in the second phase. All threats - man-made (deliberate or accidental) and natural hazards - are considered at a level of detail commensurate with the scope of the assessment. To differentiate between varied threats and determine which are more likely to pose serious concerns, each is assessed according to the **likelihood** of occurrence and the **gravity** of the event should it arise.

Given the uncertainties surrounding most threats, analysts often experience serious difficulties with this phase of a TRA project. Therefore, to facilitate the identification of threats at an appropriate level of detail, the *Harmonized TRA Methodology* introduces a comprehensive, hierarchical Threat Listing. Then, to promote comparative analysis amongst different threats,

the guide also provides simple metrics for both the likelihood and gravity of potential threat events, thereby arriving at Threat Values ranging from Very Low to Very High.

The final output from the threat assessment phase of a TRA project is simply a list of threats with relative values reflecting their likelihood of occurrence and seriousness of their potential impact on confidentiality, availability and integrity.

5 Risk Assessment

5.1 General

The fourth phase of a TRA project, the Risk Assessment, is conducted in two sequential stages. The first comprises five processes to assess vulnerabilities affecting employees' assets and services identified in the second phase that might be exploited by threats catalogued in the third phase. The second stage of the Risk Assessment involves a single process to compute the residual risk arising from each combination of assets with the related threats and vulnerabilities.

5.2 Vulnerability Assessment

In order to assess vulnerabilities, the TRA team must measure the effectiveness of existing safeguards and those pending implementation. Analyzing these data will reveal any attributes of employees and assets or the environment in which they operate that render them susceptible to compromise. The assessment of vulnerabilities may be complicated by a common misperception that they are always security weaknesses or flaws. While many vulnerabilities are negative attributes, others are positive qualities that simply have potentially adverse side effects. For example, the portability of notebook computers is a desirable feature for which one pays a premium, albeit one that makes them more susceptible to theft. Therefore, to help achieve a balanced assessment of vulnerabilities, the *Harmonized TRA Methodology* provides an extensive Vulnerability Listing suitably cross-referenced to the Safeguard Listing presented in the Recommendations Phase. As with asset and threat values, simple metrics are established to rate different vulnerabilities from Very Low to Very High.

5.3 Determining Residual Risk

Having identified and assigned values to assets (including employees and services), threats and vulnerabilities, it is a simple matter to compute the product of the three variables to produce a prioritized list of assessed residual risks for analysis during the Recommendations Phase of a TRA project.

6 Recommendations

Once the assessed residual risks have been identified, assigned relative levels from Very Low to Very High and subsequently prioritized, the TRA team must prepare suitable recommendations for the risk acceptance authority.

Where the assessed residual risks are fully acceptable to the executive team (generally those in the Very Low, Low and possibly Medium ranges), it should suffice to recommend retention of existing safeguards and completion of any security measures pending implementation, with ongoing monitoring of their effectiveness.

In some cases, where assessed residual risks are rated Very Low, it may be feasible to recommend the removal of some protective mechanisms with the acceptance of slightly elevated risk levels to achieve desirable economies or improve operational efficiency.

In cases where the assessed residual risks are unacceptable (generally those in the Very High, High and possibly Medium ranges), some remedial action is usually required. To help select a suitable response, the *Harmonized TRA Methodology* includes an extensive Safeguard Listing which is cross-referenced to the vulnerabilities they correct, the threats they mitigate and the assets (or employees and services) they protect. Furthermore, explicit safeguard selection criteria are explained in detail to facilitate comparative analysis of their relative costs and effectiveness. Finally, assessed residual risks from the Risk Assessment are revised to reflect any improvements expected once the recommendations are fully implemented. In the final TRA report, these are presented as the projected residual risks.

7 Conclusion

7.1 General

The *Harmonized TRA Methodology* describes the TRA as a project conducted in five distinct phases, each of which comprises three or more processes. The relative relationships amongst these phases and processes are illustrated in Figure MS-2.

Some TRA processes may be performed in parallel to improve scheduling and optimize the use of scarce resources. For example, where travel is necessary to collect data regarding assets, employees, services and their values, it simply makes sense to gather local threat data at the same time to avoid another trip. In most cases, however, TRA phases and processes should be completed sequentially because the output from one phase is generally necessary to determine the effort expended in the next. Thus, it may be feasible to commence the Threat Assessment Phase before asset identification has been completed, but the threats of greatest concern will not be fully evident until the assets of greatest value have been identified. Similarly, some generic vulnerabilities may be evident from the start, but others will come to light only after the assets are well understood. Even the threat assessment will drive the Vulnerability Assessment to the extent that more attention is normally devoted to those vulnerabilities most likely to be exploited by the more serious threats. Thus, individual processes within a TRA project are generally conducted in succession, as illustrated in Figure MS-2.

7.2 TRA Projects and Risk Management

The output of a TRA project - the TRA report - is a static document that assesses risk variables at a fixed point in time for a given array of assets in a set configuration. On the other hand, business requirements are not static, so programs, services and the associated assets change over time, as do the threats that may affect them. New vulnerabilities are also discovered on a regular basis, especially with respect to complex information technologies. Therefore, in an inherently dynamic environment like this, continuous risk management is essential.

To meet this fundamental requirement, managers must first monitor the implementation of approved TRA recommendations. Then, as circumstances change, the assessment must be reviewed and updated when risk variables, specifically asset values, threats or vulnerabilities, evolve significantly. A formal TRA methodology simplifies matters considerably, however, because it is not necessary to complete the entire assessment again - only those portions affected by the changes.

The relationships between a TRA project and continuous risk management with the associated decision points are illustrated in Figure MS-3.

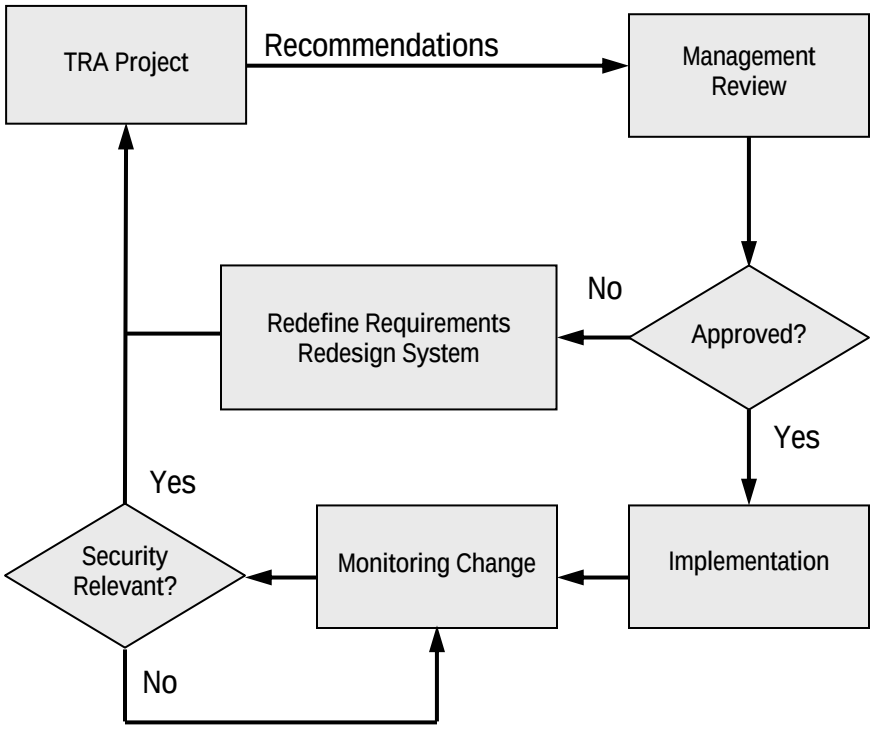

Figure MS-3: (Very) Simplified Risk Management Model

This page intentionally left blank.

Annex A - Preparation Phase

1 Introduction

1.1 General

Almost inevitably, a TRA project will take much longer and cost considerably more than necessary to complete if done without proper planning and preparation. Important inputs may be overlooked, leading to incorrect assumptions and faulty analysis. Essential safeguards may be omitted, leaving employees or assets and related services at risk, while others may be selected inappropriately, thereby imposing needless costs and restrictions on business operations.

To avoid these potential pitfalls, the Preparation Phase of a TRA project includes four important processes leading to one concrete output:

- **Management Commitment –** to ensure that senior management understands both the role of TRAs in support of the Integrated Risk Management Framework and their responsibilities for establishing and approving acceptable levels of residual risk.
- **Mandate of the TRA Project** – to clarify roles and responsibilities, and identify explicitly the risk acceptance authority.
- **Scope of Assessment –** to establish manageable boundaries for the TRA related to the purpose of the assessment and the risk environment.
- **Team Composition –** to assemble the right personnel with the knowledge and skills needed to collect essential information, analyze the data and recommend meaningful solutions to meet business objectives of the organization.
- **TRA Work Plan –** to identify the resources required, assign responsibilities equitably and establish a realistic schedule for TRA activities.

1.2 Aim

The aim of this annex is to describe the four processes and single output of the Preparation Phase of a TRA project.

2 Management Commitment

2.1 General

Successful application of a TRA methodology within a departmental security program and the Integrated Risk Management Framework depends upon the understanding and support of senior management for two primary reasons. Firstly, a broad understanding of the TRA and its role within a comprehensive risk management program is essential for knowledgeable decision making with respect to risk mitigation strategies and specific safeguards to meet business objectives. From an even more practical perspective, the resources required to conduct a TRA

and the cooperation of all parties associated with the assessment may be difficult to obtain without senior management commitment to the process.

2.2 Management Understanding

Government managers are responsible for the safety and security of employees and assets, as well as continued delivery of services. On occasion, the weight of these responsibilities has fostered a culture of risk aversion, an unwillingness to accept any risks that might jeopardize employees, assets or services. Unfortunately, this can lead to missed opportunities for service improvement. In other cases, to reap the benefits of new technologies, some managers have become quite risk tolerant, thereby endangering employees, assets or services. To achieve an effective balance between the two extremes, to avoid undue risk aversion and unwarranted risk tolerance, requires an understanding and acceptance of risk management. More specifically, senior executives and program managers should appreciate:

- the nature and extent of residual risk before it is accepted;
- the role of a TRA methodology as a tool in support of risk management decisions;
- the need for objective analysis to achieve cost-effective business solutions; and
- the value of a transparent audit trail to demonstrate due diligence should risks materialize and injuries occur.

2.3 Resources and Cooperation

Although the *Harmonized TRA Methodology* endeavours to simplify formal TRA processes considerably, the effort can still be significant, especially with larger or more complex facilities and systems. Therefore, adequate personnel and financial resources are essential to conduct an assessment in a timely manner to meet operational objectives. Access to knowledgeable staff and either the facility or system under examination are also necessary to collect the data needed for subsequent analysis. Where senior managers understand and believe in the TRA process as an effective tool to support sound risk management, these issues and other potential problems are less likely to impede a TRA project. In short, sympathetic managers can:

- **Approve/Allocate Resources.** Of course, resource requirements to conduct a TRA project will vary according to the scope and complexity of the effort. Nevertheless, senior managers are more likely to approve personnel and financial resources needed for an assessment when they understand the process and its benefits. This is particularly important in a project environment with severe financial constraints where the TRA may be viewed as a diversion of critical resources from other important activities.
- **Ensure Team Effort.** A healthy tension between project and program authorities can have positive benefits in pursuit of balanced, cost-effective solutions. A similar relationship between security advisors and either program or project staff can be equally beneficial. Unfortunately, the different perspectives of each group can, on occasion, lead to serious friction and a counterproductive waste of energy. With management commitment to the development of cost-effective solutions based on sound risk

management, most differences can be resolved to ensure a concerted team effort towards common goals.

- **Authorize Access to Facilities/Systems.** On site inspections and interviews are often valuable sources of information for an assessment. In some cases, however, they may be considered inconvenient or disruptive to daily operations. It is far easier to overcome these reservations when responsible authorities know the value of the TRA process as an analytical tool to support effective risk management decisions.
- **Promote Information Sharing.** All too often, employees and managers are reluctant to share information across organizational boundaries, especially on subjects as sensitive as threats and vulnerabilities. Since these data are crucial for a reasoned assessment, management support is invaluable to help break down barriers to effective communications and information sharing.

2.4 Practical Considerations

While senior executives understand the Integrated Risk Management Framework as one of the pillars of Modern Comptrollership, many are less familiar with the TRA process as a supporting tool for sound decision-making. Therefore, to achieve the advantages noted above, some practical measures aimed at increasing awareness and acceptance of the TRA may warrant further consideration:

- offering **executive briefings** to explain the *Harmonized Threat and Risk Assessment Methodology*, its relationship with the Integrated Risk Management Framework, and the anticipated benefits of objective analysis to achieve cost-effective solutions[1];
- aligning the TRA methodology with **strategic planning processes** to ensure consistent use at the highest level;
- integrating the TRA methodology with **other management processes**, such as the business planning and system development life cycles, so it becomes simply another routine activity; and
- establishing **clear authorities** in departmental policy to conduct TRAs and resolve any differences arising amongst program, project or security staff.

3 Mandate of the TRA Project

Before commencing a formal TRA project, it is particularly important to establish a clear mandate for the assessment. To that end, the senior executive responsible for the facilities, services or IT systems under review would normally identify an appropriate TRA team leader based on several factors examined in sections 5.3 and 5.4.7 below. This individual should be provided with explicit instructions:

- assigning authority to conduct the TRA project;

[1] The **Executive Overview** situates the TRA process within Modern Comptrollership for the benefit of senior audiences. As indicated in the Introduction, CSE and the RCMP have also developed a briefing package suitable for senior managers and executives.

- explaining management expectations regarding residual risk and business priorities; and
- prescribing roles, responsibilities, reporting relationships and approval authorities for the TRA Work Plan and the outputs from each subsequent phase of the project, especially the risk acceptance authority for the final TRA Report.

Later, these instructions should be incorporated in the TRA Work Plan.

4 Scope of Assessment

4.1 General

Before commencing a TRA project, it is particularly important to determine the scope of the assessment, to decide which employees, assets and services will be examined and at what level of detail. Unless realistic bounds are set at the start, subsequent data collection and analysis could become open-ended and the project might collapse under the sheer weight of the effort. The other extreme can also arise where the assessment is performed at such a high level that significant questions remain unanswered and residual risks are not fully understood. To avoid these potential problems, both the breadth and depth of the assessment should be clearly established as the first step of the initial planning process.

4.2 Planning Factors

4.2.1 Overview

To ensure consistency amongst TRA reports, several factors should be considered during the scoping exercise, including the purpose of the assessment, the stage in a project plan or system development life cycle, the risk environment, and practical concerns of cost or time constraints.

4.2.2 Purpose of the Assessment

TRA reports serve many different purposes ranging from broadly-based, high-level assessments to very tightly focused examinations of specific security concerns. In each case, the scope of the assessment should be adjusted to suit the stated purpose and, as indicated in section 6, the Purpose of the Assessment should be stated clearly in the TRA Work Plan. Some of the more important reasons for conducting a TRA include:

- **Departmental Assessments.** Given the size and complexity of many government institutions, departmental assessments are generally conducted at a very high level of detail where the scope is, of necessity, very broad but relatively shallow, to concentrate on strategic risks related to major business lines and the related asset groups. Although they lack the detail of more focused TRA reports devoted to a single facility, network or service, departmental assessments are very useful for establishing a solid foundation for the overall security program, prioritize individual TRA projects and establish a broad contextual framework for their review.
- **Major Crown Projects (MCP).** MCPs are, by definition, those with a projected total cost in excess of $100 million or those identified by the Treasury Board Secretariat in accordance with the *Major Crown Project Policy*. With expenditures in this order of

magnitude, the associated TRA projects tend to be the largest and most complex. Their scope is generally both broad and deep in order to identify relevant risks and the mitigating safeguards at a fairly granular level of detail. Although the effort may be onerous, more complete and rigorous analysis is generally appropriate in order to determine the most cost-effective suite of security measures. Since safeguards typically account for five to ten percent of the total project cost, even a small adjustment in the recommended security features could lead to considerable savings, thereby justifying the effort expended on a more detailed formal assessment.

- **New Facilities.** Whenever a new facility is to be acquired or constructed, it could be the subject of two different assessments. The first, usually much shorter, concentrates on the business and threat profiles of the organization to be relocated in order to determine the security criteria for evaluating proposed sites for the new facility. This tightly constrained TRA project, known as a **Security Site Brief**, supports the identification and selection of a location that can be properly secured most effeciently and cost-effectively. The second type of TRA project, normally a much lengthier effort, includes a detailed examiniation of the business and threat profiles of the organization, as well as local conditions that might contribute to threats or vulnerabilities. The aim of this analysis is to identify appropriate physical security measures for the chosen site. Recommendations in the form of **Security Design Briefs** may vary from highly conceptual at the beginning of a project to very detailed at the end to suit the facility design methodology. Thus, for larger facilities, the scope of an iterative TRA project can be as extensive as that for an MCP, especially when the facility design process has not benefited from a Security Site Brief.

Security Site Brief
A document which describes the *physical security* attributes sought in a site when relocating the facility.

Security Design Brief
A document which describes the physical protection philosophy and concepts as well as physical safeguards for a facility.

RCMP Physical Security Guide G1-005
Guide to the Preparation of Physical Security Briefs
January 2000
www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_e.htm

- **New Systems.** Clearly, the size and complexity of a system will drive the scope of the assessment. More complex assets are inherently more vulnerable, so the analysis should be conducted at a more granular level of detail to assess potential risks more precisely. With inter-networked systems, there may be a tendency to extend the breadth of the TRA project to cover all interconnected elements. To avoid an overwhelming effort and a cumbersome final report, it is frequently preferable to subdivide the workload into several modular assessments of more modest scope, each devoted to a single network segment, application or business function, as illustrated in Figure A-1.
- **Facility/System Upgrades.** As facilities or systems evolve, their TRA reports should be updated to account for significant security changes. In this case, the scope of the assessment may be restricted to those variables (asset values, threats and vulnerabilities) that actually differ from the original configuration identified in the previous assessment. Except in the case of a major overhaul or upgrade, the follow-up effort to maintain the

currency of TRA reports as part of an overall risk management program may be reduced considerably with a carefully structured process like the *Harmonized TRA Methodology*.

- **Specific Security Concerns.** Some of the most powerful and cost-effective TRAs are those intended to address specific security concerns, often a single issue or question such as the need for duress alarms and bullet-proof glass in a client-service booth or the requirement for emission security for equipment at a specified location. In most cases, the scope of the assessment may be extremely focused to concentrate on a handful of assets, threats, vulnerabilities and prospective safeguards, so the analysis may be completed very quickly and the final recommendations can be presented in a few pages.[2]

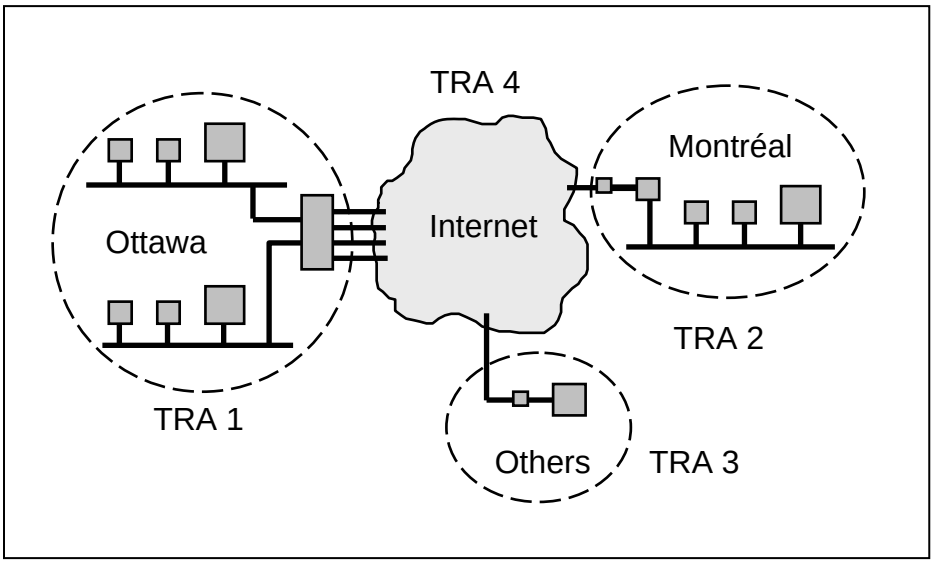

Figure A-1: Dividing an Inter-Networked System into Modular TRA Projects

4.2.3 Stage of Development

Typically, projects for both facilities and systems evolve from initial conception through requirements definition, design and development to final implementation in accordance with a project plan or system development life cycle. As a general rule, separate TRA reports should be prepared at each step of the way to support informed decision-making and design choices. At first, very little will be known about the ultimate deliverables so, of necessity, the scope of the preliminary assessment will be very general. As the project matures, however, and more details are settled, the subsequent iterations of the analysis will increase in depth, if not in breadth. Of course, the extent of the final TRA report will depend very much on the size and complexity of the facility or system in question. Appendix A-1 provides more detailed guidance on the integration of TRA projects into a generic project or system development life cycle.

[2] In fact, Appendix F-7 presents a very focused example as a Sample TRA Report to determine the requirement for emanations security measures to safeguard Protected C at a national facility in Canada.

4.2.4 Risk Environment

An informal assessment or cursory scan of the risk environment is often very useful to better define the scope of a TRA project. In general, riskier situations warrant more rigorous analysis to achieve a higher level of assurance that the security posture is, in fact, adequate. To amplify this basic principle, more valuable assets should be identified in greater detail, as should more serious threats and vulnerabilities. Conversely, less effort need be expended on the examination of lower value assets, less significant threats and more obscure vulnerabilities. Of course, this implies that the granularity of analysis should not necessarily be homogeneous throughout a given TRA project. The greater effort should always be devoted to the more important issues, the ones that generate the greatest risks.

4.2.5 Some Practical Considerations

Almost inevitably, some other practical considerations may influence the scope of a TRA. The availability of baseline security standards, for example, can simplify matters considerably, whereas cost, time and resource constraints can have a negative impact, namely:

- **Security Standards.** In cases where baseline security standards provide adequate direction and guidance to achieve an acceptable security posture, it may be possible to shorten the assessment considerably. That being said, an informal TRA is almost always necessary to determine whether or not baseline security standards offer sufficient protection. More often than not, existing security standards will address only some of the issues, so a formal TRA project will be required to cover the gaps. Nevertheless, the judicious application of various standards and other risk management techniques explored in Appendix A-2 can help to reduce the scope of the assessment and, therefore, the associated workload.
- **Cost, Time and Resource Constraints.** With proper planning and management support, sufficient time and resources should be set aside to perform essential TRAs. Nevertheless, scheduling pressures and cost constraints may arise for a variety of legitimate reasons. For example, unexpected shifts in operational priorities, sudden opportunities to improve service delivery, rapidly emerging threats and previously unforeseen vulnerabilities may require a quick response with too little time for more rigorous analysis. In cases like these, a higher level assessment with narrower scope may have to suffice pending more detailed analysis as time and resources permit. To obtain the best results, the abbreviated TRA report should concentrate on the most serious risk variables, namely the most valuable assets, the highest threats and the most significant vulnerabilities, albeit at a higher level of detail.

4.3 Summary

To achieve greater flexibility and responsiveness, a shorter assessment is generally preferable to an unmanageable exercise of massive proportion. In this regard, limiting the scope of a TRA project to concentrate on the essentials is one key to success. Larger facilities or systems may be decomposed into smaller components for analysis. Within a given TRA, the level of detail need not be constant, so less effort is expended on the evaluation of lower value assets, unlikely threats and insignificant vulnerabilities. Finally, the scope of a TRA may change during the

course of the assessment, as new threats or vulnerabilities are discovered or new assets are added to the mix.

The actual length of any TRA report will depend on many different variables, such as the complexity of the assets and services involved, the severity of the risk environment and the purpose of the assessment. Clearly, the document should be as long as necessary to convey the findings and recommendations to the risk acceptance authority. With that in mind, Table A-1 provides a very general indication of length of a typical TRA report. Exceptions to these norms may be expected but, wherever possible, they should be shorter rather than longer, consistent with the established purpose of the assessment.

Purpose of the TRA Project	Typical Length (pages)
Departmental Assessment	5-10
Major Crown Project	100-1,000+
New Facility: Site Brief	10-20
New Facility: Design Brief	50-75
New System	50-100
Facility/System Upgrade	5-75
Specific Concern	2-20

Table A-1: Typical Length of a TRA Report

5 TRA Team Composition

5.1 General

Once the scope of the assessment has been established, a suitably qualified team must be assembled to collect and analyze relevant data, and propose realistic solutions to meet business requirements. Without the right mix of personnel representing both operational interests and security considerations the results of the TRA project might be skewed, even inadvertently, to reflect narrow, parochial concerns.

5.2 Team Size

While it is feasible for a single individual to compile a TRA report, most assessments will require a team effort to understand all of the issues, collect essential data and achieve timely results. Some of the more important factors to consider when determining the size and composition of the team required to conduct a specific TRA project include:

- **Scope of the Assessment.**[3] More tightly focused assessments, especially those addressing a single issue or limited set of problems, generally require fewer resources, perhaps even one person. Conversely, to conduct a comprehensive evaluation of a major Crown project in a timely manner a much larger team may be necessary, occasionally as many as five or more specialists with different backgrounds. Teams of two or three are normally sufficient for other TRA projects that fall between these two extremes, provided that other resources with specific expertise are available for consultation when required.

[3] **Section 4.1** examines several factors governing the scope of an assessment.

- **Complexity of the Assets.** In order to understand the many nuances of extremely complex assets or business processes, a larger team may be needed to muster essential knowledge and experience to analyze the situation effectively. Again, access to suitable subject matter experts on a part-time basis may suffice to minimize the demands upon scarce technical resources.
- **Urgency of the Situation.** Where time is of the essence, a larger team might be assembled to complete the analysis as quickly as possible. There are practical limits, however, as larger groups can become unwieldy. Anything over ten team members may become counterproductive.
- **Distribution of the Assets.** Where assets are distributed over a wide area, the team might be enlarged to include personnel at each site to save travel time and costs. In this case, careful coordination is imperative to ensure consistent results for each location.
- **Availability of Qualified Personnel.** With highly qualified personnel, a smaller team is normally practicable. On the other hand, additional support may be necessary on a full or part-time basis to help less experienced staff complete a TRA project within the expected time frame and at an appropriate level of detail.

5.3 Team Qualifications

To conduct an assessment as quickly and efficiently as possible, more experienced and knowledgeable team members are preferable to complete novices. As a general rule, however, at least one member of a well-balanced team should possess the following minimum qualifications:

- an **intermediate understanding of the TRA process** based upon a combination of formal training[4] and practical experience, normally achieved by participating in two or three previous assessments;
- a **detailed understanding of the operational requirements** for the assets under examination, or at least immediate access to responsible business managers;
- a **thorough understanding of baseline security standards and other safeguards**, or at least full support from departmental security, and facility management or IT authorities, depending upon the subject of the assessment; and
- **both the authority and security screening levels** required to access relevant information and facilities.

5.4 Core Team Members

5.4.1 General

To meet minimum qualifications noted above, the core team members should include either full or part-time representatives from three or four different groups, depending upon the subject matter of the assessment. Each can offer an important perspective and key data for the TRA project.

[4] The **Foreword** points to some of the training options.

5.4.2 Business Line Managers

Program managers responsible for the business line under assessment are uniquely qualified to identify all but the more technical assets and determine their values based upon the likely operational impact of a compromise. With an understanding of the corporate culture, line managers are also well situated to advise senior executives on acceptable levels of residual risk in the final recommendations.

5.4.3 Project Managers

In a project environment, for either facilities or systems, project managers and their staff can identify the more technical assets, many of their vulnerabilities, the proposed safeguards and potential alternatives if necessary. Their input to the recommendations and their overall agreement with the proposals are crucial to a successful TRA report.

5.4.4 Facility Managers

For TRA projects involving government buildings and other public works, facility managers can identify many structural and environmental assets, local threats based upon guard reports and alarm logs, some technical vulnerabilities associated with the fabric of the building and its location, and many of the physical security measures. Often, they can provide architectural drawings and floor plans to help delineate the scope of the assessment, illustrate many assets in situ and facilitate subsequent analysis of suitable alternatives for the final recommendations.

5.4.5 IT Authorities

At a strategic level, Chief Information Officers (CIOs) and their staff can identify IT assets, especially the underlying infrastructure and important linkages with other systems. From a more tactical perspective, the contributions of systems administrators can be particularly valuable, ranging from increasingly detailed descriptions of IT assets and their actual configuration, to actual threats based on system logs, known or suspected vulnerabilities and current technical safeguards.

5.4.6 Security Authorities

The GSP and supporting documentation require departments to appoint three principal security advisors, namely a Departmental Security Officer (DSO),[5] an IT Security Coordinator (ITSC)[6] and a Business Continuity Planning Coordinator (BCPC).[7] DSOs and their staff can contribute materially to virtually all TRAs, while ITSCs should participate in all involving IT assets; and BCPCs to those regarding critical assets or services. More specifically, these authorities provide the following support:

- **DSO –** interprets the GSP and supporting documentation for departmental use; provides advice and guidance on the TRA process generally; contributes to the threat and vulnerability assessments based upon incident reporting and internal investigations; and suggests suitable safeguards for the final recommendations.

[5] **Section 10.1 of the GSP** requires the appointment of a DSO.

[6] **Section 9.1 of the Management of Information Technology Security Standard (MITS)** requires the appointment of an ITSC.

[7] **Section 3.1 of the Operational Security Standard – Business Continuity Planning (BCP) Program** directs the appointment of a BCPC.

- **ITSC –** interprets IT security standards for departmental use; offers input regarding technical threats and vulnerabilities; and suggests suitable technical safeguards for the final recommendations.
- **BCPC –** interprets BCP Program standards for departmental use; may provide relevant Business Impact Analyses (BIAs) to identify critical assets and services; offers input regarding the threats and vulnerabilities that may affect these assets and services; and suggests suitable business continuity plans, measures and arrangements, where appropriate, for the final recommendations.

5.4.7 Overall Coordination

Depending upon the purpose of the TRA project, any one of the core team members might coordinate the overall assessment, but each will have a different focus. Program managers are more likely to concentrate on business requirements, a paramount consideration. Project managers are frequently driven by cost and scheduling constraints and might, therefore, question the need for expensive safeguards. IT authorities, including the ITSC, have a better understanding of many technical issues, but may lose sight of personnel and physical security measures so important to comprehensive solutions. Conversely, the DSO has a broad understanding of the entire departmental security program, but not necessarily the technical depth for certain IT security assessments. While all of these factors should be considered when selecting a team leader, the most important issue is that of impartiality: to meet their obligations under the GSP and Modern Comptrollership deputy heads and their executive teams require objective assessments that can withstand even public scrutiny and demonstrate due diligence in the event a threat should materialize and compromise assets of value. With that in mind, the office of the DSO, as an impartial third party, should work closely with the assigned team leader to monitor and advise on the quality and completeness of the analysis.

5.5 Other Resources

5.5.1 Internal Resources

Many more departmental resources might be consulted during the course of a TRA project to obtain specialized information, advice and assistance as required:

- **ATIP Coordinators –** to help determine asset values, especially the access and privacy dimensions of information assets and, where available, provide copies of relevant Privacy Impact Assessments (PIAs) for similar purposes.
- **Finance –** to help identify financial assets and their values, as well as losses to the Crown reported in accordance with Treasury Board policies[8] as potential threat indicators.
- **Human Resources –** to explain personnel issues, identify employees at risk of violence, and suggest staff relations concerns that may indicate internal threats or vulnerabilities.
- **Internal Audit –** to share departmental audits and reviews that monitor compliance with security policies and standards as a measure of safeguard effectiveness and vulnerability.

[8] The **Policy on Losses of Money and Offences and Other Illegal Acts Against the Crown** requires departments to investigate and report all losses of money and allegations of offences, illegal acts against the Crown and other improprieties, all of which are useful indicators of threat activities.

- **Legal Counsel –** to interpret legal obligations and liabilities and, in particularly risky situations, review TRAs to assess their adequacy as records of due diligence.
- **Material Management –** to identify certain physical assets and their values based upon inventory records.
- **Occupational Safety and Health –** to provide information on hazards in the workplace for the threat assessment and suggest relevant safeguards for the recommendations.

5.5.2 External Resources

Some external resources of potential value to a TRA team include:

- **Lead Security Departments** designated by TBS,[9] especially –
  - **CSE –** for advice and guidance on the *Harmonized TRA Methodology* and technical threats, vulnerabilities and safeguards affecting IT systems.
  - **CSIS –** for an assessment of threats identified in the *CSIS Act*.
  - **PSEPC –** for advice and guidance on Business Continuity Planning and critical infrastructure protection, including Alerts, Advisories and Information Notes on potential, imminent or actual threats, vulnerabilities or incidents affecting the government of Canada or other sectors of the national critical infrastructure.
  - **PWGSC –** for advice and guidance on the security of IT systems and facilities for which it is common service provider and custodian respectively.
  - **RCMP –** for advice and guidance on the *Harmonized TRA Methodology*, all matters of physical security, criminal threats and technical threats, vulnerabilities and operational aspects of IT security.
- **Other Public Sector Authorities**, such as provincial and municipal police forces, fire departments and public utilities, which can provide valuable information regarding environmental assets, local threats and some vulnerabilities, as amplified in Appendices B-1, C-1 and D-1 respectively.
- **Private Sector Organizations**, such as the insurance industry, product vendors, professional associations and research institutes, which can also provide valuable information regarding various assets, threats, vulnerabilities and safeguards, as indicated in Appendices B-1, C-1, D-1 and F-1 respectively.
- **Private Consultants** who may be contracted for technical expertise to augment departmental resources or even conduct complete TRA projects. The use of consultants offers several advantages, albeit with some potential pitfalls. Appendix A-4 explores many of these issues in greater detail and presents some best practices to achieve more consistent results. Then, Appendix A-5 provides a sample Statement of Work for TRA consulting services as a model for departmental use.

[9] **Section 4 of Appendix A to the GSP** provides a fuller description of the roles and responsibilities of all security lead departments.

6 TRA Work Plan

Except in the case of the shortest, simplest assessments, most TRA projects will benefit significantly from a formal work plan. Although the actual length and level of detail will vary according to the scope and complexity of the assessment, a typical work plan should include:

- some **Background** material to situate the assessment within a departmental context;
- a clearly stated **Aim** or purpose of the TRA project, generally in a single sentence;
- a statement of **Scope** to identify the subject of the assessment and delineate the boundaries of the analysis;
- any **Limitations** or restrictions on the TRA, such as cost or time constraints;
- the **Target Risk Level** that is deemed acceptable;
- the **Team Composition** with terms of reference for each member;
- all **Logistic Arrangements** such as –
    - security screening requirements,
    - access requirements to facilities and data, both physical and logical,
    - travel arrangements and visit plans,
    - administrative support,
    - other resource requirements for accommodations and office equipment,
    - an itemized budget,
    - Statements of Work for consulting services (if applicable);
- A list of potential **Input Documentation** such as design documents, facility plans, MOUs for the sharing of information and other assets, and earlier TRA reports;[10]
- planned outputs or **Deliverables**, specifying the TRA methodology to be employed, the format for both electronic and hard copies of the final TRA report and the channels for its final submission; and
- the project **Schedule** listing activities with start and completion dates for each phase of the assessment and all of the associated deliverables.

7 Approval

In general, the senior manager who will review the recommendations in the TRA should approve the work plan before the team is assembled and data collection commences.

Finally, Appendix A-6 presents a Sample TRA Work Plan with detailed instructions for its completion.

[10] Fuller lists of potential source material are presented in Appendices B-1 for assets, C-1 for threats, D-1 for vulnerabilities and F-1 for safeguards.

This page intentionally left blank.

Appendix A-1 - TRAs in a Project Plan/System Development Life Cycle

1 Introduction

1.1 General

A single TRA project may be conducted to assess the risks associated with existing facilities, systems or services. Unless security concerns were addressed throughout their development, however, many of the residual risks calculated in the Risk Assessment Phase are likely to be unacceptable, leading to extensive and frequently expensive proposals for remedial action in the Recommendations Phase.

In order to avoid the difficulties of retrofitting safeguards to existing assets, iterative threat and risk assessments should be conducted at each step of the project plan or system development life cycle. This approach permits early identification of potentially dangerous risks and reasonable design alternatives to achieve business objectives with the most cost-effective security solutions.

1.2 Aim

The aim of this appendix is to provide some guidance on the integration of TRA reports into a project plan or system development life cycle.

2 Stages in a Project Plan/System Development Life Cycle

2.1 Project Planning Options

All major projects for business process re-engineering and facility or system design should be conducted in sequential stages or phases from initial conceptualization to operational deployment (and even final disposal). Various professional disciplines have defined different but basically similar models for project planning and system development. Some specific examples include:

- several representative project life cycles listed in the *Project Management Body of Knowledge (PMBOK®)*;
- a security system design process described in section 1.2 and Figure 2 of G1-005, *Guide to the Preparation of Physical Security Briefs*, published by the RCMP; and
- a generic system development life cycle examined in section 2.1.1 of MG-2, *A Guide to Security Risk Management for Information Technology Systems*, issued by CSE.

2.2 Project Life Cycle

One of the representative project life cycles identified in the *Project Management Body of Knowledge (PMBOK®)* for defence acquisition includes the following four phases:

- **Concept and Technology Development –** initial studies through concepts of operation to selection of a system architecture;
- **System Development and Demonstration –** system development, integration and demonstration in an operational environment;
- **Production and Deployment –** full scale manufacturing and installation; and
- **Support –** ongoing management and adjustment.

2.3 Facility Design Process

In G1-005, *Guide to the Preparation of Physical Security Briefs*, the RCMP describe a six-stage security system design process for government facilities as follows:

- **Planning Stage –** definition of operational needs and a safeguarding strategy;
- **Definition Stage –** analysis of site and facility attributes consistent with the safeguarding strategy;
- **Implementation Stage –** design the facility and install safeguards to ensure compliance with the safeguarding strategy;
- **Commissioning Stage –** inspect the facility to ensure compliance with the safeguarding strategy;
- **Operation Stage –** monitor operations to ensure continued compliance; and
- **Evaluation Stage –** assess the project against performance criteria and adjust safeguards accordingly.

2.4 System Development Life Cycle

In MG-2, *A Guide to Security Risk Management for Information Technology Systems*, CSE presents a six-stage system development life cycle as follows:

- **Planning for Change Stage –** examination of alternatives with the associated risks, and decision whether or not to proceed with the project;
- **Requirements Definition Stage –** determination of operational or business needs and related security functional requirements;
- **Architecture Design Stage –** identification of secure system options and selection of the preferred architecture;
- **Detailed Design Stage –** development of design specifications and specific safeguards to satisfy the system security policy and functional requirements;
- **Implementation Stage –** completion of acquisition, installation and testing; and
- **Operational Stage –** commencement of operations with ongoing maintenance and review to maintain security posture.

2.5 Summary

While there are many more project or facility planning and system development models, the three examples described above illustrate the logical flow from high level options analysis through increasingly detailed requirements definition, design, development, testing and operational deployment. Table A1-1 underlines the relative similarities amongst these processes.

Project Life Cycle	Facility Design Process	System Development Life Cycle
Concept and Technology Development	Planning Stage	Planning for Change Stage
	Definition Stage	Requirements Definition Stage
		Architecture Design Stage
System Development and Demonstration		Detailed Design Stage
Production and Deployment	Implementation Stage	Implementation Stage
	Commissioning Stage	
Support	Operation Stage	Operational Stage
	Evaluation Stage	

Source Documents		
A Guide to the Project Management Body of Knowledge (PMBOK ® Guide)	G1-005, *Guide to the Preparation of Physical Security Briefs*	MG-2, *A Guide to Security Risk Management for Information Technology Systems*

Table A1-1: Relative Stages in a Project Plan and System Development Life Cycle

3 Implications for TRA Reports

3.1 Rationale

Whatever project planning methodology or system development life cycle is selected to manage the design and deployment of a new facility, system or service, certain fundamental principles should govern the associated TRA activities. In fact, without a clearly defined relationship between project and security risk management functions, serious threats and vulnerabilities may be overlooked and essential safeguards might be neglected, thereby leading to unacceptable but largely unrecognized residual risks. Any attempt to correct security flaws after a new facility is occupied or a system has been installed is likely to fail or, at least, introduce exorbitant costs.

3.2 Basic Principles

3.2.1 Early Involvement

Firstly, and most importantly, TRA processes should be initiated in the earliest phases of a project, at the conceptual or planning stage. Of course, the first assessment will be a high level review because many assets and their associated vulnerabilities cannot be identified until

detailed designs emerge later in the project life cycle. Nevertheless, the initial TRA report can influence the direction of a project, helping to identify and avoid riskier options or alternatives.

3.2.2 Iterative Analysis

In each successive stage of the project plan or system development life cycle, more details will be captured regarding assets, their values, related threats and associated vulnerabilities. Therefore the residual risk may be assessed with greater precision and certainty at each step of the way, as illustrated in Figure A1-1.

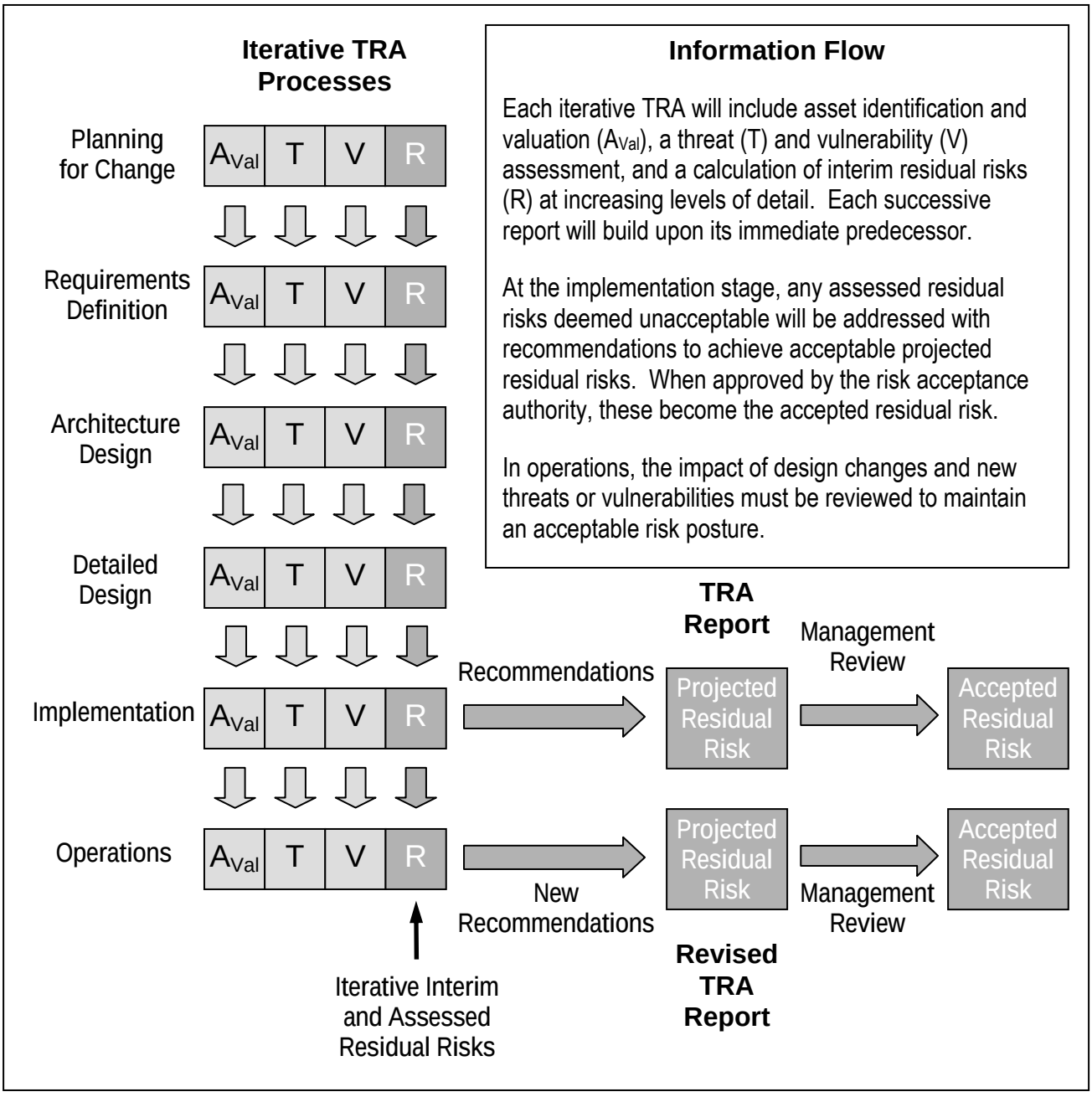

Figure A1-1: TRA Information Flows in a Project Environment

3.2.3 Interim Approval

The objective of interim TRA reports is to identify potentially unacceptable residual risks and suggest cost-effective security solutions before any irrevocable design choices are made by the project team. Both project and program managers should review and approve the recommendations in each successive TRA report, or request proposals for suitable alternatives.

3.3 Prospective Benefits

The benefits of tightly integrated project planning, system development and risk management methodologies include increased assurance of responsible decision making with a visible audit trail and clear rationale for design choices to demonstrate due diligence should risks materialize.

This page intentionally left blank.

Appendix A-2 - Security Standards versus Threat and Risk Assessments

1 Introduction

1.1 Government Security Policy (GSP) Requirements

At the highest level of abstraction, risk management is nothing more than a systematic response to uncertainty. From a security perspective, this uncertainty arises from the interaction of several independent variables, some of which are particularly difficult to assess. More specifically, risk management in a security context is an attempt to address the negative consequences of a threat agent exploiting some vulnerability to affect an asset of value adversely. In essence, risk (**R**) may be described as a functional relationship amongst asset values ($\mathbf{A_{Val}}$), threats (**T**) and Vulnerabilities (**V**):

$$\mathbf{R = } f \mathbf{(A_{Val}, T, V)}$$

Although this functional relationship is widely accepted, risk management has been the subject of heated debate in security circles. Different communities of interest have espoused different analytical approaches. Some, for example, preferred qualitative techniques, while others sought quantitative measures. Some endorsed rules-based solutions, while others conducted case studies. Despite a wealth of informed discussion and documented research, no single approach has emerged as a clear choice for security professionals.

While varied options may provide valuable flexibility, too many choices can breed confusion. Therefore, to minimize uncertainty and establish common approaches amongst federal departments and agencies, the Government Security Policy prescribes two options for risk management with the policy statement:

> "Assets must be safeguarded according to baseline security requirements and continuous risk management."[1]

In Appendix B to the policy, the Glossary, "baseline security standards" are defined as: "mandatory provisions of the Government Security Policy and its associated operational standards and technical documentation." Section 9 of the policy provides further amplification, describing a hierarchy of supporting documentation, while Appendix A assigns specific responsibilities for the development of security standards, both operational and technical, to designated lead security departments.

[1] **Section 4 of the GSP**.

For security risk management, the policy directs departments to "conduct ongoing assessments of threats and risks to determine the necessity of safeguards beyond baseline levels."[2] A four-step threat and risk assessment (TRA) process is defined to meet this directive. Appendix A also identifies lead agencies with specific responsibilities for advice and guidance on both the TRA process and the data necessary to conduct an assessment. Finally, supporting documentation, specifically the Identification of Assets and Security Risk Management Operational Security Standards provide further details on this particular approach to risk management.

Although the GSP clearly identifies the TRA as an important supplement to baseline security standards in a comprehensive risk management program, additional guidance on the relative merits of the two methods and their application in different circumstances may be useful. At the same time, some other alternatives may warrant further consideration.

1.2 Aim

The threefold aim of this appendix is to:

- describe various options for rational and responsible risk management;
- assess the relative strengths and weaknesses of each approach; and
- suggest specific situations or circumstances where each technique is more appropriate.

2 Approaches to Risk Management

2.1 General

While the variety of risk management methodologies is potentially unlimited, many options are substantially the same or simply variations on a common theme. To provide a meaningful framework for analysis, two underlying characteristics are identified to distinguish between four different techniques. The analytical complexity of a risk management tool will determine the relative expertise required to complete an assessment, as well as the time and cost of the effort. From a different perspective, some approaches are more intuitive or subjective in application while others are more objective in nature. Based on these distinguishing characteristics, the balance of this appendix will examine four different methods illustrated in Figure A2-1, namely an informal or cursory TRA, the use of subject-matter experts, the application of security standards and a comprehensive or formal TRA, only the last two of which are fully recognized and endorsed by the GSP.

[2] **Section 10.7 of the GSP**.

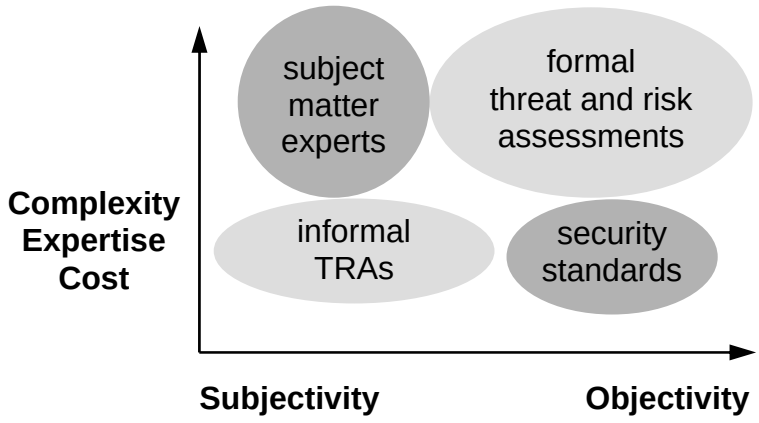

Figure A2-1: Risk Management Methodologies

2.2 Informal Threat and Risk Assessments

Intuitively, human beings make important, even critical decisions regarding their personal safety and well-being on a regular basis. From simple situations, like crossing a busy street, to more complicated problems involving financial security or health care, individuals assess the risks and choose a course of action. Often these choices are made very quickly, almost unconsciously, with little formal analysis.

At first glance, this minimalist approach to risk management might appear completely irresponsible, implying a lack of awareness or even an unwillingness to acknowledge real threats and vulnerabilities. This is almost certainly the case if the choice is entirely unconscious or purely arbitrary. However, intuitive logic like this may be perfectly reasonable where the actual risks are relatively low, in other words, where asset values or related vulnerabilities are modest and the relevant threats are either non-existent or at least highly unlikely.

By way of illustration, following limited analysis, even a conscientious risk manager might ignore flood protection for a government facility located at the top of a hill. Widespread Internet connections to departmental networks provide less trivial examples. Despite known threats and vulnerabilities, these links may be fully justified where confidentiality, availability and integrity concerns are very low. In short, an informal approach to risk management on the basis of a cursory TRA may be perfectly acceptable and entirely reasonable under the right conditions, where known risks do not merit the added expense and effort of more rigorous analysis.

2.3 Subject-Matter Experts (Delphic Wisdom)

According to ancient Greek mythology, the Oracle of Delphi could provide mere mortals with sage advice and guidance. Unfortunately, these prophecies were often obscure, ambiguous or enigmatic and, therefore, subject to misinterpretation and misapplication.

In a modern parallel, even the wisest counsel of acknowledged security experts may be equally incomprehensible to the uninitiated. All too often, reports abound with technical jargon and obscure details, some of which may confuse and confound program authorities.

Despite these difficulties, current experience with real issues and practical problems can provide a powerful basis for effective risk management. While one knowledgeable advisor might suffice, confidence levels in a proposed solution are likely to increase significantly as more subject-matter experts are involved to assess security requirements and propose viable safeguards. Almost invariably, the product of these deliberations is presented in a written report, normally in the form of a narrative assessment with specific recommendations. Although the output is generally subjective in nature, most professionals will include a variety of supporting material in data, charts, tables and costing models to justify the proposed security measures.

2.4 Security Standards

Security standards mandated by the GSP appear in a compendium of subordinate documentation introduced in Section 9. This important reference is amplified in Section 2 of the Security Organization and Administration Standard which describes both the hierarchy of documentation, illustrated at Figure A2-2, and a detailed process for its development, approval and promulgation. The hierarchical structure is particularly sound and logical because the security discipline is simply too complex to capture in a single policy, however voluminous and cumbersome. An array of increasingly detailed publications, ranging from the actual GSP through six operational standards to a veritable library of technical documentation is a more practical and realistic approach to present baseline security standards.

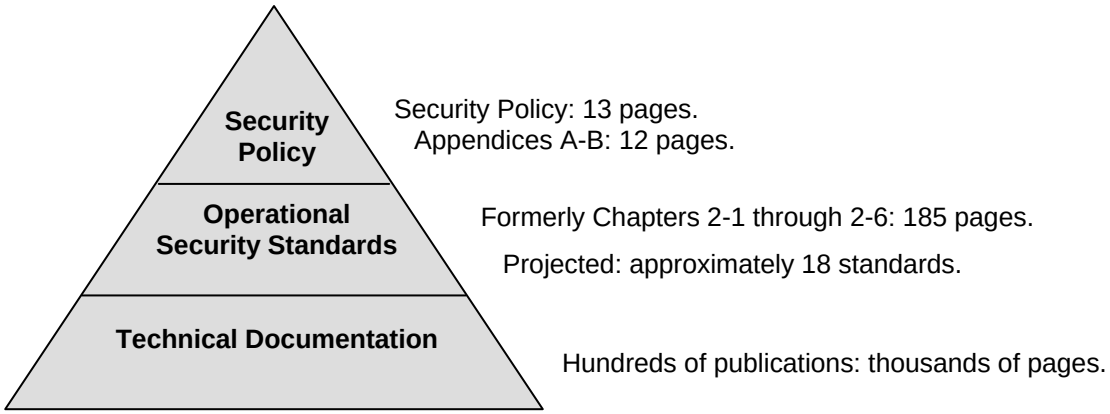

Figure A2-2: Hierarchy of Security Documentation

In the context of the federal government, three lead agencies in particular, namely the Communications Security Establishment (CSE), Public Safety and Emergency Preparedness Canada (PSEPC) and the Royal Canadian Mounted Police (RCMP), have been assigned specific responsibilities for the development of technical standards on physical and IT security, and business continuity planning.

In general, these standards prescribe certain safeguards, or combinations of protective mechanisms, for specific assets, depending upon their value and, to a lesser extent, the threat environment and their vulnerability. The recommended schedule for changing passwords provides a simple example. For access to Top Secret information, passwords should be replaced monthly. For Secret and Confidential, quarterly changes are indicated, whereas biannual updates suffice for Protected (formerly designated) material.[3] In effect, the graduated response is based solely on asset value, with no consideration for either vulnerabilities or the immediate threat environment. Other standards, like those related to physical and IT security zones, offer an array of technical safeguards to address increasing operational vulnerabilities. Trade-offs like these are common elements of many security standards.

2.5 Formal Threat and Risk Assessments

A formal threat and risk assessment is a viable alternative to the straightforward application of security standards. As defined in the Security Organisation and Administration Standard at a higher level of abstraction, the process seems relatively simple and intuitively satisfying, and comprises four basic steps:

- **Initial Planning and Statement of Sensitivity** – establishing the scope of the assessment and identifying the employees and assets to be safeguarded.
- **Threat Assessment** – determining the threats to employees and assets in Canada and abroad, and assessing the likelihood and impact of threat occurrence.
- **Risk Assessment** – assessing the risk based on the adequacy of existing safeguards and vulnerabilities.
- **Recommendations** – implementing any supplementary safeguards that will reduce the risk to an acceptable level.

Each step is hardly a trivial exercise, however, so the responsible lead agencies have produced an array of documentation to amplify the fundamental provisions of the GSP and the Security Risk Management Operational Security Standard, most of which have been superseded by the *Harmonized Threat and Risk Assessment (TRA) Methodology*. Similar publications abound in the private sector, as do a number of automated tools to help establish a structured approach to the collection and analysis of relevant data.

3 Relative Merits

3.1 General

Each approach to risk management has intrinsic strengths and weaknesses arising from their relative complexity, implementation costs, accuracy and availability in different circumstances.

[3] **Section 8.2(6) of the *Technical Security Standard for Information Technology (TSSIT)*** formerly issued by the RCMP and still available at: http://www.rcmp-grc.gc.ca/tsb/pubs/it_sec/tssit97_e.pdf.

A basic understanding of these issues is essential to an informed decision regarding the particular methodology most appropriate to a given situation.

3.2 Informal Threat and Risk Assessments

3.2.1 Advantages

Quite clearly, the informal or cursory TRA offers several important benefits because it is by far the simplest. Almost invariably, it is the easiest to apply and the least time-consuming, thereby minimizing costs and demands upon scarce security specialists. Despite the abbreviated analysis, the results can be quite accurate and fully replicable when supported by an accurate, high-level Statement of Sensitivity and threat assessment. If all decisions are formally recorded, ultimate accountability is fully evident.

3.2.2 Disadvantages

In order to avoid expensive safeguards, some managers have been tempted to apply informal techniques where they are inappropriate, even dangerous, in situations where risks are truly significant and should not be ignored. In short, misapplication of the method and misrepresentation of the results are the greatest dangers or disadvantages associated with a minimalist methodology. Other potential problems arise from failure to record important decisions. Without formal documentation, it may be difficult to demonstrate due diligence and accountability in the event of a serious security breach. Finally, by its very nature, a minimalist approach provides little analysis to justify any real expenditure on protective mechanisms, so it does not cope well with anything more than a single issue or fairly simple situations.

3.3 Subject-Matter Experts

3.3.1 Advantages

Although the consultation and report writing inherent to this approach can be labour intensive, the more experienced security professionals generally respond very quickly to most requirements. Certainly, the actual effort is easily tailored to meet almost any schedule, operating budget and asset configuration to provide focused recommendations in a cost-effective manner. Written reports usually establish an acceptable audit trail for accountability purposes.

3.3.2 Disadvantages

On occasion, a scarcity of subject-matter experts can be a real impediment, especially with respect to newer technologies or more complex systems and facilities, because fewer security professionals have had the opportunity to develop the requisite knowledge and understanding. This problem can be particularly acute in situations demanding higher assurance levels, where caution demands input from two or more sources to corroborate their findings and recommendations. The very subjectivity of the analysis is another potential problem, in that the results may vary considerably based upon the personal knowledge and experience of the analysts involved. Replication may be difficult to achieve with potentially serious implications for interoperability and even the very credibility of the process. This can have serious consequences if the recommended solutions are particularly expensive or onerous. Without more objective measures than a narrative report, the results might be questioned, even rejected by senior decision-makers, thereby undermining the entire effort.

3.4 Security Standards

3.4.1 Advantages

The outstanding virtues of security standards are their ease of application and consistent results in comparable circumstances. These benefits arise from their inherent simplicity as a risk management mechanism. In general, the security practitioner merely defines the assets at risk, with perhaps a brief description of the associated operating environment. The relevant standards then provide a list of recommended safeguards, with perhaps a few options or trade-offs. Since the choices are generally limited for a given array of assets in any particular configuration, the ultimate solutions are usually consistent across platforms, thereby promoting interoperability and system integration. While the fundamental research behind these standards should be extensive, the checklist approach to their actual application requires far less time and expertise than a formal TRA. Provided the standards are reasonably current, the recommended safeguards are invariably effective, offering a very high assurance of significant risk reduction, because most assume a high threat environment and tend to counter worst-case scenarios.

3.4.2 Disadvantages

In practice, security standards suffer two major weaknesses. Firstly, the standards development process is often cumbersome, with extensive research and consultation prior to a prolonged balloting process, further revisions and, at long last, formal approval and promulgation. A protracted effort like this is almost inevitable to ensure that proposed standards are fully explored and broadly accepted, but the lengthy gestation period also has serious side effects. New technologies emerge far more quickly than the associated security standards, so project managers, system designers and security practitioners often face difficult choices with little or no direction and guidance. Where standards do exist, their utility is often compromised for similar reasons. All too many are updated infrequently due to the laborious effort involved. Inflexibility is the second serious failing of many security standards. In the search for simplicity, most risk variables are subsumed in a few distinct solutions. In the realm of cryptography, for example, one standard applies to all classified material, however sensitive, in almost all threat environments. This begs the question, if a cryptographic standard is designed to protect the most sensitive traffic on international links, is it not excessive for less sensitive material on domestic networks? In effect, security standards often impose excessive solutions to eliminate risk entirely, rather than manage the problem at a more reasonable or at least affordable cost.

3.5 Formal Threat and Risk Assessments

3.5.1 Advantages

As an approach to risk management, the formal TRA tends to address some of the more serious weaknesses of security standards. Once a TRA methodology is chosen, it can be applied to any emerging technology without delay. Provided the tool is both modular and extensible, the analysis may be focused on a limited number of issues to achieve timely solutions to immediate concerns. In most cases, the assessment provides explicit and fully transparent justification for the recommended solutions, thereby helping to overcome resistance to the inevitable expenditures. Furthermore, the actual cost of these safeguards can be minimized because the assessment does consider both threats and vulnerabilities as well as asset values, thereby avoiding some of the more extreme recommendations. This inherent flexibility is one of the

most significant advantages or benefits associated with the threat and risk assessment. An explicit audit trail with fully documented security decisions is another, especially if it ever becomes necessary to demonstrate due diligence following a serious incident.

3.5.2 Disadvantages

Although many publications in both the public and private sectors describe various threat and risk assessment methodologies in considerable detail, all too many fall short of a complete process. For example, some manuals provide little direction and guidance on such fundamental issues as asset valuation, threat metrics and even an acceptable definition of vulnerability. The inconsistencies and incompleteness inherent to many tools have tended to discourage some security professionals, who have then shied away from TRAs generally. Others have applied flawed techniques without understanding the potential consequences and, therefore, encountered unexpected even contradictory results. On occasion, disparate recommendations arising from different methodologies have had an adverse impact on interoperability, while undermining the credibility of the process. Threat and risk assessments also suffer another major shortcoming. The effort of collecting enough data for a comprehensive TRA report can be very daunting and extremely costly, especially for complex situations or scenarios. The absence of a single repository for threat information in the federal government merely compounds an already onerous burden. Therefore, time constraints often preclude an effort of this magnitude, and project managers frequently turn to other less expensive methods providing quicker results in order to minimize the impact on strict and occasionally unrealistic schedules. Although the *Harmonized Threat and Risk Assessment (TRA) Methodology* endeavours to remedy these shortcomings, the expertise required to conduct effective TRA projects is not always available.

4 Application

4.1 General

Each approach to risk management has both positive and negative attributes. Recognizing these advantages, or benefits, and disadvantages - some of which can cause real vulnerabilities - it seems self-evident that different options are more appropriate in different circumstances. To that end, some of the more important factors to consider when selecting a risk management methodology include: (1) cost and time constraints; (2) the complexity of the facility or system; (3) the duration of the project; (4) the availability of suitable standards and security professionals; and (5) above all, the current and anticipated risk environment.

4.2 Informal Threat and Risk Assessments

A minimalist approach to risk management is only appropriate under certain, very specific circumstances. It may be applied, of necessity, to obtain an immediate decision where severe time constraints preclude more rigorous analysis. In effect, to meet operational exigencies, any recorded response is better than prolonged indecision. In a benign risk environment, where asset values, threats and vulnerabilities are very low, this may be a reasonable approach, especially where costs are serious concerns and suitable security experts are simply unavailable for a more informed assessment. Furthermore, an informal or cursory TRA is frequently useful for

determining whether baseline security standards are sufficient or whether a formal TRA is necessary. When informal assessments are conducted out of expediency for more complex assets at some level of risk, they should be revisited very quickly and supplemented with one of the more comprehensive techniques.

4.3 Subject-Matter Experts

Provided that suitable subject-matter experts are readily available, this approach to risk management can be employed effectively in many different circumstances due to its very flexibility. In the absence of relevant security standards, experienced practitioners can respond to immediate requirements very quickly, with a focused examination of specific issues. More time will be required to address complex systems, so the advantages over formal threat and risk assessments tend to diminish. Given the subjectivity of this approach, it may be more appropriate to examine single occupant facilities or discrete systems rather than shared accommodations or inter-networked environments. This, of course, is unless the same resources are employed for each module or sub-component. In the final analysis, cost considerations are a significant determinant, so the presence of suitable in-house staff versus more expensive consultants can be an important factor. This drawback can be mitigated significantly by engaging the latter to only address specific shortfalls amongst the former. Finally, in a litigious environment, the logic of even a well-written narrative report may not be sufficiently transparent to demonstrate due diligence in the event of a major security breach. The use of acknowledged subject experts might offset this risk, but the application of more objective techniques may be preferable in order to provide a more defensible audit trail.

4.4 Security Standards

When available, security standards are particularly useful in many situations. For example, it is far simpler and much quicker to apply known standards than it is to conduct a formal threat and risk assessment project or even consult subject-matter experts. Hence, they are generally more appropriate when severe time constraints or rigid schedules mandate an immediate solution to some specific problem. Even if the relevant standards impose a more expensive suite of safeguards, the rapid response time may justify added costs in the short term. Then, other techniques may be introduced at a later date to review basic requirements and reduce any unjustified overhead. Where security expertise is scarce, standards can be applied with greater confidence by less qualified personnel. In a risk-averse environment, security standards are often preferable because they provide very secure solutions. On occasion, international agreements or contractual obligations may impose specific standards under certain conditions, so there is no real choice for the security professional. Finally, baseline security standards must be applied in accordance with the GSP.

4.5 Formal Threat and Risk Assessments

An abbreviated risk assessment, addressing only a few threats to a single asset, can be completed almost as quickly as any other technique. This approach is particularly useful as part of a larger security review where standards have not yet been drafted for some newer technologies. A narrowly focused TRA project is also handy to deal with unexpected threats or vulnerabilities, or to evaluate less onerous options when the approved standards are exorbitantly expensive or inconvenient. A more comprehensive assessment for an entire system or facility will certainly take much longer and cost much more. Thus, formal TRAs are frequently better suited to a project environment where the process can be scheduled at appropriate stages of the project plan or system development life cycle. The potential savings arising from more detailed analysis leading to a tailored suite of safeguards will often justify the additional time, effort and expense.

4.6 Summary

Depending upon the circumstances, especially the immediacy and the complexity of the requirement, any one of the approaches to risk management might support the development of sound security solutions. Clearly, some are more appropriate to higher risk scenarios, while others can be implemented more rapidly. Some address emerging technologies better than others, but all offer prospective benefits and merit serious consideration.

For security practitioners, the actual choice can have serious implications for the final outcome of a project. A minimalist approach in a high threat environment may leave valuable assets at risk. Slavish adherence to outdated standards could impose needless expenditures or, worse yet, introduce significant vulnerabilities. Scarce subject-matter experts might have a hidden agenda, leading to potential conflicts of interest, whereas full-blown TRA projects might not be feasible given the practicalities of asset values, cost and time constraints. Therefore, to achieve results that meet realistic operational requirements, risk managers should be familiar with all of the different options, and their inherent strengths and weaknesses.

For simpler systems or specific problems, the preferred alternative may be obvious, both intuitively and according to the selection criteria examined above. For more complex systems or complete programs, however, the proper choice may be less evident. In fact, the different methods are not mutually exclusive, so one or more techniques may be employed in combination for more precisely focused results. For example, proven standards might be applied to one asset in a facility or one component in a system, with a formal TRA to assess the security posture of other elements or services. A cursory TRA or minimalist approach might prove sufficient for certain aspects, such as lower asset values or lesser threats as explained in section 4.2, thereby freeing scarce security resources to concentrate on other more important functions. In short, the real power of these diverse methodologies lies in the synergy possible when complementary approaches are chosen carefully to balance operational needs and security concerns in pursuit of cost-effective solutions.

5 Conclusion

To protect sensitive assets, the government security policy prescribes safeguard selection according to baseline security standards and continuous risk management based upon the threat and risk assessment. Nevertheless, some other options, such as the use of subject-matter experts, have equal merit in certain circumstances.

More objective techniques, specifically the application of security standards and formal TRA projects, are generally preferable to achieve consistent results. Common solutions like these are particularly important to promote interoperability in the highly networked environments of today. More subjective schemes have real merit, however, in the absence of relevant standards, or when cost and time constraints prohibit a comprehensive TRA.

Given the higher obligations of a federal government, the policy correctly favours security standards and formal TRAs but, on occasion, other options are necessary in the interests of flexibility and cost-effectiveness, especially when they are applied in combination to suit the immediate needs of a particular situation. To ensure an informed choice, security authorities and project managers should understand the different methods, their strengths and weaknesses, and the circumstances appropriate to each.

This page intentionally left blank.

Appendix A-3 - TRA Team Composition

DEPARTMENTAL RESOURCES		
Position/Organization		**Primary Contributions**
Core Team	• Program Manager • Operational Authority	• (non-technical) asset identification • asset valuation/business requirements
	• System Administrators • Facility Managers	• (technical) asset identification • vulnerability assessment • existing (technical) safeguards • threat assessment
	• Project Manager • (System) Security Architect	• (technical) asset identification • existing/proposed (technical) safeguards • (technical) vulnerabilities • (technical) recommendations
	• Security Authorities – o DSO o ITSC o BCPC	• threat assessment • existing/proposed safeguards – o DSO – overall security program o ITSC – IT security o BCPC – business continuity plans/BIA • guidance on TRA process • perform quality assurance function
Other Internal Resources	• ATIP Coordinators	• access and privacy considerations/PIA
	• Finance	• asset valuation • threat assessment/losses to the Crown
	• Human Resources	• personnel issues • threats to employees
	• Internal Audit	• departmental audits/reviews • safeguard effectiveness/vulnerabilities
	• Legal Counsel	• legal obligations/liabilities
	• Material Management	• asset identification/valuation
	• Occupational Safety and Health	• certain (accidental) threats • related safeguards

EXTERNAL RESOURCES		
Position/Organization		**Primary Contributions**
Lead Agencies	• CSE	• (technical) vulnerabilities • (technical) threats • (technical) safeguards • threat and risk assessments
	• CSIS	• threat assessment
	• PSEPC	• asset valuation/critical infrastructure • threat assessment • vulnerability assessment • business continuity plans/BIAs
	• PWGSC	• contract security • asset identification/shared infrastructure
	• RCMP	• threat assessment • vulnerability assessment • physical/operational safeguards
Other Government Agencies	• DFAIT	• threat assessment: certain threats overseas
	• Environment Canada	• threat assessment: certain natural hazards
	• Health Canada	• threat assessment: health hazards • vulnerability assessment
	• HRSDC	• threat assessment; many accidental threats • vulnerability assessment
Other Public Sector	• Fire Department	• threat assessment
	• Provincial/Municipal Police	• threat assessment
	• Public Utilities	• (environmental) asset identification • threat assessment • vulnerability assessment
Private Sector	• Consultants	• augment departmental resources • conduct complete TRA
	• Insurance Industry	• threat assessment • vulnerability assessment
	• Product Vendors	• vulnerability assessment • existing/proposed safeguards

Notes**:**

1. The foregoing list is not exhaustive. Departments should add any other individuals or offices that may be appropriate under the circumstances prevailing in their environment.
2. The Primary Contributions identified in the third column are related to specific phases in a TRA project where the listed agencies may contribute useful information.

Appendix A-4 - Use of TRA Consultants

1 Introduction

When assembling a team to conduct a TRA, private sector consultants can be a valuable adjunct to supplement departmental resources. With careful planning and judicious management, the potential benefits can far outweigh possible pitfalls. Furthermore, a National Master Supply Arrangement, established through PWGSC, has simplified the contracting process for IT security professional services in particular.

2 Potential Benefits

The use of consultants can offer considerable flexibility during a TRA project. For example, suitably qualified contractors are often readily available, so they can be engaged fairly quickly to meet pressing target dates, especially when departmental resources are already overextended.

Since most government employees have several different responsibilities, often with conflicting priorities, it may be difficult for them to concentrate fully on a single assessment. Therefore, to achieve more focused results, one or more consultants might be hired exclusively to conduct a specific assessment or some portions thereof.

In many organizations, the salary budget is more severely constrained than the operating and maintenance (O&M) envelope. Thus, it may be easier to hire a consultant than establish new positions for dedicated TRA analysts.

Where specialized expertise is necessary to conduct an assessment, departmental resources may be scarce or, in the case of some emerging technologies, even non-existent. To avoid expensive training costs and the associated delays for what might be a one-time requirement, it may be preferable to engage a knowledgeable consultant. The use of acknowledged experts with both knowledge and experience can also lend credibility to the findings and recommendations in a TRA report, thereby helping to justify added expenditures on essential safeguards and later to demonstrate due diligence should risks actually materialize.

As outsiders, consultants often approach problems from a different point of view, adding a fresh perspective and, as independent third parties, they may provide more impartial analysis.

Consultants are usually expected to work offsite, so they generally require neither office supplies nor government accommodation. This can be a significant advantage when quarters are severely constrained.

3 Possible Issues

In order to optimize the benefits of TRA consulting services, some issues of potential concern should be considered and addressed from the outset.

Where contracts exceed the limits for directed call-ups, the competitive bidding process may introduce some delays with an adverse impact on scheduling. This problem may be compounded near the end of the fiscal year when many departments let a number of contracts to help reduce surpluses and balance budgets.

In some cases, the demand for knowledgeable consultants can exceed the supply, so it may be difficult to obtain dedicated support, especially at short notice.

While many contractors have a sound understanding of various TRA methodologies and current information technologies, they are less likely to have a detailed knowledge of departmental programs and services that are the subject of a TRA project. Depending upon the complexity of the assets and their environment, the time needed to acquire this knowledge may be better spent training permanent staff on the TRA process.

Most TRA projects involve at least some sensitive information, especially with regard to threats and vulnerabilities. Therefore, security screening to the appropriate level is essential for individual consultants, while a facility security clearance is necessary for their firms. For most established companies this is not an issue but, with the high turnover of personnel across the industry, the time to process security assessments or reliability checks may cause some delays.

Although contractors can contribute significantly to a TRA team, over-reliance on their services may inhibit the development of suitably qualified staff, thereby creating an ongoing dependency on external versus internal resources. Apart from questions of morale, this can also be wasteful because consulting services are not inexpensive. In fact, the daily rates for most contractors tend to be double the pay scales (including benefits) for equally experienced employees.

4 Opportunities

While there are many reasons to engage consultants in support of TRA projects, some of the more positive benefits are likely to be achieved under the following circumstances:

- **Urgent Requirements.** When a rapid turnaround is required to meet compressed project schedules or respond to urgent security incidents, departmental resources may be augmented with one or more TRA consultants to expedite the assessment.
- **Specific Expertise.** On occasion, some TRA projects will require access to highly specialized and, therefore, scarce expertise to assess particularly complex technologies, and more obscure threats or vulnerabilities. Unless it becomes a regular requirement, consultants are probably best suited to meet unique, short term needs.

- **Enhanced Credibility.** In risky situations where a TRA report may be subject to public scrutiny in the event of a compromise, the cost of a highly qualified subject matter expert may be justified for added assurance and confidence in the final recommendations.
- **Peak Workloads.** As a short term expedient, consultants can supplement regular staff to offset peak workloads, as illustrated in Figure A4-1. In this example, the projected or anticipated demand for TRA services would fully occupy three full time equivalents (FTEs) but increased demand in the fall could occupy a fourth analyst. Rather than establish another permanent position, a ninety-day contract for a TRA consultant could be let cover this period. For longer commitments of six months or more, departmental employees are generally the more cost-effective solution.

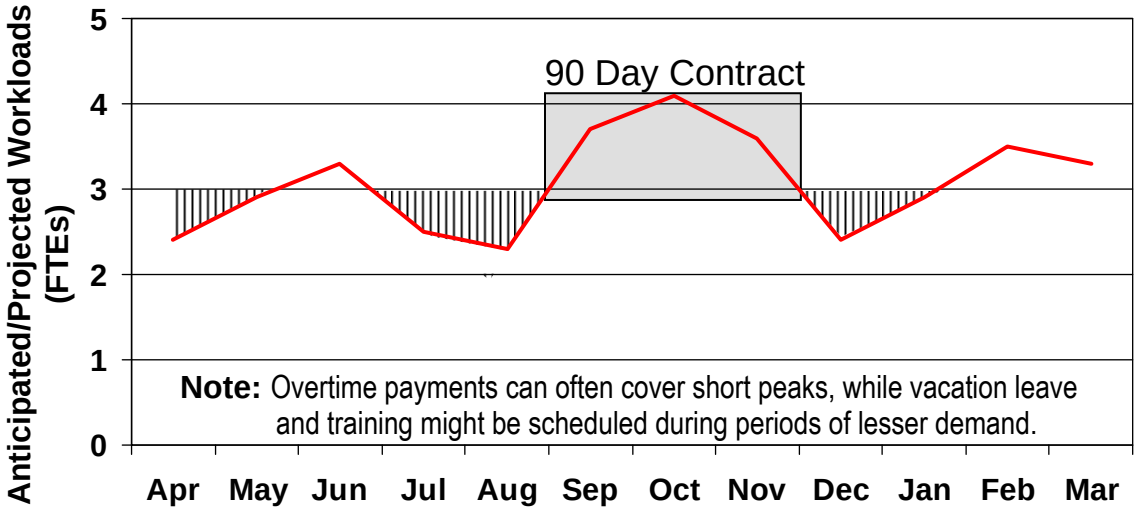

Figure A4-1: Engaging Consultants to Augment Dedicated TRA Staff

- **Dynamic Organizational Structure.** Contractors can be particularly useful for organizations in a state of flux. For example, during periods of rapid growth or structural change, TRA consultants can provide valuable stability and a useful bridging mechanism until new positions are finally staffed and the personnel fully trained. When downsizing, they can fill gaps left by departing employees until the situation stabilizes.
- **Budget Considerations.** When additional resources are required for TRA projects, but the salary envelope is fully committed and personnel cannot be reassigned from other duties, the expenditure of O&M funds on consulting and professional services contracts may be the only viable alternative. Furthermore, near the end of the fiscal year, additional TRA consultants might be engaged profitably to clear any backlog of outstanding assessments, and avoid an otherwise unacceptable budgetary surplus.

5 Best Practices

5.1 General

The use of consultants in support of a TRA may be optimized with some simple best practices regarding selection criteria, the contracting process and subsequent management of the project.

5.2 Selection Criteria

Several important factors should be considered carefully when selecting a TRA consultant:

- **Knowledge.** A sound understanding of security practices relevant to the assessment is essential, especially when the assets involve new or more complicated technologies. Specific knowledge of the organizational structure and business practices of the department sponsoring the contract is a secondary consideration, but certainly a desirable attribute to facilitate the assessment.
- **Experience.** Demonstrated experience with the preferred TRA methodology is equally important to avoid delays and misunderstandings.
- **Depth.** While a single consultant may provide excellent service, it is generally preferable to engage a firm with some depth of personnel to obtain access to a larger knowledge base and minimize the risk of delays or disruption to the TRA project in the event of accident or illness.
- **Competence.** The quality of previous work is normally a good indicator of future performance, so some effort should be made to determine how well the consulting firm has satisfied other clients.
- **Compatibility.** A subtle, but potentially significant issue is the compatibility of the consultant with the corporate culture and business practices of the contracting party. Even the most competent contractor may fail to achieve positive results if personal style or professional behaviours create barriers to effective communications and credibility.
- **Cost.** To achieve the best price-performance, consulting rates must be weighed carefully against the other selection criteria. With directed bids, a subjective comparison of costs versus professional qualifications may suffice but, in a competitive bidding process, it is particularly important to identify the weighting factors explicitly in advance, as indicated in section 5.3 below, to achieve the most cost-effective results.

5.3 Contracting Considerations

All contracts for TRA services must abide by the *Contracting Policy*, the *Supply Manual* and the Security in Contracting Management Operational Standard. In particular, departments should be aware of the current limits on directed or sole-source contracts and competitive bids processed internally versus contracts arranged through PWGSC. While it may be preferable to conduct a larger TRA project in several smaller modules, care must be taken to avoid real or perceived contract splitting. Further details regarding these important issues include:

- **Contracting Limits.** Sections 16.10 and 16.11 of the *Contracting Policy*[1] provide explicit direction and guidance on contracts for consulting and professional services. Limits for both competitive and non-competitive contracts are listed in Schedule 3 of Appendix C to the policy, while Schedule 5 imposes even more strict limitations on service contracts with former public servants in receipt of a pension.
- **Statement of Work (SOW).** A clearly worded SOW is crucial to the success of any contract for TRA consulting services. As a minimum, an SOW should include a precise objective for the TRA project, an unambiguous description of all tasks and deliverables with explicit target dates and reporting relationships for both interim and final TRA reports, a specific statement of personal qualifications expected of the contractor, the prescribed methodology to be employed, any security requirements and all relevant references. A Sample SOW for TRA Consulting Services is provided at Appendix A-5.
- **Standard Clauses.** When issuing a contract, either directly or through PWGSC, departments should include standard clauses regarding intellectual property rights to the TRA report and all other documentation within the TRA record. Security requirements, such as security screening levels for the consultants and, if they are to work off-site, a document safeguarding capability for their facility, are another important consideration, normally captured in a Security Requirements Check List (SRCL)[2]. Legal liabilities may be a concern in the event that risks materialize despite full implementation of all safeguards recommended in the TRA report.
- **Cost versus Quality.** For competitive contracts, weighted bid evaluation criteria should be identified explicitly for all selection factors in the solicitation documentation, such as a Request for Proposal (RFP), to ensure the best value for money. Otherwise, a less qualified vendor might win the competition with an artificially low bid.

5.4 Management of a TRA Contract

To avoid unexpected results, TRA consultants should not be expected or even allowed to work in isolation. Regular contact with the Technical Authority (TA) identified in the SOW is essential to manage the TRA project to a successful conclusion. More specifically, the TA should perform the following functions throughout the life of the contract:

- **Provide support** to ensure that the contractor has ready access to departmental personnel and other resources, such as reference documentation and physical assets, to collect the data necessary for analysis as quickly and efficiently as possible.
- **Review deliverables** immediately to avoid undue delays.
- **Offer constructive feedback** to keep the contract on track.
- **Assign dedicated staff** to accompany and assist the contractor wherever possible for two reasons: firstly to optimize the consultant's efforts to produce a sound assessment and, secondly, to obtain some knowledge transfer that will help develop departmental staff.
- **Review the results** in an impartial manner, not to criticize the contractor's performance, but to capture any lessons learned that may improve the output of subsequent contracts for TRA consulting services.

[1] See the TBS web site: http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/Contracting/contractingpol_e.asp

[2] Form number TBS/SCT 350-103 (2004/12) found at: http://www.tbs-sct.gc.ca/tbsf-fsct/350-103_e.asp.

6 Cyber Protection Supply Arrangement (CPSA)

As indicated in Appendix A to the GSP, CSE is the IT security technical authority for the government of Canada. In this capacity, the agency has established a National Master Supply Arrangement under the auspices of PWGSC to facilitate contracting for IT security risk management services, including TRA consultants. The quality assurance mechanisms incorporated in the CPSA are another important benefit of the program.[3]

[3] See the CSE web site: http://www.cse-cst.gc.ca/services/cpsa/cpsa-program-e.html.

Appendix A-5 - Sample Statement of Work for TRA Consulting Services

1 Objective

The purpose of this Statement of Work (SOW) is to describe the work entailed in conducting a threat and risk assessment (TRA) of the *[name of facility/system]*. *[Provide a brief description of the facility/system in the body of the SOW; all suitable plans, schematics and more detailed material are to be relegated to an annex.]* As a minimum, the TRA will include:

- a Statement of Sensitivity (SOS) to identify and categorize relevant assets according to their confidentiality, integrity and availability values based upon the injuries that may reasonably be expected in the event of a compromise;
- an identification of deliberate threats, accidents and natural hazards that might affect these assets adversely with an analysis of the likelihood of occurrence and gravity of impact;
- an assessment of current vulnerabilities, based on an evaluation of existing or proposed security measures and their adequacy;
- an analysis of residual risks for each asset which is vulnerable to specific threats; and
- where assessed residual risks exceed the *[Low or Medium]* level, a list of recommendations proposing additional safeguards to achieve a *[Low or Medium]* target risk level with an assessment of their effectiveness and cost.

2 Tasks and Deliverables

2.1 Preparation Phase

2.1.1 General

[Departmental authorities may wish to complete the Preparation Phase[1] *before issuing an SOW for consulting services to conduct the actual TRA. In that case, this section may be omitted from the SOW. If a contractor is engaged to perform the Initial Planning, however, the SOW should include a general description of the Initial Planning phase and its deliverables.]*

Careful planning is required before initiating a TRA to determine the scope of the assessment, identify resource requirements and develop a realistic work plan. To achieve these goals, the contractor must work in close cooperation with the Project Authority (PA), the Technical Authority (TA), security officials and facility or system managers. The contractor will be provided with all reference material, listed at Section 4 below, and any other information necessary for the completion of this task. Information-gathering activities may include interviews with personnel at various levels of the organization.

[1] Described in Annex A.

2.1.2 Initial Planning Deliverables

The sole deliverable for the Preparation Phase is a complete TRA Work Plan[2] which includes:

- a clearly stated **Aim** for the TRA;
- a statement of **Scope** with a description of the *[facility or system]* under consideration, its mission and concept of operation, as well as the boundaries of the assessment and any dependencies or interconnections with other *[facilities or systems]*;
- any **Limitations** or restrictions on the TRA;
- the **Target Risk Level** accepted by the responsible manager;
- a list of personnel who will participate in the TRA process as **Team Members** or sources of information;
- all necessary **Logistic Arrangements**, including security screening and access requirements, travel arrangements, administrative support and other resource requirements;
- a list of **Input Documentation** and **TRA Deliverables**; and
- a detailed **TRA Schedule** listing all major activities, assigned resources, start and completion dates, and any dependencies.

2.2 The Threat and Risk Assessment

2.2.1 General

Once the TRA Work Plan has been approved at the end of the Preparation Phase, the contractor shall develop four mandatory deliverables to address the four-step TRA process prescribed by the Government Security Policy (GSP):[3]

- **identifying the employees and assets** to be safeguarded in a Statement of Sensitivity;
- determining the **threats to employees and assets** in Canada and abroad, and assessing the likelihood and impact of threat occurrence;
- assessing **risks** based on the adequacy of **existing safeguards** and **vulnerabilities**; and
- recommending any **supplementary safeguards** that will reduce the risk to an acceptable level.

2.2.2 Asset Identification and Valuation Phase[4]

In the second phase, the contractor will identify and list employees, assets and services within the scope of the assessment, and assign values for confidentiality, availability and integrity, as appropriate, based upon the injuries that might reasonably be expected in the event of compromise. The results of this analysis shall be presented as a Statement of Sensitivity in a tabular form, the one deliverable for this portion of a TRA project, and fully annotated to justify the findings.[5]

---

2 Appendix A-6 provides a Sample TRA Work Plan.
3 Described in the Management Summary.
4 Described in Annex B.
5 Appendix B-5 provides a sample Statement of Sensitivity or Asset Valuation Table.

2.2.3 Threat Assessment Phase[6]

The third phase of a TRA project requires the contractor to identify real and potential threats that could reasonably be expected to affect employees, assets or services adversely. Pertinent threat information should be obtained from departmental security authorities and the responsible lead agencies, specifically CSIS, CSE and the RCMP. Key deliverables for this portion of the TRA comprise:

- a tabular list of real and potential threats that could injure employees or compromise assets and services within the scope of the assessment;[7] and
- an assessment of the likelihood and impact of their occurrence.[8]

2.2.4 Risk Assessment Phase[9]

In the fourth phase of a TRA project, the contractor will deliver an assessment of residual risks to employees, assets and services identified in the second phase arising from threats analyzed in the third phase. The two mandatory deliverables are the Vulnerability Assessment derived from an evaluation of existing or proposed safeguards and their effectiveness,[10] and the Risk Assessment listing all residual risks to employees, assets and services within the scope of the assessment.[11]

2.2.5 Recommendations Phase[12]

Based upon the findings of the Risk Assessment completed in previous phase, the contractor will propose the addition, modification or removal of safeguards to achieve an acceptable level of residual risk.[13] The projected residual risk, that which remains after the recommendations have been approved and implemented, shall be identified explicitly, as shall the costs of the recommended changes.[14]

3 Project Management

3.1 Project Authority (PA)

The PA for this TRA project is *[name, position and telephone number of the overall coordinator of the TRA project selected in accordance with section 5.4.7 of Annex A]*.

6 Described in Annex C.
7 Appendix C-4 provides a sample Threat Assessment Table.
8 Appendix C-3 amplifies the measures of likelihood and impact or gravity and their calculation.
9 Described in Annexes D and E.
10 Appendix D-4 provides a sample Vulnerability Assessment Table.
11 Appendix E-2 provides a sample Risk Assessment Table.
12 Described in Annex F.
13 Appendix F-3 identifies explicit Safeguard Selection Criteria while Appendix F-2 provides a Safeguard Listing to support the Recommendations.
14 Appendix F-5 provides a sample Recommendations Table.

3.2 Technical Authorities (TA)

The TAs for this project are *[names, positions and telephone numbers of designated subject matter experts who will provide technical input to the TRA, including security authorities, facility managers or systems administrators, and other members of the TRA Team]*.

3.3 TRA Methodology

The contractor shall employ the *Harmonized Threat and Risk Assessment (TRA) Methodology* for this project. *[Specify alternatives if applicable.]*

3.4 Personnel Qualifications

The contractor shall provide personnel who have solid experience and knowledge of both the TRA process and the subject of the assessment, normally demonstrated by the successful completion of at least three previous TRAs on similar *[facilities or systems]*.

3.5 Security Requirements

This SOW is *[classified (state level) or categorized (state level)]*, the work performed under this contract will be *[security classification]* and the deliverables associated with the completion of the work detailed in this document will be *[security classification]*. The contractor analyst(s) must possess valid security screening to at least the level specified for the work and the deliverables. *[Note: The Statement of Sensitivity identifies the value of employees, assets and services while the Vulnerability Assessment lists the attributes of an asset or its environment that may be exploited by threats to cause damage. These are major considerations when assigning a security category (Classified or Protected) to TRA deliverables. Where the TRA involves proprietary information from a third party, such as a product vendor, the contractor should be required to sign an appropriate non-disclosure agreement.]*

3.6 Schedule

As stipulated in Section 2.1 *[if the contractor is to conduct the Initial Planning]*, the contractor shall develop a TRA Work Plan with a detailed schedule showing milestones, critical activities and dependencies for the completion of the work by *[a date specified by the contracting authority]*. The contractor shall complete this TRA project within *[time frame cited in the TRA Work Plan]* following award of the contract, with intermediate deliverables submitted to the TA and PA in accordance with the approved TRA Work Plan. *[For greater clarity, each of the deliverables and the associated target dates might be presented in a table or, for a very complex TRA project, a GANTT chart]*.

3.7 Approval of Deliverables

All deliverables will be reviewed for quality and completeness, and signed off by the designated TAs before proceeding to the next phase of the project. The final TRA report must be approved by the PA before the contract may be finalized.

3.8 Progress Reporting

The contractor shall provide routine *[generally weekly]* progress reports to the designated TA. Verbal progress reports are acceptable. *[Where written reports are preferable, specify the format and content]*.

3.9 Place of Work

All work shall be conducted at the contractor's place of business, except for interviews with departmental personnel which shall be coordinated with the designated TA. *[If the TRA project includes sensitive information, ensure that a facility security clearance with document safeguarding capability to the appropriate level has been specified in section 3.5 above]*.

3.10 Proprietary Information

All information and documents made available to the contractor during the course of this project are deemed proprietary, and shall be returned upon completion of the TRA.

3.11 Handover

The contractor shall table the following at a handover meeting arranged by the TA, within two (2) working days of the satisfactory completion of the project:

- a list of all changes to the deliverables in response to comments from the TA and PA;
- all final deliverables in *[specify format and number of copies]*; and
- all proprietary information and documents provided to the contractor during the project.

Annex A to Sample Statement of Work (SOW)

References:

Government Security Policy, Treasury Board Secretariat, February 2002.
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg_e.asp

Operational Security Standard: Asset Identification, Treasury Board Secretariat, Draft.

Operational Security Standard: Business Continuity Planning, Treasury Board Secretariat, March 2004.
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/ossbcp-nsopca_e.asp

Operational Security Standard: Management of Information Technology Security, Treasury Board Secretariat, April 2004.
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/23RECON_e.asp

Operational Security Standard: Security Risk Management, Treasury Board Secretariat, Draft.

Harmonized Threat and Risk Assessment (TRA) Methodology, Communications Security Establishment and Royal Canadian Mounted Police, August 2007.

Privacy and Data Protection Policy, Treasury Board Secretariat, December 1993.
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/CHAP1_1_e.asp

Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks, Treasury Board Secretariat, August 2002.
http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld_e.asp

Privacy Impact Assessment Policy, Treasury Board Secretariat, May 2002.
http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr_e.asp

Risk Management Policy, Treasury Board Secretariat, April 1994.
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/riskmanagpol_e.asp

A Guide to Certification and Accreditation for Information Technology Systems (MG-4), Communications Security Establishment, January 1996.
http://www.cse-cst.gc.ca/en/publications/gov_pubs/itsg/mg4.html

[Not all of the foregoing references may be necessary for any given TRA. Simply list what is applicable. Add any other material specific to the subject of the TRA, such as business plans, design documentation and relevant threat assessments].

Appendix A-6 - Sample TRA Work Plan

1 Background

Identify the organization and provide some background material to situate the assessment within a departmental context. Depending upon the purpose of the TRA, this might include:

- a short description of the business line and its operating environment;
- any service delivery levels or obligations relevant to the assessment;
- the rationale for a new or upgraded facility or IT system; and/or
- the nature of any specific security concerns to be addressed.

2 Aim

State the purpose of the assessment in a single sentence similar to the following examples:

- "The aim of this TRA is to assess the risks associated with upgrades planned for *[facility name]* and to recommend suitable safeguards."
- "The aim of this TRA is to assess the risks associated with *[name of new IT system]* and to recommend suitable safeguards in support of system certification and accreditation."
- "The aim of this TRA is to assess the need for safeguards beyond baseline security requirements for *[identify facility or IT system]*."

3 Scope

Identify the subject of the assessment and provide a general description of the facility or IT system under assessment. Maps, charts, floor plans and system schematics can be particularly useful to delineate the boundaries of a TRA. Lists of what falls within the scope of the assessment and what does not might be attached as annexes.[1]

To minimize duplication of effort and limit the scope as much as possible, separate TRA projects might be conducted for different business lines within a facility or major components and modules of an IT system, as suggested in section 4.3 of Annex A. Although each element may be examined discretely, all of the associated assessments should be identified along with their inter-relationships.

Again, a diagram such as the one shown in Figure A6-1 can provide a visual depiction of the scope. In this particular example, a simplified cross-section of a four story building housing four distinct program activities, each business line could be the subject of a distinct TRA, with a fifth assessment addressing base building security. Then, in the statement of Scope for the Human Resources TRA, the relationship with the other assessments could be illustrated accordingly.

[1] These lists may be distilled from the comprehensive Asset Listing in Appendix B-2.

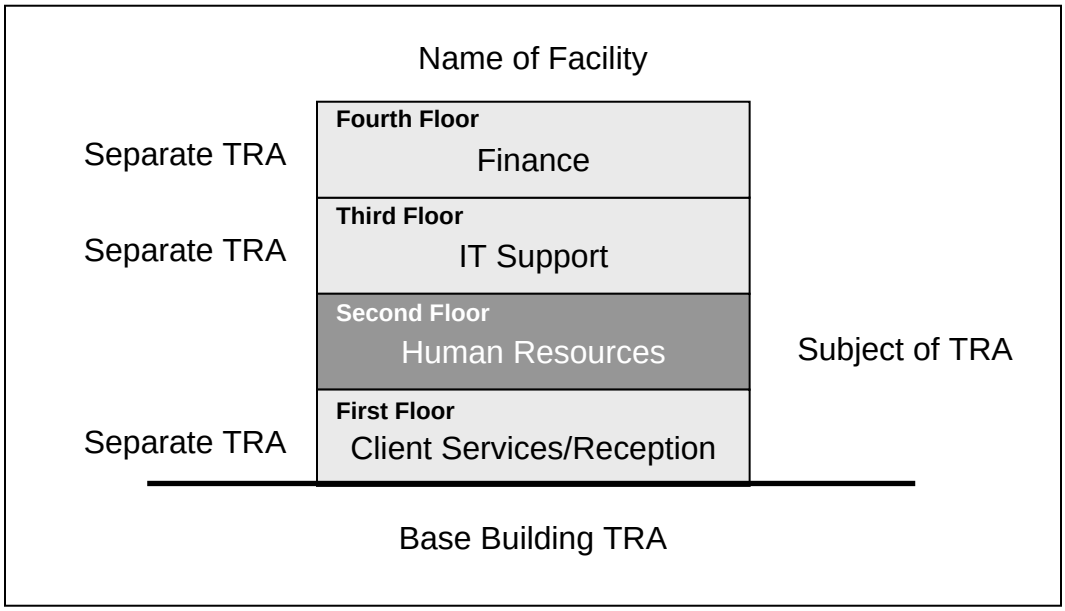

Figure A6-1: Diagram Illustrating Linked TRA Projects for a Single Facility

4 Limitations

Identify any limitations or restrictions on the TRA, such as:

- cost or time constraints that might affect the scope;
- the inaccessibility of any assets for examination;
- a lack of documentation that may constrain the analysis; and
- any deliberate exclusions of assets or threats for whatever reason, but usually those of lower values that cannot contribute significantly to overall risk.[2]

5 Target Risk Level

In order to avoid a tendency towards increasing risk tolerance when the findings of a TRA recommend additional, possibly expensive safeguards, the acceptable level of residual risk should be stated in advance, before commencing a TRA project. Initially, this may be difficult to achieve in practice because senior managers may be unfamiliar with the TRA process and the nature of residual risk. Once the analytical approach has been demonstrated in practice, however, much of the original reticence should normally disappear.

[2] While asset values and threats are normally determined during the next two steps of the TRA process, as described in Annexes B and C, some will be patently obvious from the beginning and may therefore be dropped from the actual TRA. For example, non-critical office supplies, especially in small quantities, are generally omitted from the assessment of a typical business setting.

Annex E, the Calculation of Residual Risk, provides a fuller examination of residual risk and its metrics. Section 2 of Annex F, the Recommendations Phase, explores issues of acceptability but, as a useful rule of thumb, Low or Medium levels of assessed residual risk should be acceptable in most circumstances. Anything higher would be too risky, while any attempt to achieve Very Low risk levels is likely to be prohibitively expensive and needlessly restrictive.

Thus, the content of this section of the TRA work plan can be as simple as: "The target risk level for this TRA is *[Low or Medium]*. The Recommendations Phase will propose additional safeguards to achieve this target whenever residual risks are assessed as *[Medium, High and Very High/High and Very High]*".

6 Team Composition

List the core team members with their primary responsibilities or inputs, and other resources available to help complete the TRA. A tabular form, like that illustrated in Table A6-1 is a simple method of presenting the requisite information.

Organization	Team Member(s)	Primary Responsibilities
Business Line	Name and Position	Asset Identification and Valuation
Project Office	Name and Position	Asset Identification Vulnerability Assessment Recommendations
Departmental Security Officer	Name and Position	Threat Assessment Vulnerability Assessment Recommendations
etc.		

Table A6-1: TRA Team Composition List

Both the team coordinator and the approving or accreditation authority, in the case of physical and IT security assessments respectively, should be identified explicitly.

7 Logistic Arrangements

While the logistic arrangements for a smaller, focused TRA may be very simple, those for a major Crown project can be quite complex, to address many different factors, including:

- **Security Screening Requirements** for team members to access both the information and facilities associated with the TRA, knowing that threat and vulnerability data in particular are often quite sensitive, as examined in section 5 of Annex G;
- **Access Requirements** to facilities and data, both physical and logical, based upon the need-to-know, not just the security screening level;
- **Travel Arrangements**, with formal visit requests where necessary, when facilities are distributed geographically;

- **Administrative Support**, especially clerical assistance to file and retrieve documentation, prepare copies, record and distribute correspondence and otherwise relieve the analytical team of routine chores;
- other **Resource Requirements** for accommodation, office equipment, specialized training and the associated funds needed to complete the project; and
- where applicable, any **Statements of Work** for consulting services.

A simple table should suffice to capture most of this information, while any Statements of Work should be attached as one or more Annexes.

8 Input Documentation

It is rarely feasible to list all source documentation in a TRA work plan because new material of interest is likely to emerge throughout the analytical process. Nevertheless, many of the more important references should be identified in advance to help the TRA team get off to a rapid start. Some of this documentation might include:

- federal statutes, regulations and policies relevant to the subject of the assessment;
- departmental policies and business plans;
- memoranda of understanding for the sharing of information and other assets;
- facility plans and architectural drawings;
- project documentation, ranging from functional requirements through detailed designs with any associated schematics or "as-built" drawings;
- any pertinent audits or reviews, and earlier or related TRA reports; and
- any available threat and vulnerability assessments.[3]

To keep the body of the work plan as short as possible, all of this documentation should be listed in an Annex.

9 TRA Deliverables

In each case, the most important deliverable is the final TRA report which identifies residual risks and, if necessary, recommends additional safeguards to achieve acceptable risk levels. The format and general content of the TRA should be specified in the work plan. TRA report templates and a sample TRA report are provided in Appendices F-6 and F-7 respectively.

In a project environment, other outputs may be required. For example, a preliminary, high-level assessment may address functional requirements while further refinements are developed at different stages of the project plan or system development life cycle as the design matures. Appendix A-1 examines the evolution of a TRA throughout a generic system development life cycle. For particularly complex TRA projects, interim progress reports are often advisable to help keep activities on track and identify any potential impediments as soon as possible. In some

[3] Fuller lists of potential source material are presented in Appendices B-1 for assets, C-1 for threats, D-1 for vulnerabilities and F-1 for safeguards.

cases, verbal briefings may be acceptable, but written reports are generally preferable for a permanent record.

10 TRA Schedule

Establishing a realistic TRA schedule is particularly important to allocate resources more efficiently and manage expectations throughout the process. In general, all major activities should be listed with proposed start and completion dates, the resources assigned to each task, and any interdependencies. While a simple table, like that illustrated in Table A6-2, might be adequate for shorter TRA reports, more complex assessments will benefit considerably from more sophisticated planning and tracking mechanisms, such as Gantt or PERT[4] charts, and automated tools for their generation and analysis, such as Microsoft ® Project™.

Serial	Activity	Assigned Resources	Start Date	Completion Date	Dependencies
1.	Identify Assets				
2.	Assign Asset Values				Complete #1
3.	Identify Threats				
4.	Assess Probability/Magnitude				Complete #3
5.	Assess Vulnerabilities				Complete #1
6.	Determine Residual Risk				Complete #s1-5
7.	Recommend Additional Safeguards				Complete #6
8.	Submit Final TRA				Complete #7

Table A6-2: Simple TRA Activity List

11 Approval

A formal sign-off by the responsible program or service delivery managers who must ultimately accept or reject any residual risk is highly recommended, to ensure that they understand the TRA process and the decisions they will make with regard to the final recommendations.

Approved.

Name
Position

[4] *Program Evaluation Review Technique.*

This page intentionally left blank.

Annex B - Asset Identification and Valuation Phase

1 Introduction

1.1 General

Once the mandate for a TRA project has been established, the scope of the assessment determined, the team assembled and the TRA Work Plan approved, the actual analysis may commence with the second phase, Asset Identification and Valuation, which comprises three successive processes and one major output as follows:

- **Asset Identification** – to list all of the assets that fall within the scope of the assessment at an appropriate level of detail.
- **Injury Assessment** – to determine the injuries that might reasonably be expected to arise in the event of a compromise to the confidentiality, availability or integrity of each asset.
- **Asset Valuation** – to assign asset values for confidentiality, availability and integrity, as appropriate, for each asset based upon common injury tests.
- **Prioritized Asset Listing** – to produce the Statement of Sensitivity, a comprehensive list of assets, which may be ranked from the most valuable to the least.

1.2 Aim

The aim of this annex is to describe the three processes and single output of the Asset Identification and Valuation Phase of a TRA project.

1.3 Policy Compliance

Section 10.6 of the GSP, Identification of assets, directs departments to identify and categorize assets when their compromise could reasonably be expected to cause injury to national, private or other non-national interests. Section 10.7, Security risk management, requires the identification of both employees and assets to be safeguarded. These policy requirements are amplified in two Operational Security Standards, the Identification of Assets and Security Risk Management, respectively. The Asset Identification and Valuation Phase of a TRA project builds upon and extends these policy requirements and supporting standards.

2 Asset Identification

2.1 Asset Definition

> ***Assets** (biens)* - 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.
>
> *Government Security Policy*, February 2002

Assets, as defined in the GSP, include neither employees nor services, but both require protection in accordance with the policy objective.[1] Therefore, to determine appropriate safeguards beyond baseline security as well as occupational safety and health requirements, employees, other personnel and the services they provide, must be identified explicitly, at an appropriate level of detail, if they fall within the scope of a TRA project.

2.2 Tangible Assets

Tangible assets are generally the easiest to identify for they include concrete items, such as facilities, vehicles, office supplies and furniture, works of art, cash and other negotiable instruments, IT equipment with the attendant software and firmware, and information in all forms, both hard copy and electronic. Security equipment, ranging from alarms and secure containers to anti-virus software and cryptographic devices, is a special subset of tangible assets that may be at risk and, therefore, fall within the scope of a TRA project. While government departments own and operate many tangible assets, others fall outside their direct control. Nevertheless, the compromise of certain assets in the surrounding environment could affect government operations adversely, so it is frequently necessary to extend the scope of an assessment to include things, like the power grid or the building fabric of leased accommodations, which might otherwise be overlooked.

2.3 Intangible Assets

Intangible assets, such as employee morale and public confidence, are largely matters of attitude arising from personal perceptions, both individual and collective. These perceptions of such varied issues as service quality, product branding, management practices and ethical standards are often related to the mission, vision and values of an organization which may be ill-defined and poorly understood. Thus, intangible assets are frequently more difficult to identify and categorize than their more concrete counterparts.

The analysis of intangible assets is also complicated by the fact that relatively few threats affect them directly. Of course, there are some exceptions, such as subversive propaganda or malicious rumours, which target morale or public confidence explicitly. More often than not, however,

[1] Section 3 of the GSP, Policy objective, states: "To support the national interest and the Government of Canada's business objectives by safeguarding employees and assets and assuring the continued delivery of service."

injuries to intangible assets arise from the compromise of tangible assets or employees and the services they deliver.

Despite these difficulties, it is absolutely imperative that intangible assets be identified in a TRA project because the consequences of their compromise can be more severe than the attendant injuries to other assets. For example, unauthorized disclosure of some personal information regarding a single individual might cause some embarrassment or perhaps more serious injury depending upon the level of sensitivity, but public perception of the leak may cause even greater harm, undermining both credibility and confidence in the organization generally.

To address this important issue, the relationships between employees/tangible assets and the derived intangible assets should be identified explicitly. Then, since most safeguards protect employees/tangible assets directly and intangible assets only indirectly, the values assigned to the former should be aligned with those of the underlying intangibles to ensure proper protection.

2.4 Personnel

Although employees and other personnel are not considered assets within the context of the GSP, they do require protection for at least two important reasons. Firstly, government departments have very real obligations under the *Canada Labour Code*[2] and various TBS policies, such as *Occupational Safety and Health*[3] and section 10.10 of the GSP, to safeguard employees from all hazards ranging from accidental injury to threats of violence in the workplace. Secondly, the availability of qualified staff can be a significant issue depending upon the nature and importance of the services they provide. In order to address both concerns with appropriate security solutions, employees and other personnel at risk must be identified during the second phase of a TRA project.

2.5 Services

Employees work with largely tangible assets to provide government services, such as health care and pension payments. Thus, from a departmental perspective, safeguarding employees and assets according to baseline security requirements and complimentary TRA projects might suffice to ensure satisfactory service delivery. From a client's point of view, however, the services themselves are usually the most important consideration. Therefore, to ensure a balanced assessment within the scope of a TRA project, it is important to identify all services rendered and link them with the responsible employees and relevant assets.

2.6 Asset Identification Model

Figure B-1 illustrates the varied subjects of the Asset Identification and Valuation Phase of a TRA project, namely employees and other personnel who use tangible assets to produce

[2] Available at the Justice Canada web site: http://laws.justice.gc.ca/en/L-2/index.html.
[3] Available at the TBS web site: http://www.tbs-sct.gc.ca/pubs_pol/hrpubs/TBM_119/osh_e.asp.

services, the perception of which will generate or at least affect intangible assets, such as employee morale and public confidence.

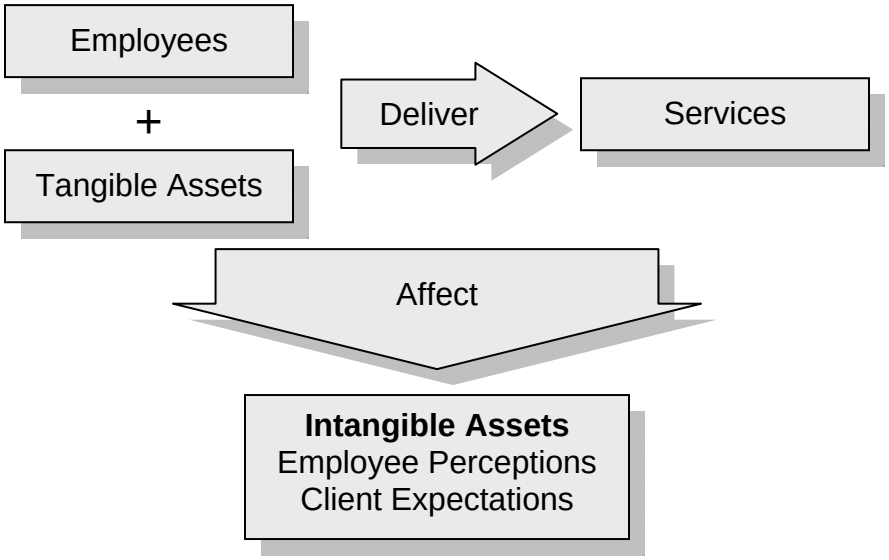

Figure B-1: Asset Identification Model

2.7 Sources of Asset Data

Data regarding assets and their associated values are readily available from many different sources. Program and project managers are often a logical point of departure to collect information regarding employees, assets and the services they deliver, but many other offices and officials within a department can provide more specialized input, depending upon the subject and the scope of the assessment. Some external resources might be consulted as well, especially with respect to environmental assets. Appendix B-1 lists a variety of potential data sources and the types of assets they might identify for a TRA Team.

2.8 Data Collection Techniques

Interviews and questionnaires can be useful methods for collecting asset data, but they may become onerous and labour intensive for larger facilities and systems. Therefore, it is often preferable to commence with a review of relevant documents including business plans, architectural drawings and design documentation. Then, with a better understanding of the assets in question, the TRA team can organize more focused meetings with both technical and business authorities to obtain further details and clarify any points of contention. This approach is more likely to minimize the impact on operational activities. Field inspections or visits are frequently useful to corroborate initial findings. In some cases, data base queries against inventories and asset management systems can provide further details. Finally, the *Harmonized TRA Methodology* includes a comprehensive list of assets in Appendix B-2 as an aide-mémoire during the asset identification process.

2.9 Asset Listing

2.9.1 Hierarchical Structure

The Asset Listing in Appendix B-2 is presented as a hierarchical table ranging from broad asset classes and categories at the higher level through more detailed asset groups, subgroups and even discrete components for increasingly granular analysis. This structure is illustrated in Figure B-2.

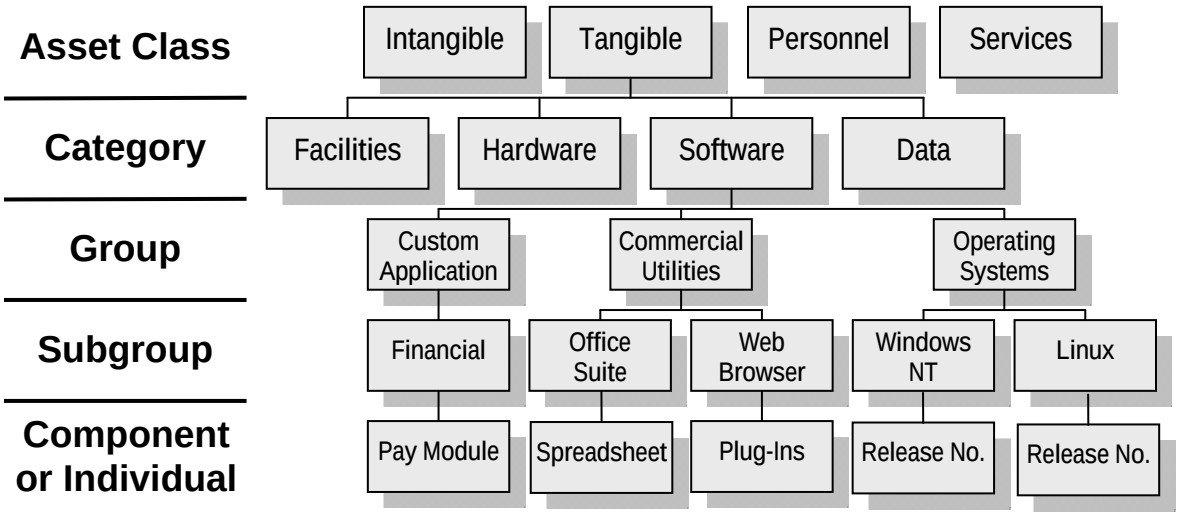

Figure B-2: Sample Segment of the Asset Listing Hierarchical Structure

2.9.2 Potential Benefits

The hierarchically structured Asset Listing offers several important advantages when conducting a TRA project:

- **Consistency.** The use of common data structures for asset identification facilitates communications within and between TRA projects to achieve consistent results that can be reproduced by different practitioners assessing the same or similar assets. It also promotes interoperability and supports asset sharing between organizations.
- **Completeness.** Important assets are less likely to be overlooked with the use of a comprehensive list to guide TRA teams.
- **Flexibility and Scalability.** Most importantly, the hierarchical structure of the Asset Listing permits analysis at different levels of detail, consistent with the scope of the assessment and the actual risk environment. In essence, less valuable assets subject to lower threats might be rolled up and evaluated in larger groups, while those at greater risk might be examined down to the subgroup or component level for greater precision. Similarly, entire branches of the tree-like structure might be ignored entirely if any particular asset category or group falls outside the scope of the assessment. Thus, TRA teams may constrain their efforts to concentrate on what is really important, as illustrated in Figure B-3.

- **Currency.** The Asset Listing is easily updated as new products or services are developed and deployed. Furthermore, given the logical groupings of similar assets, it is much simpler to categorize emerging technologies.

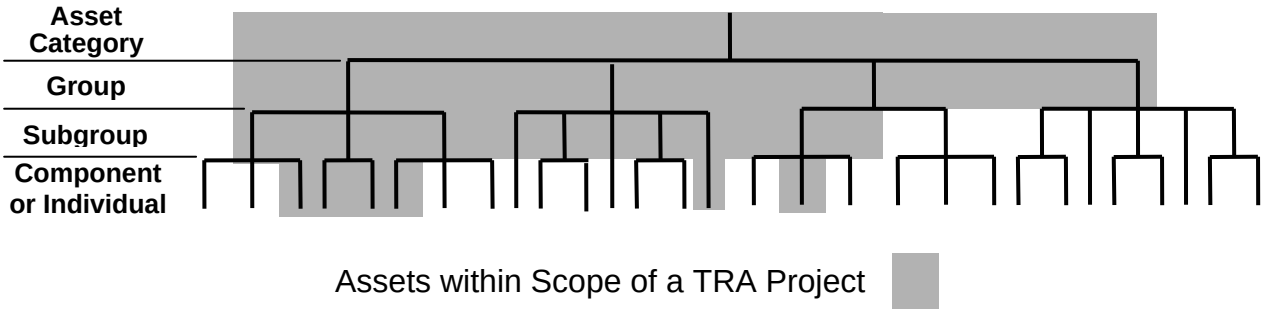

Figure B-3: Selecting Assets within the Scope of a TRA Project

2.9.3 Caveat

Despite these many benefits, the Asset Listing must be used with caution. It is not and can never be absolutely complete because new assets, especially at the component level of detail, are encountered on a regular basis due, in part, to rapidly changing technologies and emerging business opportunities. **Therefore, Appendix B-2 should be employed primarily as an aide-mémoire and guide to help organize and structure the collection and collation of relevant asset data, rather than a checklist to be followed without question.**

3 Injury Assessment

3.1 GSP Requirements

Section 10.6 of the GSP requires departments to categorize information and other assets according to the injuries that could reasonably be expected to arise from a compromise to their confidentiality, availability or integrity. If unauthorized disclosure could affect either the national or other interests adversely, the relevant assets must be identified as Classified or Protected and assigned markings based on the level of injury. With respect to availability and integrity, a similar ranking must be assigned based upon the degree of injury. The concept of value (heritage or monetary) is also introduced without specifying graduated injuries. The levels specified for confidentiality, availability and integrity are summarized in Table B-1.

GSP requirements are amplified in the Identification of Assets Operational Security Standard with many examples illustrating injuries at different levels arising from the compromise of confidentiality, availability, integrity or value. Conversely, the relationship between High Medium and Low injuries for Protected and Exceptionally Grave, Serious and simple Injury for Classified assets are not specified.

Confidentiality		Availability	Integrity
Classified (National Interest)	**Protected (Other Interests)**		
Top Secret Exceptionally Grave Injury	Protected C: High	High	High
Secret Serious Injury	Protected B: Medium	Medium	Medium
Confidential Injury	Protected A: Low	Low	Low

Table B-1: Asset Categorization Injury Levels Specified by the GSP

3.2 Comparative Analysis

3.2.1 Analytical Requirements

Quite clearly, assets may be assigned one or more values based on the anticipated impact or injury of a compromise. Furthermore, these assets may have the same or different values on each of the four or five scales (confidentiality (both Classified and Protected), availability, integrity and value). To permit consistent asset valuation and comparative analysis between different assets and asset values, and to determine their relative contributions to overall risk, the relationships amongst each of the four or five scales must be stated explicitly.

3.2.2 Aligning Asset Values

The GSP and the Identification of Assets Operational Security Standard provide several valuable indicators to suggest how the asset valuation scales may be harmonized. Firstly, the three injury levels defined for availability, integrity and value, namely Low, Medium and High, seem to correspond with Protected A, B and C respectively, as indicated in section 10.6(a) of the GSP. A similar correspondence with Classified values is slightly more complicated, but section 6.5.1.1 of the standard offers a frame of reference, acknowledging the continued existence of Restricted as a classification employed by certain allies and international organizations, and equating it with Protected A. As the next higher classification, Confidential might be aligned with Protected B and Medium injury levels, and Secret with Protected C and High injuries. At the high end of the spectrum, Top Secret sits alone with no Protected, availability, integrity and value counterparts, unless the Protected C and High ranges were extended to parallel both Secret (serious injury) and Top Secret (exceptionally grave injury). This approach has been rejected, however, because it could blur the distinction between Secret and Top Secret if both were equated to a High injury level on the Protected, availability and integrity scales.

3.2.3 Very High Asset Values

In extreme cases, the injuries arising from a compromise to availability and integrity could equal those caused by unauthorized disclosure of a Top Secret document. For example, unauthorized modification of patient records in a major metropolitan hospital could lead to widespread loss of life, as could a prolonged power outage in the middle of winter. Therefore, to permit more granular analysis for comparative purposes, the creation of an explicit threshold within the High range beyond which availability, integrity and value injuries would become Very High, the equivalent of Top Secret, seems a more appropriate solution.

3.2.4 Very Low Asset Values

At the other end of the spectrum, much information has little or no confidentiality value so it is properly categorized as Unclassified. Section 6.2 of the Identification of Assets standard also recognizes that, in some cases, the injuries arising from a compromise to availability or integrity may be negligible, thereby justifying a Very Low asset value comparable to Unclassified.

3.2.5 Comparative Injury Levels

Based on this rationale, requirements of the GSP and the related security standards, summarized in Table B-1, may be amplified and extended, as illustrated in Table B-2, to permit comparative analysis of different assets, asset values and their relative impact on residual risks based on a five-point scale ranging from Very Low to Very High.

Comparative Injury Levels	Type of Compromise				
	Disclosure		Destruction Interruption Removal	Modification	Destruction Removal
	Confidentiality		Availability	Integrity	Value
	Classified	Protected			
Very High	Top Secret		Very High	Very High	Very High
High	Secret	Protected C	High	High	High
Medium	Confidential	Protected B	Medium	Medium	Medium
Low	(Restricted)	Protected A	Low	Low	Low
Very Low	Unclassified		Negligible or Very Low		

Table B-2: Comparative Asset Values

Note: As a special case, if unauthorized disclosure of Protected information could cause a Very High injury, such as widespread loss of life, the results would undoubtedly affect the national interest, thereby warranting a Top Secret classification.

3.3 Injury Table

3.3.1 General

Although the consequences of compromise can vary considerably, depending upon the threat and the assets affected, the actual outcome can be reduced to one or more of three possible injuries, namely physical or psychological harm to human beings, or a financial loss.

3.3.2 Physical Harm

The physical impact on an individual could range from mild discomfort through minor and later serious injuries or illness to potential loss of life. The number of people affected by a single event is a second dimension to the assessment. In effect, widespread loss of life is more serious than the potential loss of a single human being.

3.3.3 Psychological Harm

Psychological effects on an individual can also be measured on a graduated scale ranging from minor inconvenience or embarrassment, through serious alarm or stress to major psychological trauma. Again, as the number of people affected grows, the severity of the injury will increase.

3.3.4 Financial Loss

Financial losses include many different expenditures or opportunity costs associated with a compromising threat event, such as the replacement value for lost or stolen equipment, reconstruction costs for damaged facilities or corrupted data, lost revenue, legal expenses in the event of litigation, and the cost of recruiting and training replacement staff. Once these varied possibilities have been assessed the relative financial injury may be ranked on a simple linear scale ranging from less than $1,000 to more than $1 billion.

3.3.5 Comparative Injury Table

Table B-3 offers an abbreviated version of the graduated injury scales used to determine asset values ranging from Very Low to Very High. Since the same measures apply to any type of compromise, to confidentiality, availability and integrity, the common Injury Table is a crucial element of the *Harmonized TRA Methodology* that permits comparative analysis of different values for one asset or varied assets with different values to determine which contribute to the greater risks. Appendix B-4 contains an expanded version of this table with further examples and explanations to facilitate the asset valuation process.

Level of Injury	Injury to People		Financial Impact
	Physical	Psychological	
Very High	Widespread Loss of Life	Widespread Trauma	> $1 billion
High	Potential Loss of Life	Serious Stress/Trauma	> $10 million
Medium	Injury/Illness	Public Suspicion/Doubts	> $100 thousand
Low	Discomfort	Minor Embarrassment	> $1 thousand
Very Low	Negligible	Negligible	< $1 thousand

Table B-3: Abbreviated Injury Table and Asset Values

3.3.6 High Water Mark

Any compromise to the confidentiality, availability or integrity of a single asset could cause injuries in two or three dimensions, both physical and psychological impacts on human beings and possibly a financial loss as well. Where the relative levels of these different injuries arising from a single threat event affecting one asset value (confidentiality, availability or integrity) differ, the higher level should be assigned as the ultimate asset value. For example, unauthorized disclosure of a single personnel file, a confidentiality compromise, might not cause physical harm to the subject, so the related physical injury level would be rated Very Low. If the loss were likely to invoke a penalty of $5,000, however, the financial injury level would be rated Low. On the other hand, the psychological impact on the person affected by the compromise and other individuals associated with the organization might be much more severe, causing public suspicion or doubts. Therefore, the information in question should be assigned a Medium confidentiality value (Protected B) on the basis of the psychological impact because, in this case, it is the most serious consequence of the confidentiality compromise.

4 Asset Valuation

4.1 General Considerations

All assets within the scope of a TRA project must be assigned one or more values based upon the level of injury that could reasonably be expected to arise in the event of compromise to their confidentiality (unauthorized disclosure), availability (unauthorized destruction, interruption, removal or use) or integrity (unauthorized modification). The actual level selected from the Expanded Injury Table in Appendix B-4 should reflect the worst case scenario, the maximum impact if the asset were completely compromised. In most cases, the actual damage and the associated risk will be much less for three reasons:

- firstly, threat events are rarely so overwhelming that they cause complete compromise, because deliberate threat agents are frequently less than totally capable and the magnitude of most accidents and natural hazards is not absolute;
- secondly, the likelihood or probability of occurrence for most threat events is something less than 100 percent; and
- thirdly, existing safeguards tend to mitigate the effects of many vulnerabilities, so the exposure to even serious threats may be reduced significantly.

Given these moderating factors, most risks are less than the actual asset value. As threats approach the worst case scenario, however, and as vulnerabilities become absolute, the resulting risk is maximized at the assigned asset value, as illustrated in Figure B-4.

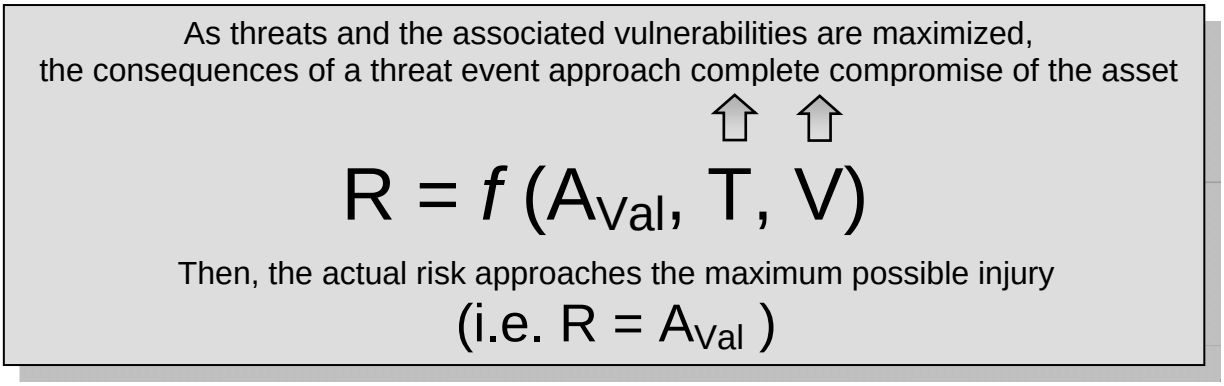

Figure B-4: Asset Values Based on Complete Compromise

4.2 Practical Application

4.2.1. General

While every asset must have at least one value (availability), very few, apart from data or information, will have all three or four (confidentiality, availability, integrity and value). Some of the following practical considerations will determine which of the three or four values apply to different assets in different circumstances.

> ***Confidentiality*** (*confidentialité*) - 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*.
>
> *Government Security Policy*, February 2002

4.2.2 Confidentiality

Confidentiality value, the degree of injury that could reasonably be expected to arise in the event of unauthorized disclosure, certainly applies to **information**, all of which may be categorized and assigned values ranging from Very Low (Unclassified) to Very High (Top Secret). Some **physical assets** may also warrant protection for reasons of confidentiality. For example, unauthorized access to some military equipment may reveal operational capabilities; other products might be analyzed to determine trade secrets, using reverse engineering techniques if necessary; and some security hardware might be studied by potential adversaries to discover exploitable vulnerabilities. In each case, unauthorized disclosure of the assets' attributes or characteristics could cause discernable injuries, so the material concerned must be identified and assigned appropriate confidentiality values. Although information about **employees** and other **personnel** may be sensitive to unauthorized disclosure, and individuals must possess security clearances or reliability status in order to access Classified or Protected information, human beings are not normally assigned confidentiality values. In some rare cases, unauthorized disclosure of certain physical attributes, such as fingerprints or other biometric measures, may cause injury and warrant categorization for confidentiality purposes. Although information related to many government **services**, such as clients' personal data, may have confidentiality values, the actual services may not. For example, neither the collection of census data, nor the related forms are sensitive, at least until they are completed. In effect, the service has no confidentiality value, but the data does. In other cases, unauthorized disclosure of the actual service, such as certain medical procedures, may cause injury and therefore warrant categorization for confidentiality.

4.2.3 Availability

> ***Availability*** (*disponibilité*) - the condition of being usable on demand to support operations, programs and services.
>
> *Government Security Policy*, February 2002

Availability value, the degree of injury that could reasonably be expected to arise in the event of unauthorized destruction, interruption, removal or use, applies to all **assets**, both tangible and intangible, **personnel** and **services**. Employees and other personnel are a special case, with potentially two different availability values. From an occupational health and safety perspective, when considering risks associated with violence in the workplace and other direct threats to people, the **intrinsic value** of one person or a small group is High, while that of a larger assembly is by definition Very High. Where the risks do not involve direct physical harm to employees and others, their availability value is normally determined by the likely injuries if

they were unable to perform their assigned duties. For example, the **intrinsic availability value** of a single pay clerk would be High whatever task he or she might perform. On the other hand, the individual's **operational availability value** would be assigned according to the impact on business functions and clients of his or her absence. Similar considerations apply to most tangible assets, such as information, IT systems and facilities. Their availability values are generally derived from the importance of the services they support. Finally, the availability values of intangible assets tend to reflect the psychological impact of service interruptions on clients and the general public.

4.2.4 Integrity

> ***Integrity*** (*intégrité*) - the accuracy and completeness of assets, and the authenticity of transactions.
>
> *Government Security Policy*, February 2002

Integrity value, the degree of injury that could reasonably be expected to arise in the event of unauthorized modification, applies primarily to **information**. Some other **physical assets**, such as measuring instruments, alarms or sensors, might also be sensitive to unauthorized modification which could cause false readings with potentially confusing or misleading results. Although the term integrity is frequently used to describe an employee's honesty or reliability, **personnel** are not really subject to unauthorized modification, so people are not assigned integrity values in the context of the *Harmonized TRA Methodology*. Of course, any attempt to undermine an individual's loyalty or reliability is a matter of concern and should, therefore, be examined during the Threat Assessment Phase (Annex C), while any susceptibility to subversion or recruitment is a personal attribute that should be considered during the Vulnerability Assessment (Annex D). For similar reasons, **intangible assets** are not assigned integrity values. Conversely, many **services** can be affected adversely by unauthorized modification of processes or procedures, so these should be assigned integrity values based upon likely injuries.

4.2.5 Value

> ***Value*** (*valeur*) - estimated worth, monetary, cultural or other.
>
> *Government Security Policy*, February 2002

The fourth measure of asset value is, perhaps, the least useful in the context of the *Harmonized TRA Methodology* for several reasons. Most significantly, the other three injury scales for confidentiality, availability and integrity take into account all types of damage arising from a compromising threat event. For example, monetary value or replacement cost would be subsumed under the financial impact of unauthorized destruction or removal. The cultural value of even a "priceless" painting or sculpture might be expressed in terms of the psychological impact on the art community and the general public if it were lost, stolen or destroyed, and a dollar value based on its likely bidding price at auction. Since confidentiality, availability and integrity values are assigned to reflect the maximum injury that could reasonably be expected in the event of a complete compromise of an asset, they tend to drive the calculation of residual risk following the threat and vulnerability assessments. In a few cases, however, the straight dollar value or replacement cost of an asset may be worth noting independently of the availability value. Typically, this could occur when unauthorized destruction, interruption or removal of an asset might disrupt service delivery, thereby causing some level of physical or psychological injury and financial loss. While these are generally the greater impacts and, therefore, warrant more attention in the balance of the assessment, lesser

risks associated with petty theft or pilferage may still require some consideration relative to the lower injury or replacement cost.

4.2.6 Multiple Values

In cases where an asset has more than one value based upon the different injuries arising from compromise, the assigned levels may be different. For example, unauthorized modification of a medical file might be life threatening, a High integrity value, whereas unauthorized disclosure might cause serious embarrassment and public concern, a Medium confidentiality value. Therefore, to differentiate which assets and asset values contribute to the greater risks, confidentiality, availability and integrity values are assessed and assigned independently for all applicable assets.

4.3 Other Issues

4.3.1 General

The asset valuation process in a TRA project may be complicated by several secondary considerations such as changing asset values over time, the effects of aggregation and inference, and some administrative or security conventions that occasionally skew asset values away from the actual injury levels that could reasonably be expected in the event of compromise. Where appropriate, these concerns may be factored into the assessment of asset values based upon the graduated injury levels.

4.3.2 Variable Asset Values

Asset values are not necessarily constant and may, in fact, vary considerably over time, increasing or decreasing for a variety of reasons. For example, the federal budget is assigned a High confidentiality value (Secret) throughout its development, but once it is announced most of the associated information becomes public knowledge. In other words, the confidentiality value drops to Very Low (Unclassified). The same is frequently true of research data until patents are approved, military plans until they are executed and business negotiations until they are concluded. To a more limited degree, confidentiality values may increase over time because the injury arising from unauthorized disclosure may rise as plans or programs mature and the relevant data become more focused or precise. Availability values can be equally volatile. Although a widespread power outage in summer months could cause serious injuries, a similar interruption of service in mid-winter could have disastrous consequences with extensive loss of life. Availability values for some assets may change upward or downward in response to different business cycles, such as year-end accounting or summer leave periods. Integrity values tend to be more stable, but the consequences of errors or omissions can become more critical as deadlines approach because normal verification mechanisms may be too slow or cumbersome. Finally, dollar values or replacement costs frequently appreciate or depreciate depending upon the nature of the assets. Since different safeguards may be required as asset values change, both high and low measures should be noted in the Asset Valuation List or Statement of Sensitivity.

4.3.3 Aggregation and Inference

As indicated in Section 6.3 of the Identification of Assets standard, aggregation and inference are two factors to consider when categorizing assets.

Aggregation *(Regroupement)* — the situation where a collection of assets may be categorized at a higher level of sensitivity than its component parts due to the increased injury that could result if it is compromised. Generally aggregation applies to confidentiality, but it can also apply in certain circumstances to availability and integrity.

Section 2, *Identification of Assets* standard.

- **Aggregation.** As the number of assets increases, the injuries arising from compromise may grow as well. For example, unauthorized disclosure of a single personnel file might be expected to cause some embarrassment to the individual and generate public anxiety regarding an organization's ability to protect personal information. If all human resource (HR) records for a major department were released inappropriately, however, the adverse effects could be significantly worse. From a confidentiality perspective, aggregation has two dimensions: sensitivity tends to increase as more data elements are added to a record, and as more records are collected in a file or data base. In each case the confidentiality value of the whole may be greater than that of the individual parts, based upon the increased injury expected in the event of unauthorized disclosure. Aggregation applies equally to availability and integrity values. For example, the destruction of one asset, such as a single vehicle, might have clearly defined consequences, whereas the loss of an entire fleet would be much more serious. Unauthorized modification of a single record or complete corruption of a large data base would be the integrity equivalent. In each case, the *Harmonized TRA Methodology* facilitates the analysis of increasing asset values associated with aggregation because the graduated levels presented in Appendix B-4, the Expanded the Injury Table, may be applied with complete confidence to categorize single assets or large groupings accurately and consistently without under or over-estimating their worth.
- **Inference.** By its very nature, inference applies only to confidentiality, where access to seemingly innocuous data of little or no sensitivity may allow a knowledgeable individual to draw much more damaging conclusions regarding another organization's capabilities or intentions. For example, studying personnel movements to identify the qualifications and affiliations of executives and other employees selected for different positions may provide useful indicators of future policy platforms or business plans. Unfortunately, the relationships amongst different data and data sources may be very subtle, even tenuous, so opportunities for inference are generally far more difficult to identify and assess. Nevertheless, where the possibility exists, the graduated Injury Table does permit objective asset valuation of the inferred conclusions. From a practical point of view, inference must be assessed cautiously because complex scenarios can exaggerate the risk and lead to needless overclassification.

Inference *(inférence)* – the situation where assets categorized at one level of sensitivity may be analyzed to draw conclusions that could result in greater injury.

Section 2, *Identification of Assets* standard.

4.3.4 Asset Valuation Conventions

In some cases, asset values for confidentiality are assigned according to administrative or operational conventions rather than a scrupulous application of the injury tests. For example, records and drafts that constitute confidences of the Queen's Privy Council for Canada and fall within the Cabinet Papers System are usually classified Secret,[4] a High asset value, whatever the actual injury that might reasonably be expected in the event of unauthorized disclosure. Much personal information is categorized Protected B, a Medium asset value, even in cases where the most likely injury arising from unauthorized disclose might be mild embarrassment or frustration. Similarly, some operational plans and intelligence documents are routinely classified Secret and Top Secret without reference to the probable consequences of compromise. Although strict adherence to these conventions may artificially elevate the assessed levels of residual risk in a TRA project, the rules should not be questioned. In some rare cases, however, it may be useful to reassess the residual risk using more realistic asset values to determine whether some other safeguards may be more appropriate under the circumstances.

5 Prioritized Asset Valuation Table/Statement of Sensitivity

As indicated above, every asset within the scope of the TRA project must be assigned one or more values based upon the maximum injuries that could reasonably be expected in the event of compromise. Confidentiality values indicate the most serious consequences of unauthorized disclosure; availability values reflect the potential impacts of unauthorized destruction, interruption, removal or use; while integrity values denote the worst effects of unauthorized modification. In some cases, dollar values or replacement costs may be recorded separately for analytical purposes. For greater refinement, asset values that fall near the boundary between two levels might be highlighted for re-examination during the final Calculation of Residual Risk.[5] Then, all of these values should be recorded in an Asset Valuation Table, also known as a Statement of Sensitivity, the final output of the Asset Identification and Valuation Phase of a TRA project. Simply sorting by asset values, from Very Low to Very High, can quickly prioritized assets and identify those of greatest value.

This list is illustrated in Table B-4 and amplified in Appendix B-5.

[4] See Appendix B of the Identification of Assets Operational Security Standard.
[5] See section 2.4.3 of Annex E for an explanation of this particular option.

Class	Category	Group	Subgroup	Component	C	A[6]		I	$
						i	o		
Legend C – Confidentiality Value. A – Availability Value. i – Intrinsic Availability Value for Personnel. o – Operational Availability Value for Personnel. I – Integrity Value. $ - Replacement Cost.									

Table B-4: Sample Asset Valuation Table/Statement of Sensitivity

[6] As indicated in Section 4.2.2, personnel may be assigned two asset values for availability, intrinsic value (i) where there are threats of violence and operational value (o) reflecting the impact of their absence on service delivery.

Appendix B-1 - Sources of Asset Data

DEPARTMENTAL RESOURCES	
Data Source	**Types of Assets**
• Program Managers	• Business Plans/Services • Employees • Office Equipment/Supplies • Budget/Finances • R&D Reports
• Project Managers	• Design Documentation • Floor Plans • Equipment Schematics/As Built Drawings • Operating Procedures
• Material/Asset Managers	• Inventories • Contract Documentation • Vehicles
• Facility Managers	• Building Plans • Emergency Services o Fire o Paramedics o Police • Heating/Ventilation/Air Conditioning Systems • Physical Security Measures o Alarms o Access Controls • Public Utilities o Electricity o Sewer o Water
• Human Resources	• Employees • Approved Positions/Qualifications • Personal Data
• Finance	• Budgets • Program Costs
• Chief Information Officer	• IT Infrastructure • Common/Shared Applications
• Systems (Security) Administrator	• Hardware/Software Configurations • Technical Security Measures
• Audit and Review	• Audit Reports/Reviews

DEPARTMENTAL RESOURCES	
Data Source	**Types of Assets**
• Departmental Security Officer	• Physical Security Measures • Security Plans/Inspections
• IT Security Coordinator	• Technical Security Measures
• BCP Coordinator	• Business Impact Analyses
• ATIP Coordinator	• Privacy Impact Assessments
• Occupational Health and Safety Officer	• Health and Safety Equipment/Procedures

EXTERNAL RESOURCES	
Data Source	**Types of Assets**
• Building Custodians	• Building Plans • Heating/Ventilation/Air Conditioning Systems • Public Utilities • Physical Security Measures/Alarms/Access Controls
• Public Utilities	• Power/Water Services
• Emergency Services	• Fire/Police/Paramedics
• Service Providers	• Communications Infrastructure
• Product Vendors	• Product Descriptions/Specifications/Schematics
• Clients	• Products and Services

Note: The foregoing list of sources for asset information is not complete. It is merely intended to provide a useful point of departure for the data collection process. Other possibilities will be added and amplified from time to time. Any suggestions for further references or contacts may be submitted to the offices identified in the Foreword.

Appendix B-2 - Asset Listing

Class	Category	Group	Subgroup	Component/Individuals
People	Employees	Senior Executives		
		Program Staff	Managers	
			Supervisors	
			Business Analysts	
			Engineers	
			Scientists	
			Production Workers	
		Policy Analysts		
		Marketing Specialists		
		Communications		
		Legal Counsel		
		Auditors		
		Project Management	Project Director	
			Project Manager	
			System Architects	
			Application Programmers	
			Hardware Engineers	
			Technical Writers	
		IT Staff	Systems Administrators	
			Security Administrators	
			Software Maintainers	
			Hardware Technicians	
			Helpdesk Operators	
		Support Staff	Administrative Assistants	
			Records Management Staff	
			Drivers	
			Couriers	
		Translators		
		Facility Management	Building Manager	
			Cleaning Staff	
			Electricians	
			HVAC Technicians	
			Plumbers	
		Finance	Accountants	
			Accounts Payable Clerk	
			Accounts Receivable Clerk	
		Human Resources	Classification	
			Staffing	
			Staff Relations	
			Trainers	
			Employee Assistance	
		Occupational Health/Safety	Analysts	
			Investigators	
		BCP Staff		
		Intelligence	Intelligence Analyst	

Class	Category	Group	Subgroup	Component/Individuals
			Collator	
		Security	Management	
			Analysts	
			Business Continuity Planning	
			Investigators/Inspectors	
			IT Security Staff	
			COMSEC Custodian	
			Guards	
			Alarm Console Operator	
	Contractors	(any of the above)		
	Subcontractors	(any of the above)		
	Product Vendors	(any of the above)		
	Service Providers	(any of the above)		
	Other Governments	(any of the above)		
	Allied Agencies	(any of the above)		
	Academic Institutions	(any of the above)		
	Clients			
	Public			
Tangible	Information	Personal Data	Employees	Identification
				Education and Training
				Other Qualifications
				Employment History
				Appraisals
				Disciplinary Records
				Medical History
				Pay and Allowances
				Leave Records
				Security Screening File
				Criminal Records
			Clients	Identification
				Income
				Credit History
				Transaction History
				Account Balances
		Cabinet Documents		
		Policies/Standards	Federal Policies	Government Security Policy
				Access to Information Policy
				EAA Policy
				Privacy Policy
				Other Policies
			Federal (Security) Standards	Business Continuity Planning
				Identification of Assets
				Management of IT Security
				Physical Security
				Readiness Levels
				Security in Contracting
				Security of Information Act
				Security Risk Management
				Security Screening
				Security Training/Awareness
			Departmental Policies	Security

Class	Category	Group	Subgroup	Component/Individuals
				Other
		Business Plans	Business Strategies	
			Marketing Plans	
			Client Lists	
		Financial Records	Expenditure Plans	
			Annual Reports	
			Payroll	Salaries
				Benefits
			O&M Budget	Travel
				Supplies
			Service Pricing	
			Transactions	Accounts Payable
				Accounts Receivable
			Capital Budget	IT Equipment
				Other Materiel
		Routine Correspondence		
		Audit Reports	Internal Audits	
			Reviews	
		Project Documentation		
		Architectural Documents		
		System Documentation	Vendor Manuals	
		Scientific/Technical Data	R&D Proposals	
			Research Papers	
			Experimental Data	
		Legal Files	Case Files	Civil Proceedings
				Criminal Proceedings
			Legal Opinions	
			Contracts	
			MOUs	Information Sharing
				International
				Other Governments
				Private Sector
		Police/Criminal Records	Investigation Reports	
			Witness Statements	
			Criminal Records	Fingerprint Files
			Evidence	
		Intelligence Reports	Political	
			Economic	
			Security	Intelligence Services
				Foreign Influenced Activities
				Terrorism
			Criminal Intelligence	
			Open Source	
		Third Party Information	Allied Agencies	
			Other Governments	Provincial
				Municipal
			Critical Infrastructure	Financial Institutions
				Health Sector
				Public Utilities
				Telecommunications Sector
				Transportation Sector
			Other Private Sector	Vendors Non-Disclosure

Class	Category	Group	Subgroup	Component/Individuals
				Trade Secrets
	Hardware	Processors	Supercomputers	
			Mainframes	
			Mini-Computers	
			Servers	
			Personal Computers	Hard Drive
				Memory Chips
				Math Co-Processor
				Network Card
				Keyboard
				Monitor
				Mouse
				Speakers
			Notebooks	
			Personal Digital Assistants	Blackberries
		Peripherals	Printers	
			Scanners	
			Disk Packs	
		Network Components	Routers	
			Hubs	
			Cabling	Fibre Optic
				Co-Axial
				Twisted Pair
			Firewalls	
			Wireless Devices	
		Security Components	Cryptographic Devices	
			Biometric Equipment	Retinal Scanner
				Thumb Print Reader
			Advanced Card Technologies	
			Secure Remote Access Devices	
		Media	Tapes	
			Diskettes	
			CDs	
			DVDs	
			CD ROM	
			USB Drives	
			Hard Drives	
	Firmware			
	Software	Operating Systems	Windows NT	Release/Patch
			Windows XP	Release/Patch
			Linux	Release/Patch
			Solaris	Release/Patch
		Commercial Applications	Office Automation	Microsoft Word
				Microsoft PowerPoint
				Microsoft Excel
				Corel WordPerfect
				Lotus WordPro
			Electronic Messaging	Microsoft Outlook
			Web Browsers	Microsoft Internet Explorer
				Netscape Communicator
			Graphics Packages	Corel Draw
				Adobe Illustrator/Photoshop

Class	Category	Group	Subgroup	Component/Individuals
				AutoCad
		Customized Applications	Financial Systems	Source Code
				Object Code
			Personnel Systems	Source Code
				Object Code
			Material Management	Source Code
				Object Code
		Security Utilities	Encryption Packages	Entrust
				PGP
				SecureDoc
			Virus Detection Software	McAfee VirusScan
				Norton AntiVirus
			Intrusion Detection Systems	Network Based
				Host Based
			Intrusion Prevention Systems	Network Based
				Host Based
		Third Party/Leased Software	(any of the above)	
		Shareware	(any of the above)	
		Freeware	(any of the above)	
	Facilities	Buildings	Office Accommodations	Enclosed Offices
				Open Office Accommodation
				Reception Areas
				Sensitive Discussion Areas
				Secure Rooms
				Shielded Enclosures
			Data Centres	
			Wiring Closets	
			Medical Facilities	Doctors' Offices
				Patient Accommodations
				Operating Theatres
				Medical (Drug) Storage
			Storage and Warehousing	
			Laboratories	
			Security Facilities	Operations Centres
				Information Protection Centres
				Guard Stations
		HVAC Systems	Heating System	
			Ventilation Fans	
			Air Conditioning	
		Plumbing Systems		
		Electrical Systems	Wiring	
			Circuit Breakers	
		Office Furnishings	Desks	
			Chairs	
			Storage Cabinets	
		Other Office Equipment	Photo-Copiers	Non-Memory Resident
				Memory Resident
			Facsimile Machines	Non-Memory Resident
				Memory Resident
			Telephones	Desktop
				Cellular
		Office Supplies	Stationary	

Class	Category	Group	Subgroup	Component/Individuals
			Pre-Printed Forms	
	Security Devices	Alarm Systems	Intrusion Alarms	Area Sensors
				Contact Switches
				Monitor Consoles
			Smoke Detectors	
			Fire Alarms	
		Security Containers		
		Locks		
		Shredders		
		Cryptographic Devices		
		Biometric Equipment	Retinal Scanner	
			Thumb Print Reader	
		Advanced Card Technologies		
	Processes	Business Processes		
		System Engineering Processes	Capacity Management	
			Change Management	
			Configuration Management	
			Patch Management	
			Release Management	
			System Development Life Cycle	Planning for Change
				Requirements Definition
				Architectural Design
				Detailed Design
				Implementation
				Testing & Evaluation
		Security Processes	Access Management	
			Authorization	
			Business Continuity Planning	
			Identification & Authentication	
			Certification & Accreditation	Departmental Programs
				Shared/Common Services
			Security Incident Handling	
		Operating Procedures	Manual Processes	
			IT Operating Instructions	
			Configuration Mgt. Plans	
			Emergency Procedures	
	Others	Vehicles	Passenger Vehicles	
			Trucks	Light Vans
				Heavy Transports
			Forklifts	
			All Terrain Vehicles	
			Emergency Vehicles	Ambulances
				Patrol Cars
				Fire Trucks
				Snow Removal Equipment
			Construction Equipment	Bulldozers
				Road Graders
				Back Hoes
				Cranes
			Prototypes	
		Ships/Boats		

Class	Category	Group	Subgroup	Component/Individuals
		Aircraft		
		Medical Supplies	Medications	Drugs
				Vaccine
			Medical Equipment	
		Hazardous Materials	Combustible Liquids	
			Compressed Gases	
			Corrosive Chemicals	
			Flammable Aerosols	
			Flammable Gases	
			Flammable Liquids	
			Flammable Reactive Agents	
			Flammable Solids	
			Oxidizing Agents	
			Reactive Agents	
	Negotiable Instruments	Cash	Canadian Currency	
			Foreign Currency	
		Cheques		
		Bonds		
		Precious Gems		
		Precious Metals		
Services	Government Services	Agriculture and Agri-Food	(Departmental Business Lines)	
		Heritage	(Departmental Business Lines)	
		Citizenship/Immigration	(Departmental Business Lines)	
		Environment	(Departmental Business Lines)	
		Finance	(Departmental Business Lines)	
		Fisheries and Oceans	(Departmental Business Lines)	
		Foreign Affairs	(Departmental Business Lines)	
		International Trade	(Departmental Business Lines)	
		Human Resources	(Departmental Business Lines)	
		Indian Affairs	(Departmental Business Lines)	
		Northern Development	(Departmental Business Lines)	
		Industry	(Departmental Business Lines)	
		Justice	(Departmental Business Lines)	
		National Defence	(Departmental Business Lines)	
		Natural Resources	(Departmental Business Lines)	
		PSEPC	(Departmental Business Lines)	
		PWGSC	(Departmental Business Lines)	
		Transport	(Departmental Business Lines)	
		Treasury Board	(Departmental Business Lines)	
		Veterans' Affairs	(Departmental Business Lines)	
		Network Services	Local Area Network	
			Remote Access	
			Wireless Access	
			Internet Services	High Speed
				Dial Up
		GoC Shared Services		
	Environmental Services	Public Utilities	Electricity	
			Water	
			Sewer	
			Natural Gas	
			Garbage Collection	
			Snow Removal	

Class	Category	Group	Subgroup	Component/Individuals
			Highway Maintenance	
		Telecommunications	Telephone	
			Television	Cablevision
			Other IT	Service Bureaus
				Consultants
		Emergency Services	Police	Federal
				Provincial
				Municipal
			Fire	
			Medical	Ambulance
				Paramedic
Intangible	Internal	Employee Morale		
		Employee Confidence/Trust		
		Management Credibility		
	External	Public Confidence/Trust		
		Competitive Advantage		
		Product Identity		
		Organizational Credibility		

Notes:

1. Clearly, the Asset Listing is not and cannot ever be complete. New assets, especially at the component level of detail appear on a daily basis. Therefore, additional entries will be added from time to time. Any suggestions to expand the list may be submitted to the offices identified in the Foreword.
2. When developing a Statement of Sensitivity for a TRA project, all assets within the scope of the assessment may be transferred at the appropriate level of detail from the Asset Listing above to the first five columns of the Asset Valuation List/Statement of Sensitivity presented at Appendix B-5.

Appendix B-3 - BIA, PIA and TRA

1 Introduction

1.1 General

Business Impact Analysis (BIA) and the Privacy Impact Assessment (PIA) are mandatory requirements of the GSP, specifically section 10.14 on Business Continuity Planning, and the PIA Policy respectively. As analytical processes, both the BIA and PIA serve comparable purposes to the TRA. Therefore, a sound understanding of the similarities and dissimilarities amongst the three interrelated activities can enhance the utility and improve the effectiveness of these complementary disciplines.

1.2 Aim

The dual aim of this appendix is to compare and contrast the purpose, scope and content of the BIA, PIA and TRA, and suggest how they may be applied in a coordinated manner.

2 Purpose

According to the GSP and the PIA Policy, the three activities serve similar purposes, albeit with some distinct differences. The primary goals of each process may be summarized as follows:

- **BIA** – "to identify and prioritise the department's critical services and assets."[1]
- **PIA** – "to ensure that privacy is considered throughout the design or re-design of programs and services" and provide "assurance that all privacy issues have been identified and resolved or mitigated."[2]
- **TRA** – "to determine the necessity of safeguards beyond baseline levels."[3]

In short, all three processes involve an element of analysis in support of recommendations for future action to address various risks. With a BIA, the prioritized list of critical services and assets provides an objective basis for selecting suitable BCP plans, measures and arrangements to address availability risks. In a similar fashion, the PIA helps responsible authorities make fully informed policy, system design and procurement decisions to avoid or mitigate privacy risks. Finally, the TRA identifies unacceptable risks to employees, assets and service delivery, and recommends additional safeguards beyond baseline controls to achieve cost-effective security solutions.

1 GSP, section 10.14(b).
2 PIA Policy, page 2.
3 GSP, section 10.7.

3 Scope

3.1 General

Although the BIA, PIA and TRA are complementary analytical methods for assessing and ultimately mitigating various risks, the scope of the three activities can differ significantly.

3.2 Scope of a TRA

In general, the TRA tends to encompass a broader array of assets and asset values than either the BIA or PIA. Depending upon the subject of the assessment, a TRA might analyze risks to all assets (tangible, intangible, personnel and services) and asset values (confidentiality, integrity and availability), as illustrated in Figure B3-1.

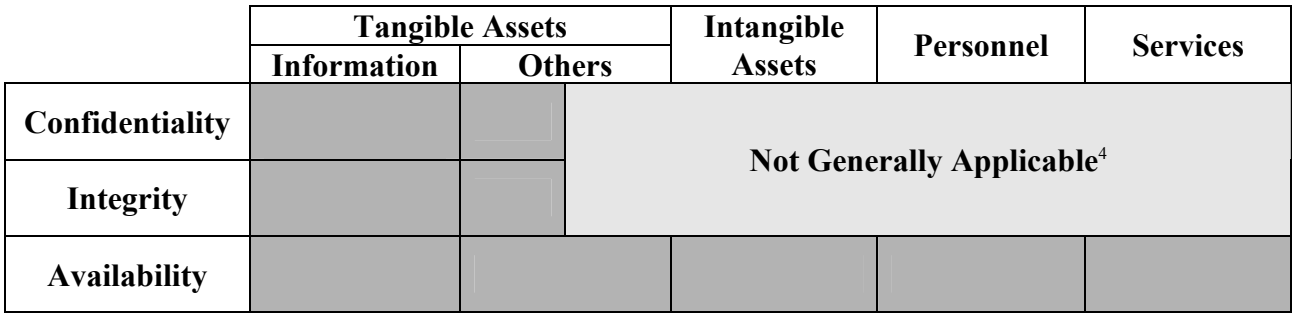

Figure B3-1: Scope of a TRA

3.3 Scope of a BIA

In order to identify critical assets and services, the BIA concentrates on the availability and, to a lesser extent, integrity values of assets whose compromise (unauthorized destruction, removal, modification, interruption or use) could cause a high degree of injury. Of course, confidentially concerns must be addressed during the subsequent selection and implementation of BCP plans, measures and arrangements, but assets with high and very high availability values remain the primary focus of a BIA, as illustrated in Figure B3-2.

[4] As explained in section 4.2 of Annex B, the Asset Identification and Valuation Phase, confidentiality and Integrity values are not normally applicable to personnel, services and intangible assets.

<table>
<tr><th></th><th colspan="2">Tangible Assets</th><th rowspan="2">Intangible Assets</th><th rowspan="2">Personnel</th><th rowspan="2">Services</th></tr>
<tr><th></th><th>Information</th><th>Others</th></tr>
<tr><td>Confidentiality</td><td></td><td></td><td colspan="3" rowspan="2">Not Generally Applicable[5]</td></tr>
<tr><td>Integrity</td><td></td><td></td></tr>
<tr><td rowspan="2">Availability</td><td colspan="5">Critical Assets and Services</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Figure B3-2: Scope of a BIA

3.4 Scope of a PIA

The PIA only applies to programs and services that handle personal information, an important but limited subset of tangible assets. Other information, facilities, personnel, services and intangible assets generally fall outside the scope of assessment. Unlike the BIA, however, the PIA considers all three dimensions of asset value, assessing risks to confidentiality and integrity as well as availability, as illustrated in Figure B3-3.

<table>
<tr><th></th><th colspan="3">Tangible Assets</th><th rowspan="2">Intangible Assets</th><th rowspan="2">Personnel</th><th rowspan="2">Services</th></tr>
<tr><th></th><th colspan="2">Information</th><th>Others</th></tr>
<tr><td>Confidentiality</td><td rowspan="3">Personal Info.</td><td></td><td></td><td colspan="3" rowspan="2">Not Generally Applicable[6]</td></tr>
<tr><td>Integrity</td><td></td><td></td></tr>
<tr><td>Availability</td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Figure B3-3: Scope of a PIA

4 Content

4.1 Analytical Processes

4.1.1 BIA

The BIA is the second of five elements in a complete BCP program described in section 10.14 of the GSP. The others include BCP governance, BCP plans and arrangements, BCP program readiness, and continuous review testing and audit. Section 3.2 of the *Operational Security Standard – Business Continuity Planning (BCP) Program* identifies five steps within the BIA to

[5] As explained in section 4.2 of Annex B, the Asset Identification and Valuation Phase, confidentiality and Integrity values are not normally applicable to personnel, services and intangible assets.

[6] As explained in section 4.2 of Annex B, the Asset Identification and Valuation Phase, confidentiality and Integrity values are not normally applicable to personnel, services and intangible assets.

establish a sound basis for subsequent recommendations regarding appropriate BCP plans, measures and arrangements. As indicated in Table B3-1, these five steps (identify business lines/services, determine impact of disruptions, assess high level injuries, identify/prioritize critical services, and obtain management approval) correspond closely to the Data Analysis component of a PIA and the Asset Identification/Valuation Phase of a TRA. Thus, the BIA by itself is a more tightly constrained activity than either the PIA or the TRA. That being said, other elements of a complete BCP Program, such as the selection of BCP plans and arrangements, match the Conclusion and Path Forward portion of a PIA and the Recommendations Phase of a TRA to establish closer parallels. Finally, a BCP Program has no equivalent to the Threat Assessment and Risk Assessment Phases of a TRA because the inevitability of disruptive threat events is an underlying assumption throughout the analytical process.

4.1.2 PIA

The *Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks* prescribe a four-step PIA process: (1) Project Initiation; (2) Data Analysis; (3) Privacy Analysis; and (4) Privacy Impact Assessment. An examination of the subordinate activities within each step reveals that Project Initiation is substantially the same as the Preparation Phase of a TRA. Data Analysis corresponds closely with the Asset Identification and Valuation Phase. As with the BIA, there is no equivalent to the Threat Assessment Phase, but Privacy Analysis is similar to the Risk Assessment and Recommendation Phases of a TRA. Thus, the purpose and scope of a PIA are certainly more focused than those of a TRA, but there remains a strong resemblance between the analytical processes to assess and mitigate risks.

4.1.3 TRA

With its unique Threat Assessment Phase and a more explicit Vulnerability Assessment, a typical TRA tends to be longer with many more details than either the BIA or PIA. Nevertheless, the Calculation of Residual Risk and Recommendations Phase map very well with the Privacy Impact Assessment step of a PIA and the BCP Plans and Arrangements element of a BCP Program. As noted above, these relationships are illustrated in Table B3-1.

BCP Program	PIA	TRA
BCP Governance • Establish Management Committee • Appoint BCP Coordinator	Project Initiation • Define Scope of PIA Process • Designate Team Resources • Adapt Tools to Reflect Scope	Preparation Phase • Establish TRA Mandate • Determine Scope of Assessment • Select TRA Team • Draft TRA Work Plan
Business Impact Analysis (BIA) • Identify Business Lines/Services • Determine Impact of Disruptions • Assess High Level Injuries • Identify/Prioritize Critical Services • Obtain Management Approval	Data Analysis • Describe Business Processes • Identify Personal Information • Develop Data Flow Charts	Asset Identification/Valuation • Identify Assets • Perform Injury Assessments • Assign Asset Values
		Threat Assessment • Identify Threats • Determine Threat Likelihood • Assess Threat Gravity • Assign Threat Levels
	Privacy Analysis • Complete Questionnaires • Analyze and Clarify • Describe Issues/Implications	Risk Assessment: Vulnerability Assessment • Identify Safeguards • Assess Safeguard Effectiveness • Identify Vulnerabilities • Analyze Vulnerability Impacts • Assign Vulnerability Levels
	Privacy Impact Assessment • Summarize Privacy Risks	Risk Assessment: Calculation of Residual Risk • Compute Residual Risks • Prioritize Residual Risks
BCP Plans and Arrangements • Develop Recovery Options • Assess Benefits/Costs • Obtain Management Approval • Develop Business Continuity Plans • Brief/Train Staff	• Identify Actions to Mitigate • Conclusion and Path Forward	Recommendations • Identify Unacceptable Risks • Select Potential Safeguards • Identify Associated Costs • Assess Projected Residual Risks
BCP Program Readiness • Ongoing Review/Revision • Additional Training • Regular Testing/Validation • Audit Cycle/Reporting to TBS		

Table B3-1: Comparative Mapping of BIA, PIA and TRA Processes

4.3 Comparative Metrics

Although the BIA includes an estimate of the minimum service levels and maximum allowable downtime, the final measure of availability value, a high level of injury, is not defined explicitly. Similarly, the PIA does not prescribe graduated scales for the sensitivity of personal information or the associated privacy risks. Conversely, the Harmonized TRA Methodology provides clear metrics for asset values, threats, vulnerabilities and residual risks to promote objective analysis.

5 Complementary Application

5.1 Inputs and Outputs

5.1.1 BIA/PIA as Inputs to a TRA

Both the BIA and PIA can be valuable inputs to a TRA project, especially the Asset Identification and Valuation Phase, as indicated in sections 5.4.6 and 5.5.1 of Annex A. The response to questionnaires A and B in the Privacy Analysis step of a PIA can also provide useful information for the Vulnerability Assessment, as can the mitigating factors or safeguards specified in the final step of the PIA.

5.1.2 TRA as an Input to a BIA/PIA

In the absence of either a BIA or PIA, the data collected during a TRA project may be culled to produce the other related documents, especially if this objective is clearly identified at the outset. For example, the Statement of Sensitivity in a TRA report should provide enough information to compile both a BIA and the Data Analysis step of a PIA. Then, the Vulnerability Assessment and Recommendations Phase should contain a thorough analysis of availability safeguards, including BCP plans and arrangements, the third element of a complete BCP program. Similarly, the information collected for the Vulnerability Assessment should address most of the questions in Questionnaires A and B of the Privacy Analysis step of a PIA, especially those related to the following privacy principles: (5) disclosure and disposition; (6) accuracy of personal information; (7) safeguarding personal information; and (9) individual's access to personal information.

5.2 Comparative Analysis

With concrete metrics, the TRA offers real opportunities to refine both the BIA and PIA to help prioritize BCP and privacy risks. This capacity for comparative analysis can be particularly useful to adjudicate the allocation of scarce resources when establishing BCP plans, measures and arrangements or selecting actions to mitigate privacy risks. In addition, the cost and the effectiveness of existing and proposed safeguards calculated during both the Vulnerability Assessment and Recommendations Phase of a TRA project provide concrete evidence that the proposed BCP plans, measures and arrangements, and the recommended actions to mitigate privacy concerns do, in fact, achieve acceptable levels of residual risk an affordable cost.

5.3 Program Evaluation

Both the GSP and the PIA Policy require ongoing compliance monitoring to determine the effectiveness of departmental BCP, privacy and security programs.[7] The TRA report for any facility, system or service provides an objective analysis of safeguard effectiveness and, therefore, vulnerabilities related to critical assets and services within a BCP program and personal information subject to the PIA Policy within the scope of the assessment. Furthermore, any unacceptable residual risks are identified in the Recommendations Phase along with proposals for remedial action. Thus, the analytical processes in a TRA project offer an ideal mechanism to evaluate the effectiveness of at least major elements of both the BCP and PIA programs, as well as a departmental security program generally.

6 Conclusion

In summary, the scope of a BIA, PIA and TRA may differ significantly, but the underlying purpose of each activity, to support informed risk management, is remarkably similar. Furthermore, clear parallels may be drawn between the internal processes of a complete BCP program, the PIA and a TRA, as illustrated in Table B3-1. Given the complementary nature of the three mandatory practices, the relationships amongst responsible authorities should be strengthened within and between departments in order to:

- achieve more consistent application of complementary and, therefore, cost-effective safeguards to address BCP, privacy and security risks in a holistic manner;
- reduce the overall workload by promoting the re-use of outputs from one process as inputs to another, as discussed in sections 5.5.1 and 5.5.2 above;
- minimize potential conflicts or tensions between confidentiality mechanisms recommended in a PIA or a TRA and availability measures identified in BCP plans and arrangements or another TRA; and
- better allocate scarce resources amongst complementary BCP, privacy and security programs.

[7] Section 11 of the GSP requires active monitoring and internal audits of departmental security programs, whereas section 10.14(d) requires departments to monitor overall BCP readiness. Page 10 of the PIA Policy requires departments to conduct internal reviews, audits and evaluations to assess their compliance with the policy.

This page intentionally left blank.

Appendix B-4 - Expanded Injury Table

Level of Injury	Injury to People		Financial Impact
	Physical	Psychological	
Very High	1. Widespread Loss of Life	1. Widespread Psychological Trauma 2. Potential Civil Unrest	> $1 billion
High	1. Potential Loss of Life for Some 2. Permanent Disability for Some 3. Serious Illness or Injury for Many 4. Serious Physical Hardship for Many	1. Serious Embarrassment for Many 2. Serious Doubts/Uncertainty for Many 3. Widespread Public Suspicion 4. Alienation of Large Groups	> $10 million
Medium	1. Serious Illness/Injury to Some 2. Serious Discomfort for Many 3. Minor Pain for Many	1. Serious Embarrassment for Some 2. Serious Doubts/Uncertainty for Some 3. Serious Inconvenience for Many 4. Minor Embarrassment for Many 5. Minor Doubts/Uncertainty for Many	> $100 thousand
Low	1. Serious Discomfort for Some 2. Minor Pain for Some 3. Minor Discomfort for Many	1. Serious Inconvenience for Some 2. Minor Embarrassment for Some 3. Minor Doubts/Uncertainty for Some 4. Minor Inconvenience for Many	> $1 thousand
Very Low	1. Negligible 2. Minor Discomfort for Some	1. Negligible 2. Minor Inconvenience for Some	< $1 thousand

Note: Although the threshold between "some" and "many" remains open to interpretation, one thousand people may be a useful demarcation.

1 Instructions

For each asset within the scope of the TRA project, assign appropriate asset values as follows:

1.1 Step One

Determine the relevant level of detail (Asset Group, Subgroup, Component or Individual) for subsequent analysis based upon the scoping considerations examined in section 4 of Annex A.

1.2 Step Two

Assess the maximum level of injury that could reasonably be expected to arise in the event of compromise:

- select the confidentiality value for information and other assets, where appropriate, based on the likely injury in the case of unauthorized disclosure;
- select the availability value for all personnel (both intrinsic and operational), assets, both tangible and intangible, and services based on the likely injury in the case of unauthorized destruction, interruption, removal or use; and

- select the integrity value for information and related processes or sensors based on the likely injury in the case of unauthorized modification.

1.3 Step Three

Where the injuries to people (either physical or psychological) and the financial impact arising from a single compromise to one asset differ, record the highest value in the Asset Valuation Table/Statement of Sensitivity (Appendix B-5):

- For example, if unauthorized disclosure of one record might reasonably be expected to cause no physical injury, serious embarrassment to some and a financial loss in excess of $10 million, indicating Very Low, Medium and High injury levels respectively, this asset should be assigned the highest of the three levels, namely High (Protected C or perhaps Secret), for its confidentiality value.
- Conversely, when the injuries arising from different compromises to the same asset are not the same, in other words when confidentiality, availability or integrity values differ, record each value separately in the Asset Valuation Table/Statement of Sensitivity.
- For example, if unauthorized disclosure of a medical record might cause minor embarrassment to an individual (a Low injury), but unauthorized loss or destruction might delay treatment of a serious ailment with potential loss of life (a High injury) and unauthorized modification of the data might lead to mistreatment with life threatening consequences (also a High injury level), this asset should be assigned a Low confidentiality value and High for both availability and integrity.

1.4 Step Four

Asset values that fall close to the threshold between two levels should be flagged for subsequent analysis during the Risk Assessment Phase of the TRA project, using arrows (↑↓) to indicate whether they fall near the high or low boundary of the range. For example, if the anticipated financial impact of a compromise were estimated to be $9.8 million, a Medium value falling close to the High range, the entry should be marked accordingly.

2 Examples

2.1 Personal Record(s)

Both the nature of the information in each record and the matter of aggregation are important factors to consider when assessing the confidentiality, availability and integrity values of personal data.

- **Confidentiality.** Unauthorized disclosure of a single leave form may cause virtually no injury, but accidental or deliberate exposure of a police informant's identity might be life threatening. Thus, one should be assigned a Very Low (Unclassified) confidentiality value, while the latter would qualify for High (Protected C). If the entire witness protection program were leaked, the consequences might be widespread loss of life, thereby warranting a Very High (Top Secret) confidentiality value. That being said, most

personnel files in government institutions warrant a Protected B categorization reflecting a Medium confidentiality value.

- **Availability.** Unauthorized destruction of a single leave record might, in the worst case scenario, cause a financial loss in excess of $1,000 but certainly less than $100 thousand, if an individual's pay record were adjusted to reflect a month long vacation. If all of the leave records for a major department were destroyed, however, this injury might be increased by a factor of 10,000 or more, with potential financial losses in excess of $10 million. Therefore, a single record should be assigned a Low availability value, but the entire leave data base would likely warrant a High availability value.
- **Integrity.** The same logic could be applied to the integrity values assigned to a single leave record and the entire data base, because unauthorized modification or corruption of the data could lead to similar financial losses.

2.2 Medical Team

By definition, a small group of doctors would have a High intrinsic availability value. Depending upon the functions they performed, their operational availability value might vary considerably. For example, if they were just a few of many general practitioners in a large metropolitan clinic, their absence might simply cause some inconvenience and rescheduling of routine patient examinations, a Very Low or Low injury based on the number of patients affected, few or many. At the other extreme, however, the medical team might be assigned a Very High operational availability value if they were the only ones capable of containing a major pandemic and thereby preventing widespread loss of life. Although the medical team would undoubtedly have access to sensitive information and other assets, they would not normally be assigned confidentiality or integrity values.

This page intentionally left blank.

Appendix B-5 - Asset Valuation Table / Statement of Sensitivity

Class	Category	Group	Subgroup	Component or Individual	Asset Values				
					C	A[1]		I	$
						i	o		
People									
Tangible	Information								
	Hardware								
	Software								
	Processes								
	Facilities								
Services									
Intangible									

Legend

C – Confidentiality Value. A – Availability Value.

i – Intrinsic Availability Value for Personnel. o – Operational Availability Value for Personnel.

I – Integrity Value. $ - Replacement Cost.

[1] The availability column is split in two for people to record both intrinsic and operational availability values.

INSTRUCTIONS

Step One. Enter all assets within the scope of the TRA project at the appropriate level of detail (Group, Subgroup and Component or Individual) from the Asset Listing in Appendix B-2.

Step Two. Based upon the maximum injury levels that could reasonably be expected to arise in the event of a compromise to their confidentiality (C), availability (A) and integrity (I), insert the relevant asset values determined in accordance with the Expanded Injury Table in Appendix B-4 ranging from Very Low through Very High (VL through VH). In cases where personal safety is a potential concern, assign both intrinsic (i) and operational (o) availability values for the affected personnel.

Step Three. If the assessed value falls near the boundary between two levels, insert arrows to indicate that it lies in the high (↑) or low (↓) end of the range.

Annex C - Threat Assessment Phase

1 Introduction

1.1 General

The third phase of a TRA project, the Threat Assessment, comprises four successive processes and one major output as follows:

- **Threat Identification** – to list all threats that might affect assets within the scope of the assessment at an appropriate level of detail.
- **Likelihood Assessment** – to assess the probability of each threat actually occurring;
- **Gravity Assessment** – to determine the prospective impact of each threat.
- **Threat Assessment** – to assign threat levels ranging from Very Low to Very High for each threat based upon common metrics for likelihood and gravity.
- **Prioritized Threat Listing** – to produce a comprehensive list of threats which may be ranked from the most serious to the least.

1.2 Aim

The aim of this annex is to describe the four processes and single output of the Threat Assessment Phase of a TRA project.

2 Threat Identification

2.1 Threat Definition

The GSP defines threat as "any potential event or act, deliberate or accidental, that could cause injury to employees or assets."[1] Although this is quite correct, the definition might be extended in two directions. Firstly, another broad category of threats, namely natural hazards, must be considered in every threat assessment because they can have very serious consequences, especially with respect to availability. Secondly, any injury to employees or assets is likely to affect service delivery, so the definition of threat should be expanded to accommodate this eventuality.

Threat (*menace*) - any potential event or act, deliberate, accidental or natural hazard, that could cause injury to employees or assets, and thereby affect service delivery adversely.

Expanded GSP Definition

[1] Appendix B to the GSP, Glossary.

2.2 Threat Classes

2.2.1 General

As indicated in the expanded GSP definition, threats may be categorized according to the root cause, either by human beings or through forces of nature. The former may be further subdivided into deliberate threats which are planned events and accidents which are unplanned. Each of the three broad classes of threat has varied characteristics to be considered during the Threat Assessment Phase of a TRA project.

2.2.2 Deliberate Threats

By definition, all deliberate threats involve human beings and a measure of planning or premeditation. Admittedly, some spontaneous acts are committed on the spur of the moment, with little consideration for the consequences. Nevertheless, even these opportunistic threats involve a conscious decision to take some action. Since deliberate threats are often conducted covertly, they may be more difficult to identify, assess and predict than accidents and natural hazards. Furthermore, the selection of suitable countermeasures to mitigate the associated vulnerabilities can be much more complicated because an intelligent adversary will frequently analyze the situation and take steps to circumvent visible safeguards while employing subterfuge to avoid detection. Deliberate threats may cause all types of compromise (unauthorized disclosure, destruction, removal, modification, interruption or use of assets) to confidentiality, availability and integrity. Potential impacts vary considerably, from almost innocuous pilferage of office supplies to the massive damage of a major terrorist attack.

2.2.3 Accidental Threats

All accidents arise from human error in one form or another. Untrained or ill-informed employees and other personnel can make many different mistakes ranging from inadvertent data corruption or disclosure through operating errors to design flaws leading to mechanical and even structural failure. As with deliberate threats, the possible consequences of accidents include every form of compromise, with potential impacts on confidentiality, availability and integrity. Accidents, such as a spilled cup of coffee or a mistyped letter, are frequently inconsequential, but the adverse effects of some threat events, like a major toxic spill or pilot error in a large commercial airliner, can be truly catastrophic.

2.2.4 Natural Hazards

While natural hazards are just as varied as accidents and deliberate threats, their consequences are generally more focused. In essence, forces of nature rarely cause unauthorized disclosure or modification, compromises to confidentiality and integrity respectively. Of course, there are some limited exceptions, where a tornado might destroy a building and deposit sensitive papers across the countryside, or a lightning strike might set off a power spike that could corrupt electronic data files. Nevertheless, the more common outcomes of natural hazards are various compromises to availability, such as injuries to people, the destruction of other assets and the interruption of services. Potentially damaging natural phenomena arise on a regular basis, but serious disasters occur much less frequently.

2.2.5 Threat Model

Figure C-1 illustrates the relationships amongst the three broad classes of threat in a general threat model.

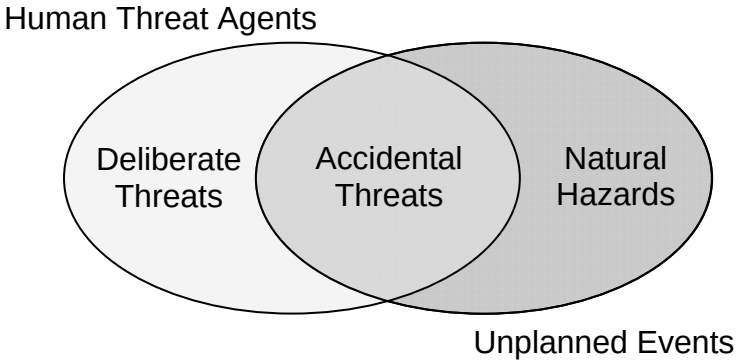

Figure C-1: General Threat Model

2.3 Sources of Threat Data

Many risk analysts view the Threat Assessment as the most challenging phase of a TRA project due to a perceived scarcity of relevant data or current intelligence. Nothing could be further from the truth, however, for there is, in fact, a wealth of information readily available from a variety of reputable sources. While program managers and employees may be aware of some immediate issues, especially with respect to certain accidental threats and some insider concerns, departmental security authorities, facility managers and systems administrators are more likely to have a broader view of current threat levels. Incident reports, intelligence assessments and internal audits are frequently useful sources of threat information. The news media, especially local and national newspapers can provide valuable input, while an array of professional journals and related Web sites can be equally useful. These and other sources are listed in Appendix C-1.

2.4 Data Collection Techniques

Although threat data are readily available, there is no single repository for all of this material. Thus, the real dilemma for security practitioners lies with the collection, collation and analysis of widely dispersed references in a timely manner to meet the needs of each TRA project. Without an ongoing program to maintain a current inventory of threats in a centralized location, all too many risk analysts start from zero with each assessment, thereby prolonging the effort, increasing the cost and risking dangerous oversights if significant threats are overlooked.

To avoid these pitfalls, departments may wish to consider two different options for the collection, collation and analysis of threat data. For smaller agencies that conduct relatively infrequent TRA projects, it is probably more cost-effective to engage a suitably qualified consultant to compile the requisite threat assessments. For larger organizations, however, with regularly recurring requirements, it may be more efficient to establish a dedicated cell of threat analysts to develop and maintain a current threat data base in support of all TRA projects.

2.5 Threat Listing

2.5.1 Structure

The Threat Listing in Appendix C-2 is presented as a hierarchical table with a structure much like the Asset Listing in Appendix B-2. From the three broad threat classes defined in section 2.2 at the highest level, the list branches out to encompass more detailed threat activities, threat agent categories, threat agents, threat events and, if warranted, precise threat scenarios for increasingly granular analysis. Each subordinate level is defined below, and the actual structure is illustrated in Figure C-2.

- **Threat Activity.** A generic group of threats with common consequences or outcomes intended to facilitate data collection by responsible government departments or agencies.
- **Threat Agent Category.** A subdivision of threat activity, intended to focus on deliberate threats with common motivation or accidental threats and natural hazards with similar causal factors.
- **Threat Agent.** An identifiable organization, individual or type of individual posing deliberate threats, or a specific kind of accident or natural hazard.
- **Threat Event.** An actual incident in which a threat agent exploits a vulnerability with potentially adverse effects on an asset of value.
- **Threat Scenario.** A detailed chronological and functional description of an actual or hypothetical threat event intended to facilitate risk analysis generally and the identification of appropriate safeguards in particular.

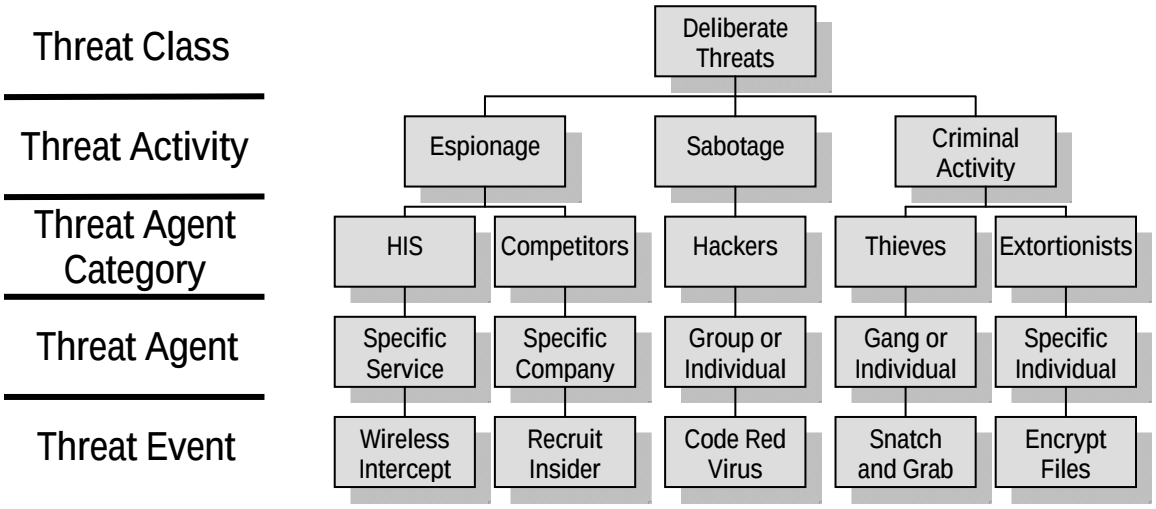

Figure C-2: Sample Segment of the Threat Listing Hierarchical Structure[2]

[2] The abbreviation HIS stands for Hostile Intelligence Service.

2.5.2 Benefits

Like the Asset Listing, the hierarchically structured Threat Listing offers several important advantages when conducting a TRA project:

- **Consistency.** The use of common data structures and definitions for threat identification facilitates communications within and between TRA projects to achieve consistent results that can be replicated by different practitioners assessing the same or similar threats. It also promotes interoperability and the sharing of threat data between organizations.
- **Completeness.** Important threats are less likely to be overlooked with the use of a comprehensive list to guide TRA teams.
- **Flexibility and Scalability.** Most importantly, the hierarchical structure of the Threat Listing permits analysis at different levels of detail, consistent with the scope of the assessment and the actual risk environment. In essence, less serious threats affecting less valuable assets might be rolled up and evaluated at a higher level, while those causing greater risks might be examined down to the threat agent or threat event level for greater precision. Similarly, entire branches of the tree-like structure might be ignored entirely if any particular threat activity or threat agent category falls outside the scope of the assessment. Thus, TRA teams may constrain their efforts to concentrate on what is really important.
- **Currency.** The Threat Listing is easily updated as new threats are identified. Furthermore, given the logical groupings of similar threats, it is much simpler to categorize new or emerging problems.

2.5.3 Caveat

Again, as with the Asset Listing, the Threat Listing must be used with caution. It is not and cannot be complete because new threats, especially at the event level of analysis, are encountered on a regular basis due, in part, to rapidly changing technologies and threat agent capabilities. **Therefore, Appendix C-2 should be employed as an aide-mémoire and guide to help organize and structure the collection and collation of relevant threat data, rather than a checklist to be followed without question.**

2.6 Threat Activities

2.6.1 General

The three broad classes of threat, deliberate, accidental and natural hazards, comprise many different threat activities that can compromise assets, both tangible and intangible, injure employees and disrupt service delivery.

2.6.2 Deliberate Threat Activities

Threat Activities within the Deliberate Threat Class include:

- **War**. Both international and civil wars or revolutions can be extremely destructive, with the potential to compromise almost every conceivable asset in every possible way. The very magnitude of war as a threat activity can complicate any associated

threat assessments considerably. Therefore, the *Harmonized TRA Methodology* tends to concentrate on peacetime threats and risks, even though the analytical processes are no less applicable to a wartime environment.

- **Espionage.** The collection of information by covert or clandestine means is not confined to hostile intelligence services. In the economic arena, for example, some competitors conduct industrial espionage to gain competitive advantage. Many hackers, both individuals and organized groups, pose similar problems as they seek unauthorized access to computers and data files, sometimes out of sheer curiosity, but more frequently with criminal and malicious intent. Other attempts to gather information, even surreptitiously, may be completely legal. These would include investigative journalism and competitive intelligence, an entirely ethical pursuit involving the collection and analysis of open source data to gain business insights and competitive advantage. In each case, unauthorized disclosure, a confidentiality concern, is the primary consequence of espionage and related information gathering activities, but there may be an availability dimension as well when sensitive material is stolen for subsequent examination and, on occasion, reverse engineering.
- **Sabotage**. The *Criminal Code of Canada* provides an explicit definition of sabotage as ". . . an act or omission that (a) impairs the efficiency or impedes the working of any vessel, vehicle, aircraft, machinery, apparatus or other thing; or (b) causes property, by whomever it may be owned, to be lost, damaged or destroyed",[3] if it is conducted for a purpose prejudicial to the safety, security or defence of Canada or any allied forces in Canada. While this is an apt definition in a national context, other interests and organizations may be targets for similar attacks. For instance, disgruntled employees, individual activists, radical groups and even commercial competitors have damaged material and disrupted services for personal profit or misplaced ideals. In each case, the primary consequences are the destruction of tangible assets, with an associated interruption of service, two availability impacts.
- **Subversion**. Subversion differs from other threat activities in that it generally targets intangible assets, such as public confidence and employee morale. At the high end of the spectrum, the *Canadian Security Intelligence Service (CSIS) Act*, defines subversion to comprise both state sponsored or "foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person" and domestic "activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of the constitutionally established system of government in Canada".[4] Of course, the act also contains explicit provisions to protect lawful advocacy, protest and dissent. Nevertheless, even entirely legal behaviour, such as lawful picketing and pamphleteering, may warrant analysis within a TRA project to help mitigate the impact on productivity, public opinion and employee expectations.
- **Terrorism**. Like subversion, terrorism is defined in the *CSIS Act* to comprise "activities within or related to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of

[3] *Criminal Code*. R.S., 1985, c. c-46, s.52(2).
[4] *Canadian Security Intelligence Service Act*. 1984, c. 21, s. 2.

achieving a political objective within Canada or a foreign state".[5] Quite clearly, the consequences of both domestic and international terrorism can include injuries to people, the destruction of valuable assets and the interruption of important services, with potentially serious availability impacts.

- **Criminal Acts**. The *Criminal Code of Canada* and related statutes, such as the *Narcotic Control Act*, establish a statutory basis for law enforcement while defining an array of illegal activities that constitute threats to public order, the administration of law and justice, public morals, private citizens, public officials, property, currency, contracts and trade amongst other tangible and intangible assets of value. Given the variety of offences, the potential consequences of criminal acts include every possible type of compromise, with impacts on confidentiality, integrity and availability, as well as replacement cost. Admittedly, the distinction between criminal acts and other deliberate threat activities noted above is somewhat artificial because the others almost invariably involve one or more criminal offences. For example, some acts of espionage may qualify as treason [s. 46(2)] and some entail the interception of private communications [s. 184(1)] or unauthorized use of a computer [s. 342(1)]; as previously noted, sabotage [s. 52(2)] is already a criminal offence; subversive activities may include sedition [s. 59(1)], unlawful assembly [s. 63(1)], spreading false news [s. 181], mischief [s. 430(1)] or, in extreme cases, riot [s. 64]; and, finally, all terrorist attacks also involve criminal offences, such as murder [s. 229], using explosives [s. 81(1)] or kidnapping [s. 279(1)]. Thus, the deliberate threat activities listed in Appendix C-2 are not always mutually exclusive. Rather than collapse or combine the list, however, it remains useful to distinguish between the seven different groupings to facilitate data collection, collation and analysis, especially where different agencies have primary responsibilities for investigating certain activities.
- **Other Deliberate Threat Activities**. As indicated above, most deliberate threats involve some degree of criminal activity, but there are some notable exceptions. For example, excessive absenteeism, personal web surfing, unsolicited e-mail (spam) and legal strikes can have serious consequences, but they are lawful pursuits in Canada, despite their adverse impact on the availability of employees, assets and services.

2.6.3 Accidental Threat Activities

All accidents arise from human error at some level of detail, either directly or indirectly. Causal factors include undue haste, inattention to instructions or standard operating procedures, inadequate training, poor workmanship, poor housekeeping, inaccurate calculations, cost-cutting measures and overwork or fatigue. The consequences of accidents can include all forms of compromise to confidentiality, availability and integrity. While the impact of some accidental threat events, such as spelling mistakes in a report or misplaced office supplies, may be innocuous, the effects of others, like the power failure of August 2003 or the core meltdown at Chernobyl, can be extremely serious. The varied threat activities within the Accidental Threat Class include:

- **Office Accidents.** A variety of miscues which generally affect confidentiality (misdirected correspondence or incorrect data categorization) or availability (hastily

[5] *Ibid.*

deleted data files or a dropped notebook computer) often with only minor consequences but occasionally more serious results, such a personal injury or death.

- **Data Corruption.** An integrity concern arising from data entry errors and other mistakes during the collection, processing and dissemination of information.
- **Lost Assets.** An availability concern when tangible assets, such as office equipment or negotiable instruments, are inadvertently misplaced and cannot be employed for their intended purpose.
- **Mechanical Failures.** Design flaws, improper maintenance and operator error can contribute to equipment failure, normally an availability issue, with a range of consequences from negligible (a broken pencil) to catastrophic (a major train derailment).
- **Software Errors.** Coding errors, imperfect software integration and other installation errors can compromise both confidentiality and integrity, but the more common impacts are availability problems when the affected systems malfunction.
- **Hardware Flaws.** Like mechanical equipment, hardware can fail due to design defects, improper maintenance and operator error, with a range of consequences from almost insignificant (a burned out monitor) to extremely serious (multiple chip failures in the avionics package aboard a jumbo jetliner). Although most incidents affect availability, some have had integrity implications (faulty math co-processors).
- **Structural Failures.** Relatively rare but potentially serious events arising from engineering miscalculations, construction errors or maintenance problems, leading to partial or complete collapse of buildings and other structures, often compounded by concurrent natural hazards, such as freezing rain or heavy snowfall.
- **Fires.** An availability problem with potentially serious consequences for employees, tangible assets and, therefore, service delivery, usually arising from carelessness, poor housekeeping, improper maintenance or operator error.
- **Traffic Accidents.** Generally caused by driver error, often aggravated by adverse weather or road conditions, but occasionally arising from design flaws or improper maintenance, with potentially serious consequences for the availability of vehicles, their occupants and other assets nearby.
- **Industrial Accidents.** A broad grouping of availability concerns, usually attributed to operator error and, less frequently, equipment failure, with impacts ranging from inconsequential (short delays) to extremely grave (major toxic spills) affecting employees and other people, tangible assets and, therefore, service delivery.
- **Nuclear Accidents.** Relatively rare events with potentially serious availability consequences for people and tangible assets in contaminated areas, as well as the services they provide and, therefore, intangible assets, such as public confidence.

2.6.4 Natural Hazard Threat Activities

Many different forces of nature can generate a wide variety of threat events with varied availability impacts. Threat Activities within the Natural Hazard Threat Class include:

- **Disease.** Illnesses affecting people or the plants and animals upon which they depend, generally caused by micro-organisms or genetic defects, with impacts ranging from mild discomfort (minor cold) to catastrophic (worldwide flu pandemic).

- **Earth Movement.** Some, such as erosion and land subsidence, tend to undermine structures fairly slowly over a long period of time, while others, such as landslides, volcanoes and earthquakes can cause both localized and occasionally widespread damage very suddenly, with little forewarning.
- **Flooding.** Seasonal rainfall, spring runoff, severe storms, high tides and, far less frequently, tsunamis can cause water levels to rise, sometimes very quickly, to injure people, damage tangible assets and disrupt services, some times for prolonged periods across a wide area.
- **Environmental.** Both people and tangible assets can be susceptible to injury from a variety of environmental factors, such as airborne particles (both dust and pollen), extreme temperatures (both heat and cold) and ambient radiation (radon), while others, such as humidity, geomagnetic storms and static electricity generally affect material assets more severely.
- **Severe Storms.** Injuries to people, damage to tangible assets and the disruption of services caused by high winds may be tightly concentrated (tornadoes) or broadly dispersed across large areas (hurricanes and typhoons), while other side effects of severe storms, such as lightning strikes, heavy rainfall, freezing rain, heavy snowfall and hailstones, can also cause serious damage.
- **Plants and Animals.** Noxious weeds can displace indigenous varieties with long-term ecological effects, while poisonous or toxic plants can cause more immediate harm to people and other living creatures. On occasion, human beings are attacked directly by various animals, including bears, sharks and various poisonous insects or reptiles, but other threat events involve collisions (deer, moose and bird strikes), insect infestations (ants, cockroaches and termites), some of which may include serious disease vectors (deer ticks transmitting Lyme disease), and even power outages arising from gnawed insulation and the resulting short circuits.

2.7 Direct and Indirect Threats

2.7.1 Definitions

The interaction of threats with assets of value can range from very simple events to extremely complex scenarios. **Direct threats**, where a single threat agent exploits a vulnerability to compromise an asset, are generally straightforward and easy to analyze. With **indirect threats**, however, the train of events may be much more complicated, with one or more threat agents working together or independently to exploit successive vulnerabilities and ultimately compromise some asset. Figure C-3 illustrates both direct and a simple indirect threat.

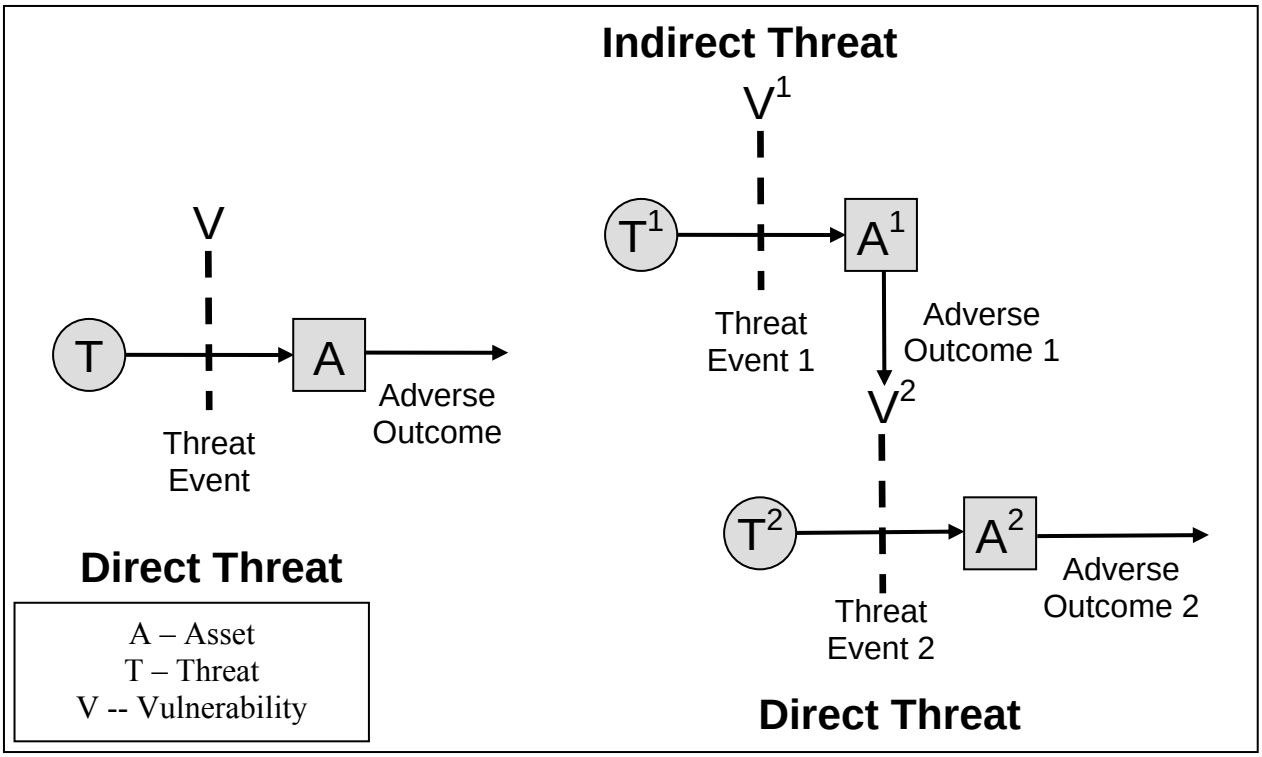

Figure C-3: Direct and Indirect Threats

2.7.2 Practical Implications

While it is possible to construct very convoluted attack scenarios during the Threat Assessment Phase of a TRA project, the effort is rarely warranted for two important reasons. Firstly, each step in an elaborate chain of events has a finite probability of failure and these are cumulative, so the final likelihood of success diminishes very quickly with each intermediate element of a complex threat. Secondly, safeguards selected during the Recommendation Phase of a TRA project to mitigate direct threats and the simpler indirect threats will often counter the more complicated threats as well. Therefore, TRA analysts should concentrate on direct threats and the more obvious indirect threats rather than waste time on highly imaginative speculations during a formal assessment.

2.8 Threat Metrics

2.8.1 GSP Requirements

At the highest level of abstraction, section 10.7 of the GSP requires government departments to determine what threats might affects employees and assets, and assess the **likelihood** and **impact** of their occurrence.

2.8.2 Harmonized TRA Metrics

These two dimensions of any threat provide the basis for objective measurement to permit comparative analysis. In effect, highly probable or likely threat events contribute more to risk than other more remote possibilities. In a similar vein, as the magnitude or gravity of a threat event increases, the impact or extent of the ensuing compromise should be greater. The

Harmonized TRA Methodology builds upon these concepts to establish ordinal metrics for objective threat assessments.

3 Likelihood Assessment

3.1 General

On occasion, current intelligence may predict some deliberate threats, and various sensors might provide forewarning of certain accidents or natural hazards. Unfortunately, indicators like these may not be available and they are not always reliable. Furthermore, the projections are often confined to the short term, leaving little opportunity for long-range risk assessments and the selection of appropriate safeguards. Given these limitations, some other measures are normally required to assess the likelihood of any threats that fall within the scope of a TRA project.

3.2 Frequency

Intuitively, recent experience probably provides the best indicator of future trends. In essence, threat events which have occurred more frequently in the past are more likely to arise in the future, unless some other factor comes into play to change the underlying patterns. For example, where theft has been a persistent problem over the last six months or more, it is likely to remain a serious concern in the foreseeable future. Other threats, such as catastrophic earthquakes, are extremely rare in most locations, and likely to remain so. Thus, for analytical purposes, the likelihood of relevant threat activities or events, namely those in the immediate locale which affect asset subgroups within the scope of the assessment, should be derived from sources listed in Appendix C-1, and assigned one of four levels in Table C-1, based on past frequency ranging from daily occurrence to more than 10,000 days, about 30 years or more, between threat events.

3.3 Other Considerations

3.3.1 Threat Agent Intentions

The likelihood of deliberate threats can be more volatile than that of accidents and natural hazards because the intentions of threat agents can change with little forewarning. For example, terrorist groups who have confined their attacks to one region in the past have on occasion shifted their attention to other targets elsewhere in the world. Thus, it is insufficient to base the likelihood of deliberate threat events solely on past experience with similar asset subgroups in the immediate vicinity of the TRA project. Threat events in other locations and those affecting other asset subgroups can also provide important indicators.

3.3.2 Location

Quite clearly, the likelihood of many deliberate threats can vary from one location to another. For example, armed robberies often occur more frequently in large metropolitan areas than small rural centres. Almost inevitably, there are some exceptions where threat levels remain relatively constant from one site to another. For instance, threats to IT assets connected to the Internet are generally consistent for similar targets whatever their location because the systems are all potentially accessible from anywhere in the world. In most cases, however, threat events that

have happened in the immediate vicinity are more likely to cause future harm than others experienced elsewhere at some distance. That being said, if a deliberate threat has materialized at another location, there is some possibility that it could affect assets within the scope of the assessment at a future date because threat agent intentions may change. To reflect this reality, the likelihood of a remote threat should be adjusted downward as indicated in the third column of Table C-1 to represent a more realistic probability at the TRA site.

3.3.3 Assets Affected

In a similar vein, deliberate threats directed towards asset subgroups within the scope of a TRA project are more serious concerns than similar activities aimed at different assets outside the scope of the assessment, even at the same location. Nevertheless, threat events affecting other assets in the same category should not be ignored because, once more, threat agent intentions and, therefore, targets may change. For example, jewellery theft, whatever the likelihood in a given area, might not be considered relevant in a TRA project for a clothing store. It would be prudent, however, to include theft in the Threat Assessment and assign a lower probability from column 3 in Table C-1 to reflect current intentions.

3.3.4 Location and Assets Affected

Finally, a deliberate threat that has occurred at some distance and affected asset subgroups outside the scope of the assessment may still pose a credible risk and warrant an entry in the Threat Assessment, albeit with a much reduced likelihood selected from column 4 of Table C-1.

3.4 Threat Likelihood Table

For each threat event or activity, depending upon the granularity of analysis, determine the frequency of past events affecting assets within the scope of the assessment at the same location based upon actuarial data and other sources listed in Appendix C-1. Select the appropriate range in column 1 to determine the likelihood level, from Very Low to High, in column 2. Where deliberate threats have occurred elsewhere or affected assets outside the scope of the assessment, choose the appropriate level from column 3. Finally, for deliberate threats involving different assets at remote sites, use the likelihood levels in column 4.

Past Frequency	**Same Location Similar Assets**	Remote Location but Similar Assets OR Same Location but Different Assets	**Remote Location Other Assets**
Daily	High	High	High
1-10 Days	High	High	Medium
10-100 Days	High	Medium	Low
100-1,000 Days	Medium	Low	Very Low
1,000-10,000 Days	Low	Very Low	Very Low
Over 10,000 Days	Very Low	Very Low	Very Low

Table C-1: Threat Likelihood Table

4 Gravity Assessment

4.1 General

The impact or gravity of a threat event is a measure of the amount of damage or the extent of compromise that is likely to arise should it actually occur. When considering deliberate threats, the capabilities of threat agents, in terms of knowledge, skills and resources, are sound indicators of the expected outcome. For example, organized gangs are more likely to cause greater harm than a single, inexperienced thief. With accidents and natural hazards, the anticipated injuries are normally directly proportional to the magnitude of the event. In other words, an earthquake of 8.0 on the Richter scale is more serious than one that measures only 5.0 or less. In each case, however, the real objective is to estimate the likely effects of a threat event upon any assets within the scope of the assessment.

4.2 Deliberate Threats

In general, the capabilities of deliberate threat agents may be assessed in terms of their skills, knowledge and resources relevant to specific threat events or threat scenarios.

- **Skills.** A measure of the threat agent's aptitude to exploit certain vulnerabilities to compromise assets within the scope of the assessment, also known as tradecraft in certain circles. Skill levels may range from absolute mastery of a given technique, through moderate ability to complete ineptitude. For example, elite hackers typically demonstrate very high skill levels while young neophytes tend to fall at the lower end of the spectrum, so the former are more likely to cause more serious damage than the latter if they choose to attack any given target.
- **Knowledge.** A measure of the threat agent's awareness of an asset of potential interest, its value and associated vulnerabilities. Although knowledge differs somewhat from skill, the two are generally combined to provide an essentially qualitative dimension of deliberate threat agent capability.
- **Resources.** The complementary quantitative measure of threat agent capabilities includes an assessment of the financial and human resources available to an attacker, and any other tools, such as computing power and other advanced technologies, relevant to the associated threat events.

4.3 Accidents and Natural Hazards

In general, the amount of damage arising from an accident or natural hazard is directly proportional to the magnitude or size of the threat event.

- **Severe Impact.** The threat event could reasonably be expected to cause a major compromise involving unauthorized disclosure, destruction, removal, modification or use of 25% or more of an asset subgroup, or a prolonged interruption of services of more than five working days.

- **Moderate Impact.** The threat event could reasonably be expected to cause a serious compromise affecting up to 25% of an asset subgroup, or interrupting services for as much as five working days.
- **Limited Impact.** The threat event could reasonably be expected to cause a minor compromise in which less than 5% of an asset subgroup is affected, or services are interrupted for less than three hours.

4.4 Threat Gravity Table

The capabilities of deliberate threat agents and the magnitude of accidents and natural hazards are mapped to their potential impacts or seriousness in Table C-2, the Threat Gravity Table, for each threat affecting assets within the scope of the assessment.

Deliberate Threat Agent Capabilities	Magnitude of Accidents or Natural Hazards	**Threat Impact or Gravity**
Extensive Knowledge/Skill Extensive Resources	Highly Destructive Extremely Grave Error Widespread Misuse	High
Limited Knowledge/Skill Extensive Resources **or** Extensive Knowledge/Skill Limited Resources **or** Moderate Knowledge/Skill Moderate Resources	Moderately Destructive Serious Error Significant Misuse	Medium
Limited Knowledge/Skill Limited Resources	Modestly Destructive Minor Error Limited Misuse	Low

Table C-2: Threat Gravity Table

5 Threat Assessment

5.1 Threat Levels

Once the threat likelihood has been determined using Table C-1 and the gravity specified in accordance with Table C-2, these values are inserted in Table C-3 to determine the overall rating for each threat affecting assets within the scope of the assessment, from Very Low to Very High.

Threat Impact	Threat Likelihood			
	Very Low	**Low**	**Medium**	**High**
High	Low	Medium	High	Very High
Medium	Very Low	Low	Medium	High
Low	Very Low	Very Low	Low	Medium

Table C-3: Threat Levels Table

5.2 Practical Application

5.2.1 General

As explained above, all threats affecting assets within the scope of a TRA project must be assigned one or more ratings based upon the likelihood of occurrence and the potential impact. The Threat Assessment may be complicated, however, by some other important considerations. For example, threat levels may not be constant. Also, a single threat event may have multiple impacts, affecting several different assets or asset values.

5.2.2 Variable Threat Levels

Both the likelihood and the gravity of any given threat may vary over time. For many natural hazards there are seasonal fluctuations where, for instance, flooding may occur more frequently, so the impacts may be more severe in springtime rather than the fall or winter. With accidents, the time of day or day of the week may be important factors, for people are more likely to make mistakes when they are tired or exceptionally busy. The likelihood of some deliberate threats also follows certain cyclical patterns. For example, the incidence of shoplifting and other petty thefts often rises with increases in the cost of drugs at the street level, and minor acts of sabotage or wilful damage are frequently more prevalent during periods of labour unrest and tension in the workplace. Similarly, threat agent capabilities and, therefore, the gravity of deliberate threats may change as threat agents develop new skills or gather more resources. In general, the higher threat levels should be recorded in the Threat Assessment. Where any peaks are isolated and readily predictable, however, both values might be captured and assessed during the next phase of the TRA project to determine the associated variations in overall risk. This may permit the selection and recommendation of more focused and cost-effective safeguards for peak periods during the final phase of the assessment.

5.2.3 Multiple Threat Levels

With respect to deliberate threats, the gravity of a threat event is not necessarily uniform for different threat scenarios concerning the same or different assets because threat agent capabilities may differ for each attack profile. For example, an espionage agency may employ human intelligence (HUMINT) or signals intelligence (SIGINT) techniques amongst others to compromise the confidentiality of sensitive information, but the skills and resources it can bring to bear may vary significantly amongst the different methods. Thus, the Threat Assessment may, of necessity, include two or more different threat levels for a single threat agent targeted against even one asset. At an even lower level of granularity, a single threat agent's ability to exploit one vulnerability may differ widely from its capability against others. Therefore, depending

upon the scope of the assessment, two or more threat levels may be assigned for a single threat event based upon different scenarios exploiting different vulnerabilities in an attempt to compromise a single asset. Normally, this level of complexity should be avoided except in the riskiest situations, where both asset values and threats are high.

5.2.4 Multiple Assets Affected

Some threat events are very tightly constrained. For example, a thief may concentrate on a single asset subgroup, like oil paintings, or even a single component, a specific work of art. Conversely, some other threat events may affect many different assets: a single act of arson or an accidental fire might damage property, injure people, destroy materiel and undermine morale or public confidence. Nevertheless, a single threat level will suffice in the Threat Assessment, unless the gravity of the threat event varies for different assets. That being said, the single threat level will be used repeatedly when the risks to each asset are computed later, and the three variables (asset value, threat and vulnerability) are combined in the Risk Assessment Phase of the TRA project.

5.2.5 Multiple Threat Impacts

Most threat events compromise only one asset value, confidentiality, availability or integrity. In some cases, however, a second value and, even more rarely, a third might be affected by a single threat event. For example, a lightning strike causing a power surge is most likely to damage delicate equipment or disrupt power distribution, both availability problems. On occasion, a power spike might corrupt data either during transmission or on magnetic media, an integrity issue. It is perhaps even conceivable that the same incident might misdirect a sensitive signal to the wrong address, a confidentiality concern. In effect, one threat event could have multiple impacts, each of which should be assigned the appropriate threat level, all of which may be different, based on the likelihood of occurrence and the gravity of the different outcomes.

5.2.6 Level of Granularity

The hierarchical Threat Listing permits data to be captured and analyzed at different levels of granularity commensurate with the scope of the assessment. As a general rule of thumb, however, data is more likely to be collected regarding threat agents and specific threat events. To determine the gravity of deliberate threats in particular, threat agent capabilities may be assessed against specific vulnerabilities in even more detailed threat scenarios but, wherever possible, threat levels should be rolled up to a higher column in the Threat Listing, preferably the threat agent category or even threat activity to reduce the number of variables in the subsequent Risk Assessment Phase of the TRA project. Of course, this is only feasible if the relative threat levels of different threat events within the category or activity are relatively consistent. To simplify matters when there are wide variations between the highest and lowest threat levels in one particular category, data may still be consolidated as much as possible by grouping threat events with similar threat levels.

5.3 Summary

The determination of threat levels based upon the likelihood and gravity of threat events and activities using common metrics to permit comparative analysis is fundamental to the *Harmonized TRA Methodology*. The last three steps in the Threat Assessment are amplified with more detailed instructions and examples in Appendix C-3.

6 Prioritized Threat Assessment Table

As indicated above, all threats affecting assets within the scope of an assessment must be assigned one or more threat levels based upon their likelihood of occurrence and potential impact. A single threat event might injure one or more assets to compromise confidentiality, availability and/or integrity, so threat levels should be determined for each different outcome. Each of these threat levels should be entered in the Threat Assessment Table, the final output of the Threat Assessment Phase of a TRA project. Simply sorting by threat levels from Very High to Very Low can quickly prioritize threats, identifying those of greatest concern.

This list is illustrated in Table C-4 and amplified in Appendix C-4.

Threat Class	Threat Activity	Threat Agent Category	Threat Agent	Threat Event	Threat Levels Affecting			Asset Subgroup(s) Affected
					C	A	I	
Legend C – Confidentiality. A – Availability. I – Integrity.								

Table C-4: Sample Threat Assessment Table

This page intentionally left blank.

Appendix C-1 - Sources of Threat Data

Departmental Resources	
Data Source	**Types of Threats**
Program Managers	• Service Disruptions • (Some) Insider Threats • Employee Errors
Material/Asset Managers	• Material Losses to the Crown o Theft of Material o Accidental Loss/Destruction o Accounting Errors
Facility Managers	• Local Security Incidents • Heating/Ventilation/Air Conditioning Failures • Power Outages • Floods/Other Environmental Hazards
Human Resources	• Violence in the Workplace • Labour Unrest • Disciplinary Problems
Finance	• All Losses to the Crown • Accounting Errors
Chief Information Officer	• System Integration Failures
Systems (Security) Administrator	• Intrusion Detection System Reports • Security Audit Logs • Malicious Code Incidents • Hardware Failures • Software Flaws
Departmental Security Officer	• Security Incidents/Investigations • Lead Agency Security Intelligence Reports
IT Security Coordinator	• IT Security Incidents/Investigations
BCP Coordinator	• Major Incidents/Emergencies
Internal Audit/Review	• Internal Mismanagement • Forensic Audit Reports
Legal Council	• Lawsuits against the Crown
Occupational Health and Safety	• Accidents • Health Hazards

External Resources: Security Lead Departments	
Data Source	**Types of Threats**
Canadian Security Intelligence Service http://www.csis-scrs.gc.ca/en/index.asp	• Unclassified Commentaries/Perspectives • Classified Threat Assessments o Espionage o Sabotage o Foreign Influenced Covert Activities o Terrorism
Communications Security Establishment http://www.cse-cst.gc.ca/index-e.html	• COMSEC Incidents • IT Security Alerts/Bulletins • Foreign Intelligence (SIGINT)
Foreign Affairs and International Trade Canada http://www.voyage.gc.ca/main/before/faq/tip-en.asp#tu	• Travel Information Program o Country Updates o Travel Warnings o Threats Abroad
Public Safety and Emergency Preparedness Canada http://www.psepc-sppcc.gc.ca/index-en.asp	• Canadian Cyber Incident Response Centre • PSEPC Daily Briefs o Accidents/Natural Hazards o IT Security Incidents
Public Works and Government Services Canada Building Custodians	• Local Security Incidents • Heating/Ventilation/Air Conditioning Failures • Power Outages • Floods/Other Environmental Hazards
Royal Canadian Mounted Police http://www.rcmp.ca/crimint/ci_reports_e.htm	• Criminal Intelligence Reports

External Resources: Other Government Agencies	
Data Source	**Types of Threats**
Canadian Centre for Occupational Health and Safety http://www.ccohs.ca/	• Biological Hazards • Diseases/Disorders/Injuries • Health and Safety Report
Environment Canada http://www.ec.gc.ca/data_e.html	• National Climate Data/Information Archive • National Pollutant Release Inventory
Health Canada http://www.hc-sc.gc.ca/index_e.html	• Health and Safety Hazards • Advisories, Warnings and Recalls
Meteorological Service of Canada http://www.msc-smc.ec.gc.ca/contents_e.html	• (Extreme) Weather Conditions

External Resources: Other Public Sector Agencies	
Data Source	**Types of Threats**
Council of Canadian Fire Marshals and Fire Commissioners http://www.ccfmfc.ca/	• Fire Losses in Canada
Local Fire Department	• Accidental Fires/Arson
Local Police	• Criminal Threats
Provincial Governments	• Labour Disruptions
Public Utilities	• Power/Water Disruptions

External Resources: Private Sector	
Data Source	**Types of Threats**
Insurance Industry	• Various Threats
Service Providers	• Service Disruptions
Product Vendors	• Hardware Failures • Software Flaws

External Resources: Professional Journals
American Intelligence Journal http://www.nmia.org/
Canadian Geographic http://www.canadiangeographic.ca
Competitive Intelligence Magazine http://www.scip.org
Journal of Competitive Intelligence and Management http://www.scip.org
Computer Fraud and Security http://www.elsevier.com/wps/find/journaldescription.cws_home/405876/description#description
Contingency Planning and Management (CPM) Magazine http://www.contingencyplanning.com
Counterintelligence News and Developments Newsletter http://www.loyola.edu/dept/politics/hula/cind1.html
Cryptologia Journal http://www.dean.usma.edu/math/pubs/cryptologia
Defense Intelligence Journal http://www.jmicfoundation.org/Foundationpages/DIJ/defenseintelligencejournal.htm
Disaster Recovery Journal http://www.drj.com/drj2/drj2.htm

External Resources: Professional Journals
Global Crime http://www.tandf.co.uk/journals/titles/17440572.asp
Intelligence and National Security http://www.routledgestrategicstudies.com/journals.asp
International Journal of Intelligence & Counterintelligence http://www.tandf.co.uk/journals/tf/08850607.html
Jane's Information Group http://www.janes.com/
Journal of Safety Research. http://www.elsevier.com/wps/find/journaldescription.cws_home/679/description#description
Journal of Strategic Studies http://www.tandf.co.uk/journals/titles/01402390.asp
Security Studies http://www.tandf.co.uk/journals/titles/09636412.asp
Small Wars and Insurgencies http://www.tandf.co.uk/journals/titles/09592318.asp
Studies in Conflict and Terrorism http://www.tandf.co.uk/journals/titles/1057610X.asp
Studies in Intelligence https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/index.html
Terrorism and Political Violence http://www.tandf.co.uk/journals/titles/09546553.asp

Notes:

1. The foregoing list of threat sources is not complete. Other material will be added from time to time. Any suggestions for further references or contacts may be submitted to the offices identified in the Foreword.
2. The inclusion of any professional journal or web site should not be construed as an endorsement. Similarly, the exclusion of other potentially useful sources is not a rejection. The list is merely intended to illustrate the wealth of information that is readily available to security practitioners and risk managers.

Appendix C-2 - Threat Listing

	Class	Activity	Agent Category	Agent	Event
1.	Deliberate	War	Nation States	Nations	Military Invasion
2.					Information Operations
3.			Revolutionaries	Factions	Insurrection
4.			Rebels	Factions	Guerrilla Warfare
5.		Espionage	Hostile Intelligence Service	Services	COMINT
6.					ELINT
7.					FISINT
8.					Emanations Interception
9.					Network Exploitation
10.					HUMINT
11.					IMINT
12.					Open Source Collection
13.					Break and Enter
14.			Other State Sponsored	Organizations	Repeat Serials 8-13.
15.			News Media	Companies	HUMINT
16.					Competitive Intelligence
17.				Individuals	HUMINT
18.					Competitive Intelligence
19.			Industrial Espionage	Companies	HUMINT
20.					Electronic Eavesdropping
21.					Wiretapping
22.					Business Partnerships
23.					Reverse Engineering
24.					Competitive Intelligence
25.					Break and Enter
26.				Individuals	HUMINT
27.					Competitive Intelligence
28.					Break and Enter
29.			Hackers	Groups	Network Exploitation
30.					Social Engineering
31.				Individuals	Network Exploitation
32.					Social Engineering
33.			Organized Crime	Groups	HUMINT
34.					Electronic Eavesdropping
35.					Network Exploitation
36.		Sabotage	State Sponsored	Organizations	Information Operations
37.			Competitor	Organizations	Product Tampering
38.			Disgruntled Employees	Groups/Individuals	Frivolous Grievances
39.					Vandalism
40.					Delete/Destroy Records
41.					Corrupt Data
42.					Encrypt Files
43.					Misconfigure Software
44.					Misconfigure Hardware

	Class	Activity	Agent Category	Agent	Event
45.			Outside Activists	List Groups	Destroy Equipment
46.			Hackers	Wannabees	Denial of Service Attacks
47.					Malicious Code
48.					File Corruption
49.				Script Kiddies	Repeat Serials 46-48.
50.				Fully Capable	Repeat Serials 46-48.
51.				Elite Hackers	Repeat Serials 46-48.
52.		Subversion	State Sponsored	Organizations	Propaganda
53.			Political Activists	Groups	Distribute Pamphlets
54.					Intimidate Employees
55.			Lobbyists	Groups	Pressure Tactics
56.				Individuals	Bribery
57.			Competitors	Organizations	Rumour Mongering
58.					(False) Advertising
59.			Labour Unrest	Groups	Demonstrations
60.			Hackers	Script Kiddies	Web Defacement
61.					Hoaxes
62.				Fully Capable	Repeat Serials 60-61.
63.				Elite Hackers	Repeat Serials 60-61.
64.		Terrorism	International Terrorists	Groups	Assassination
65.					Kidnapping
66.					Bombing
67.					Aircraft Hijacking
68.					Chemical Agents
69.					Nuclear Agents
70.					Fundraising
71.					Recruiting
72.					Training
73.					Money Laundering
74.			Domestic Terrorists	List Groups	Letter Bombing
75.					Fire Bombing
76.					Pipe Bombing
77.		Criminal Acts	Insiders	Employee(s)	Arson
78.					Assault
79.					Copyright Violations
80.					Extortion
81.					Forgery
82.					Fraud
83.					Homicide
84.					Property Damage
85.					Bribery
86.				Temporary Help	Repeat Serials 77-85.
87.				Subcontractors	Repeat Serials 77-85.
88.				Service Staff	Repeat Serials 77-85.
89.				Security Guards	Repeat Serials 77-85.
90.			Outsiders	Clients	Repeat Serials 77-85.
91.				Contractors	Repeat Serials 77-85.
92.				Visitors	Repeat Serials 77-85.
93.				Public	Repeat Serials 77-85.

	Class	Activity	Agent Category	Agent	Event
94.				Hackers	Identity Theft
95.				Young Offenders	Graffiti
96.					Vandalism
97.				Petty Criminals	Theft
98.					Robbery
99.			Organized Crime	Groups	Gambling
100.					Money Laundering
101.					Drug Trafficking
102.					Identity Theft
103.			Competitors	Companies	Patent Infringement
104.					Copyright Violations
105.					Affecting Public Markets
106.		Others	Spammers	Individuals	Spam
107.			Employees	Individuals	Constant Web Surfing
108.					Unauthorized Use
109.					Absenteeism
110.			Organized Labour/Unions	Groups	Work to Rule
111.					Work Slowdowns
112.					Work Stoppages
113.					Block/Delay Access
114.			Demonstrators	Activist Groups	Peaceful Marches
115.					Blocking Roadways
116.					Violent Confrontations
117.					Riots
118.					Building Occupations
119.				Ethnic Groups	Repeat Serials 114-118.
120.				Organized Labour	Repeat Serials 114-118.
121.	Accidents	Office Accidents	Employees	Office Staff	Delete Files
122.					Spill Coffee/Other Liquids
123.					Trip/Personal Injury
124.					Misdirect Mail
125.					Forget Password
126.				Cleaning Staff	Unplug Equipment
127.		Lost Assets	Employees	Individuals	Lose Notebook Computers
128.			Contractors	Organization	Misdirect Shipments
129.		Data Corruption	Employees	Data Entry Clerks	Data Entry Errors
130.				Data Base Admin.	Operating Errors
118.			Clients	Individuals	Inaccurate Data Input
131.		Software Errors	Software Vendors	Companies	Software Bugs
132.			System Integrators	Organizations	Software Integration Errors
133.			Internal Programmers	Individuals	Coding Errors
134.			System Administrators	Individuals	Software Configuration Errors
135.		Hardware Failures	Hardware Vendors	Companies	Design Flaws
136.					Equipment Malfunction
137.			System Integrators	Organizations	Installation Errors
138.			System Administrators	Individuals	Hardware Configuration Errors
139.					Operator Errors/Misuse
140.		Mechanical Failures	Equipment Vendors	Companies	Design Flaws
141.					Equipment Malfunction

	Class	Activity	Agent Category	Agent	Event
142.			Public Utilities	Organizations	Water Outage
143.					Power Failures
144.			Building Custodians	HVAC Maintainers	Loss of Heating
145.					Condensation
146.				Plumbers	Leaks/Water Damage
147.			Equipment Operators	Individuals	Inadvertent Misuse
148.		Structural Failures	Architects	Companies	Design Flaws
149.			Construction Industry	Companies	Substandard Construction
150.			Building Occupants	Organizations	Overstress Floors
151.		Fires	Employees	Smokers	Discarded Cigarettes
152.				Cleaning Staff	Spontaneous Combustion
153.				Electricians	Short Circuit
154.		Industrial Accidents	Transportation Workers	Truck Drivers	Toxic Spill
155.			Manufacturing Teams	Equipment Operators	Personal Injury
156.					Disrupt Production
157.		Traffic Accidents	Employees	Individuals	Private Motor Vehicle Accident
158.				Transport Drivers	Public Motor Vehicle Accident
159.		Nuclear Accidents	Nuclear Power Plant	Operations Staff	Radiation Leak
160.					Core Melt Down
161.			Medical Facilities	Medical Staff	Accidental Overdose
162.	Natural Hazards	Disease	Bacteria	Staphylococcus	Food Poisoning
163.				Other Bacteria	Pandemic
164.					Epidemic
165.					Local Outbreak
166.					Individual Infection
167.			Spirochete	Syphilis	Individual Infection
168.				Other Spirochetes	Repeat Serials 163-166.
169.			Virus	Avian Flu	Repeat Serials 163-166.
170.				Other Viruses	Repeat Serials 163-166.
171.			Fungus Infection	Histoplasmosis	Severe Illness/Death
172.				Other Fungi	Illness/Death
173.			Parasites	Malaria	Illness/Death
174.				Other Parasites	Illness/Death
175.			Cancer	Leukemia	Prolonged Illness/Death
176.				Other Cancers	Illness/Death
177.			Heart Disease	Heart Attack	Disability/Death
178.				Stroke	Disability/Death
179.		Earth Movement	Erosion	Water Erosion	Undermine Building
180.				Wind Erosion	Strip Topsoil
181.			Land Subsidence	Groundwater Loss	Undermine Building
182.					Roadway Sinks
183.					Local Flooding
184.				Carbonate Rock	Repeat Serials 181-183.
185.			Landslides	Rainfall/Seepage	Buildings Collapse
186.					Disrupt Transportation
187.				Water Erosion	Repeat Serials 185-186.
188.			Volcanoes	Lava Flows	Destroy Buildings
189.					Disrupt Movements
190.					Block Water Flows

	Class	Activity	Agent Category	Agent	Event
191.				Volcanic Ash	Bury Buildings
192.					Suffocate People
193.					Contaminate Water Supplies
194.			Earthquakes	Interplate Earthquake	Micro (2.0 Richter Scale)
195.					Minor (2.0-3.9)
196.					Light (4.0-4.9)
197.					Moderate (5.0-5.9)
198.					Strong (6.0-6.9)
199.					Major (7.0-7.9)
200.					Great (8.0-8.9)
201.					Rare Great (9.0-9.9)
202.				Intraplate Earthquake	Repeat Serials 194-201.
203.		Flooding	Lake	Specific Site	Spring Runoff
204.					Ice Dam
205.					Flash Flood
206.			River	Specific Site	Repeat Serials 203-205.
207.			Ocean	Specific Site	High Tide
208.		Environmental	Airborne Particles	Dust	Media Contamination
209.				Pollen	Allergic Reactions
210.			Temperature	Heat Wave	Dehydration/Death
211.				Extreme Cold	Frostbite
212.				Prolonged Cold	Loss of Life
213.			Humidity	High Humidity	Dry Rot/Structural Damage
214.					Spores/Allergic Reactions
215.				Low Humidity	Static Electricity
216.			Magnetism	Geomagnetism	Navigational Interference
217.			Radiation	Radon Gas	Health Hazard
218.			Static Electricity	Static Discharge	File Corruption
219.			Stellar Phenomena	Cosmic Rays	Cell Damage
220.				Meteors	Damage Satellite
221.				Sunlight	Acute Sunburn
222.					Damage Exposed Fabric
223.				Geomagnetic Storms	Disrupt Communications
224.					Power Outage
225.		Severe Storms	High Winds	Hurricanes	Category 1 Saffir-Simpson
226.					Category 2 Saffir-Simpson
227.					Category 3 Saffir-Simpson
228.					Category 4 Saffir-Simpson
229.					Category 5 Saffir-Simpson
230.				Tornadoes	F0 Fujita Scale
231.					F1 Fujita Scale
232.					F2 Fujita Scale
233.					F3 Fujita Scale
234.					F4 Fujita Scale
235.					F5 Fujita Scale
236.					F6 Fujita Scale
237.				Typhoons	Repeat Lines 225-229.
238.			Thunderstorms	Lightning Strikes	Power Surge
239.					Power Outages

	Class	Activity	Agent Category	Agent	Event
240.					Fire
241.				Severe Rainfall	Flooding
242.			Snowstorms	Heavy Snowfall	Traffic Congestion/Delays
243.					Power Outages
244.			Hailstorms	Large Hailstones	Crop Damage
245.			Freezing Rain	Ice Accumulation	Falling/Personal Injuries
246.					Vehicle Accidents
247.					Power Outages
248.		Animals	Larger Mammals	Deer	Vehicle Collision
249.			Rodents	Squirrels	Gnawed Insulation
250.			Birds	Seagulls	Bird Strikes
251.			Reptiles	Snakes	Snake Bites
252.			Fish	Sharks	Shark Attacks
253.			Insects	Ticks	Lyme Disease Vector
254.		Plants	Noxious Weeds	Variety	Displace Native Plants
255.			Toxic Plants	Poison Ivy	Individual Contact
256.				Poison Oak	Individual Contact
257.				Poison Sumac	Individual Contact
258.			Poisonous Plants	Algae	Poison Water Supply
259.				Fungi	Poison Individuals
260.				Leafy Plants	Poison Individuals

Notes:

1. Clearly, the Threat Listing is not and cannot ever be complete. New threats, especially at the threat event level of detail appear on a regular basis. Therefore, additional entries will be added from time to time. Any suggestions to expand the list may be submitted to the offices identified in the Foreword.
2. When developing a Threat Assessment for a TRA project, all threats within the scope of the assessment may be transferred at the appropriate level of detail from the Threat Listing above to the first five columns of the Threat Assessment Table presented at Appendix C-4.

Appendix C-3 - Threat Metrics

1 Instructions

For each threat within the scope of the TRA project, determine the appropriate levels as follows:

- **Step 1.** Ascertain the relevant level of detail or granularity (threat activity, threat agent category, threat agent or threat event) for each entry based upon the scoping criteria identified in Section 4 of Annex A.
- **Step 2.** For each threat, assess the likelihood of occurrence from Very Low to High based upon current intelligence or sensor readings, if available, or in most cases, past experience and actuarial data –
    - select the closest frequency of past threat events in column 1 of Table C3-1, the Threat Likelihood Table;
    - for all threats (deliberate, accidental and natural hazards) affecting asset subgroups within the scope of the assessment at the same location, choose the corresponding likelihood from Column 2 and proceed to Step 3; and
    - in the case of deliberate threats, however, threat agent intentions may change over time, so threats affecting asset subgroups and locations outside the scope of the assessment may be a matter of future concern and the associated probabilities should be adjusted accordingly:
        - for threats at the same location, but affecting asset subgroups outside the scope of the assessment, select the level from column 3 corresponding to the past frequency identified in column 1,
        - similarly, for threats affecting asset subgroups within the scope of the assessment at different locations outside the scope of the TRA project, select the level from column 3 corresponding to the past frequency identified in column 1, and
        - for threats affecting assets outside the scope of the assessment at different locations, select the level from column 4 corresponding to the past frequency identified in column 1.

Column 1	Column 2	Column 3	Column 4
Past Frequency	**Same Location Similar Assets**	Remote Location but Similar Assets or Same Location but Different Assets	**Remote Location Other Assets**
Daily	High	High	High
1-10 Days	High	High	Medium
10-100 Days	High	Medium	Low
100-1,000 Days	Medium	Low	Very Low
1,000-10,000 Days	Low	Very Low	Very Low
Over 10,000 Days	Very Low	Very Low	Very Low

Table C3-1: Threat Likelihood Table

- **Step 3.** Assess the potential gravity of likely threats based upon the capabilities of deliberate threat agents or the magnitude of accidents and natural hazards, and assign the appropriate level in Table C3-2, the Threat Gravity Table, from Low to High.

Deliberate Threat Agent Capabilities	Magnitude of Accidents or Natural Hazards	Threat Impact or Gravity
Extensive Knowledge/Skill Extensive Resources	Highly Destructive Extremely Grave Error Widespread Misuse > 25% of Asset Subgroup Affected Interruptions > 5 Working Days	High
Limited Knowledge/Skill Extensive Resources or Extensive Knowledge/Skill Limited Resources or Moderate Knowledge/Skill Moderate Resources	Moderately Destructive Serious Error Significant Misuse > 5% of Asset Subgroup Affected Interruptions > 3 Working Hours	Medium
Limited Knowledge/Skill Limited Resources	Modestly Destructive Minor Error Limited Misuse < 5% of Asset Subgroup Affected Interruptions < 3 Working Hours	Low

Table C3-2: Threat Gravity Table

- **Step 4.** Determine the level of each threat from Very Low to Very High by correlating the assessed likelihood in the horizontal axis of Table C3-3, the Threat Level Table, with the threat gravity in the vertical axis.

Threat Gravity	**Threat Likelihood**			
	Very Low	**Low**	**Medium**	**High**
High	Low	Medium	High	Very High
Medium	Very Low	Low	Medium	High
Low	Very Low	Very Low	Low	Medium

Table C3-3: Threat Levels Table

- **Step 5a.** Depending upon the nature of the expected compromise, enter the results under the appropriate Threat Levels columns for confidentiality, availability and/or integrity in the Threat Assessment Table at Appendix C-4.
- **Step 5b.** Whenever doubts remain regarding the actual threat level, both the high and low values may be entered in the Threat Assessment and used for the calculation of residual risk during the Risk Assessment Phase (Annex E) to determine if this uncertainty has any impact on the assessed residual risk.

- **Step 5c.** Threats that fall close to the threshold between two levels should be flagged for subsequent analysis during the Risk Assessment Phase of the TRA project, using arrows (↑↓) to indicate whether they fall near the high or low end of the range. For example, if the past frequency of a threat has been every 110 days, in the Medium but close to a High likelihood, the ultimate threat level should be marked (↑) accordingly.
- **Step 5d.** Whenever the likelihood of a deliberate threat is rated Low or Medium, a second threat level should be computed on the basis of a High likelihood and subsequently used to calculate a second assessed residual risk during the Risk Assessment Phase because threat agent intentions can change far more quickly than the necessary countermeasures can be acquired and installed.
- **Step 6.** Enter the results under the appropriate columns in the Threat Assessment Table at Appendix C-4.

2 Examples

2.1 Theft

If the theft of office supplies and personal possessions from government facilities in the immediate area of a TRA project occurred on a weekly basis over the past year, the likelihood of further incidents affecting similar assets should be assessed as High. If the culprits were generally individuals with only moderate knowledge, skills and resources, the impact or gravity would be Medium, for an overall threat level of High to the Availability of the associated assets.

2.2 Armed Robbery

If local businesses in the private sector suffered armed robberies every two or three weeks, the likelihood of similar threats materializing in the future would be assessed as High. If government offices had not been affected, however, the relative probability should be tempered, using column 3 (Same Location but Different Assets) in Table C3-1 to derive a Medium likelihood. Where the armed robberies were conducted by well-organized gangs with significant knowledge, skills and resources, the impact or gravity would be High, for an overall threat level of High to the Availability of the associated assets in government facilities, and Very High in the private sector.

2.3 Misdirected E-Mail

If careless employees misdirect Protected A messages to the wrong addressees about once or twice a year, the likelihood of recurrence would be assessed as Medium. If these errors affected less than one percent of all Protected A traffic, the impact or gravity would be Low, thereby indicating a Low level accidental threat to Confidentiality.

2.4 Floods

If local floods disrupt operations for three or four days in a typical year, the likelihood of future interruptions would be rated Medium, because four days annually represents a Past Frequency less than once every 100 days spread out over the entire year. If the impact were a ten percent loss of productivity, the gravity should be rated Medium, to give an overall threat level of Medium to the Availability of the affected services.

This page intentionally left blank.

Appendix C-4 - Threat Assessment Table

Threat Class	Threat Activity	Threat Agent Category	Threat Agent	Threat Event	Threat Levels Affecting			Asset Subgroup(s) Affected
					C	A	I	
Deliberate	Espionage							
	Sabotage							
	Subversion							
	Terrorism							
	Criminal Acts							
	Others							
Accidental	Office Accidents							
	Data Corruption							
	Software Errors							
	Hardware Failures							
	Mechanical Failures							
	Structural Failures							
	Fires							
	Industrial Accidents							
	Nuclear Accidents							
Natural Hazards	Disease							
	Earth Movement							
	Flooding							
	Environmental							
	Severe Storms							
	Plants & Animals							

Legend
C – Confidentiality. A – Availability. I – Integrity.

1 Instructions

Enter all threats within the scope of the TRA project at the appropriate level of detail (Threat Activity, Threat Agent Category, Threat Agent and Threat Event) from the Threat Listing in Appendix C-2.

Based upon the Expanded Threat Metrics in Appendix C-3, determine the relevant levels for each threat ranging from Very Low through Very High (VL through VH) with respect to the confidentiality (C), availability (A) and/or integrity (I) of the affected asset subgroups.

2 Examples

2.1 Espionage

If the espionage threat posed by a specific intelligence service were assessed to be High with respect to the confidentiality of military plans based upon the likelihood of occurrence and the capabilities of the adversary, the following would be noted in the Threat Assessment Table:

Threat Class	Threat Activity	Threat Agent Category	Threat Agent	Threat Event	Threat Levels Affecting			Asset Subgroup(s) Affected
					C	A	I	
Deliberate	Espionage	Intelligence Services	Specific Service	–	H	–	–	Military Plans

2.2 Hacker

If the hacker threat to corporate data files were assessed as Medium for both unauthorized access (Confidentiality) and unauthorized modification (Integrity) but High for denial of service attacks (Availability), the following entries would be noted in the Threat Assessment Table:

Threat Class	Threat Activity	Threat Agent Category	Threat Agent	Threat Event	Threat Levels Affecting			Asset Subgroup(s) Affected
					C	A	I	
Deliberate	Espionage	Hackers	–	Unauthorized Access	M	–	–	Corporate Data Files
	Sabotage	Hackers	–	Unauthorized Modification	–	–	M	Corporate Data Files
	Sabotage	Hackers	–	Denial of Service	–	H	–	Corporate Data Files

2.3 Power Surge

If threat of periodic power surges causing physical damage to sensitive electrical instruments were assessed as High (Availability) but that of concurrent data corruption were deemed to be Low (Integrity), the following entries would be noted in the Threat Assessment Table:

Threat Class	Threat Activity	Threat Agent Category	Threat Agent	Threat Event	Threat Levels Affecting			Asset Subgroup(s) Affected
					C	A	I	
Accidental	Mechanical Failure	Public Utilities	Power Company	Power Surge	–	H	–	Electrical Instruments
Accidental	Mechanical Failure	Public Utilities	Power Company	Power Surge	–	–	L	Data Files

This page intentionally left blank.

Annex D - Vulnerability Assessment

1 Introduction

1.1 General

The fourth phase of a TRA project, the Risk Assessment, is conducted in two sequential segments, namely the Vulnerability Assessment and the Calculation of Residual Risk. The former comprises five successive processes and one major output as follows:

- **Safeguard Identification** – to list all existing and proposed safeguards that fall within the scope of the assessment at an appropriate level of detail;
- **Safeguard Effectiveness Assessment** – to determine the effectiveness of these safeguards in mitigating potential risks;
- **Vulnerability Identification** – to identify remaining vulnerabilities that expose assets within the scope of the assessment to threats identified during the third phase;
- **Vulnerability Impact Analysis** – to assess the effects of vulnerabilities on the likelihood of threat occurrence, the probability of compromise and the severity of ensuing damage;
- **Vulnerability Assessment** – to assign relative levels from Very Low to Very High for each vulnerability based upon common metrics for increased exposure to the compromise of confidentiality, availability or integrity; and
- **Prioritized Vulnerability Assessment Table** – to produce a comprehensive list of vulnerabilities which may be ranked from the most serious to the least.

1.2 Aim

The aim of this annex is to describe the five processes and single output of the Vulnerability Assessment within the Risk Assessment Phase of a TRA project.

2 Safeguard Identification

2.1 Safeguard Definition

> ***Safeguards*** *(Mesures de protection)* – assets or external controls that reduce overall risk to employees, other assets or service delivery by decreasing the likelihood of a threat event, reducing the probability of compromise, or mitigating the severity of the outcome through direct or indirect interaction with asset values, threats or vulnerabilities.
>
> New Definition

Safeguards are security measures or controls that perform one or more functions to mitigate overall risk by reducing asset values, threats or vulnerabilities within the scope of a TRA project. Ultimately, these reductions in the primary risk variables are intended to decrease the likelihood of a threat event occurring in the first place, diminish the probability of compromise should a threat event actually arise, or moderate the severity of the outcome, as indicated in the new definition.

2.2 Safeguard Listing

In order to assess vulnerabilities that expose assets within the scope of a TRA project to greater risk, existing and proposed safeguards must first be identified and then analyzed to determine their relative effectiveness. Since most security measures or mechanisms are also assets, many should have been captured during the Asset Identification Phase. To complement this effort, however, the Recommendation Phase of a TRA project, detailed at Annex F, provides further guidance including an examination of safeguards and safeguard selection criteria to address any residual risks that are deemed unacceptable. Some useful sources of safeguard data are cited at Appendix F-1 while Appendix F-2 presents an extensive listing of security measures as an aide-mémoire to facilitate the Safeguard Identification Process within the Vulnerability Assessment.

3 Safeguard Effectiveness

3.1 General

As a general rule, risk and the causal vulnerabilities are inversely proportional to safeguard effectiveness. In essence, as more robust security measures are implemented to protect assets within the scope of an assessment, vulnerabilities and the associated risks tend to decrease accordingly. Within the *Harmonized TRA Methodology*, two factors are considered when assessing safeguard effectiveness. Firstly, the security functions performed by all protective measures indicate how they interact with the primary risk variables, namely asset values, threats and vulnerabilities. Secondly, their impact on threat events, specifically the likelihood of occurrence, probability of compromise and severity of the outcome, are examined as indicators of overall effectiveness.

3.2 Security Functions: Impact on Risk Variables

Recognizing that risk management involves the acceptance of some risks with the possibility of certain threats injuring employees or assets and disrupting service delivery, the GSP introduces the concept of active defence, especially with respect to IT assets, "to prevent, detect, react to and recover from security incidents."[1] In effect, most safeguards perform one or more of these basic security functions, namely prevention, detection, response and recovery. Two more options, specifically avoidance and deterrence, should also be considered to complete the model.

- **Avoidance.** In some cases, it is possible to reduce or avoid risk by lowering asset values. For example, many convenience stores limit cash on hand to a small amount after normal working hours. Although this security measure has absolutely no effect on vulnerabilities and does nothing to prevent armed robberies, it can mitigate at least some of the consequences by limiting the financial loss. (A secondary benefit may include some deterrent value, convincing would-be thieves to look elsewhere for more lucrative targets.) For some threats, chiefly natural hazards, the likelihood of occurrence may be

[1] **Section 10.12 of the GSP** identifies the requirement which is subsequently amplified in **section 15 of the *Management of IT Security (MITS) Operational Security Standard***.

controlled significantly by avoiding certain locations prone to various problems. For instance, building on higher ground can diminish the likelihood of flooding, while facilities located on the Canadian Shield suffer fewer earthquakes than those situated along major fault lines.

- **Deterrence.** Some safeguards, such as visible warning signs and large barking dogs, aim to dissuade deliberate threat agents who may be contemplating an attack, thereby decreasing threat agent intentions and, therefore, the probability of occurrence. Like avoidance measures, deterrent mechanisms do not address vulnerabilities directly, so their effects are considered during the Asset Identification and Valuation (for some avoidance safeguards) and the Threat Assessment Phases of a TRA project.[2]
- **Prevention.** A few preventive measures target deliberate threat agents in order to reduce the likelihood of occurrence. For example, the successful prosecution of thieves can limit their ability to conduct further burglaries for at least the duration of their incarceration and, in theory, gun control legislation should decrease the incidence of armed robberies. In general, however, most preventive measures tend to address specific vulnerabilities, thereby decreasing the probability of compromise should a threat actually arise. Robust identification and authentication mechanisms, for example, may do little to dissuade hackers and reduce the likelihood of an attack, but they should defeat most attempts to gain unauthorized access to a computer system, thereby reducing the probability of compromise.
- **Detection.** Early detection of threat events can address certain vulnerabilities and permit a rapid response to contain the damage and limit the severity of the outcome.
- **Response.** Alone, detection mechanisms do little to restrict the damage of a threat event. Coupled with a quick response, however, the combination of safeguards can do much to mitigate risk by reducing the amount of harm arising from a compromise.
- **Recovery.** Recovery mechanisms, such as backup procedures and offsite storage of critical data, can correct other vulnerabilities and promote an early return to normal operations, again mitigating the severity of the outcome.

3.3 Safeguards: Impact on Threat Events

As noted above, some safeguards help avoid certain threats, especially natural hazards, while others may deter deliberate threat agents. Many security measures are intended to prevent a compromise when threats actually occur. A few control the amount of damage sustained by limiting asset values, but many more mitigate injuries through early detection coupled with rapid response and recovery mechanisms. The relationships amongst these varied effects and the overall impact upon the likelihood of occurrence, probability of compromise and severity of outcome are the fundamental measures of safeguard effectiveness.

- **Likelihood of Occurrence.** Whenever feasible, choosing sites where threat events of a certain kind have rarely if ever occurred in the past can be extremely effective as an avoidance mechanism to reduce the likelihood of future problems. For example, the city of Vancouver suffers far fewer debilitating snowstorms than some eastern counterparts,

[2] The impact of avoidance measures on asset value are considered in section 4 of Annex B, while the effects of both avoidance and deterrence mechanisms on threat likelihood are examined in section 3 of Annex C.

but the west coast is inherently more susceptible to earthquakes than much of the country. Frequently, the relative probabilities at different sites can be calculated quite precisely to provide an accurate assessment of safeguard effectiveness for many avoidance measures. On the other hand, the effectiveness of deterrent mechanisms, such as warning signs, to reduce the probability of threat events is generally more questionable. Since it is virtually impossible to avoid or deter all threats, other approaches must be included in a balanced suite of mutually supporting safeguards to optimize overall effectiveness.

- **Probability of Compromise.** More rigorous preventive measures are more likely to thwart a compromise should a threat event actually occur. For example, a high quality combination lock is more likely to prevent surreptitious access to sensitive assets than a keyed padlock, so it is a more effective safeguard. In some cases, the actual reduction in the probability of compromise can be measured quite precisely and expressed in very concrete terms, as with cryptographic algorithms and passwords of different lengths and structures. For other safeguards, such as security awareness and training, the impact is more nebulous, and any assessment of effectiveness will be far more subjective.
- **Severity of Outcome.** Knowing that avoidance, deterrence and prevention mechanisms are rarely foolproof, other safeguards should normally be implemented in a layered defence to limit the amount of damage in the event of a compromise, and to facilitate a quick and complete recovery. More effective detection systems, such as intrusion alarms, are generally more difficult to evade and more likely to provide an early warning of unauthorized activities, with fewer false alarms. In a similar vein, the relative effectiveness of any response may be measured in terms of its capacity to limit or contain the injury arising from the threat event. For example, well-engineered buildings can frequently withstand even serious earthquakes without significant damage. In effect, structural integrity as a safeguard has no bearing on the likelihood of occurrence, but it may limit or contain the injury that might otherwise be expected.[3]

3.4 Safeguard Impact Table

The effects of safeguards on risk variables and threat events are summarized in Table D-1, the Safeguard Impact Table, according to the security functions they perform. These relationships are explored in greater detail in Annex F, the Recommendation Phase of a TRA project.

[3] In fact, structural integrity may prevent damage in the first place, thereby decreasing the likelihood of compromise. Thus, this safeguard may perform both the prevention and response or containment security functions.

Security Functions	Impact of Safeguards						
	On Risk Variables				On Threat Event		
	A_{Val}	T		V	O_{Prob}	C_{Prob}	O_{Sev}
		L	G				
Avoidance[4]	⇓	↓			↓		⇓
		⇓			⇓		
Deterrence		⇓			⇓		
Prevention[5]			↓	⇓	↓	⇓	
Detection				⇓			⇓
Response				⇓			⇓
Recovery				⇓			⇓

Legend

A_{Val} – Asset Value. **T** – Threat. **L** –Threat Likelihood.
G – Threat Gravity (Threat Agent Capabilities). **V** – Vulnerability.
O_{Prob} – Likelihood of Threat Occurrence. C_{Prob} – Probability of Compromise.
O_{Sev} – Severity of Outcome.
Primary Impact – ⇓ Secondary Impact – ↓

Table D-1: Safeguard Impact Table

4 Vulnerability Identification

4.1 Vulnerability Definition

4.1.1 GSP Definition

In the GSP, vulnerability is defined as "an inadequacy related to security that could permit a threat to cause harm."[6] While this statement certainly captures one important aspect of vulnerabilities, specifically the negative implications of poor safeguards, some other dimensions merit further consideration.

4.1.2 Vulnerabilities as Attributes

It is often misleading to characterize vulnerabilities solely as "inadequacies" because they can include some of the most positive features of an asset. For example, it serves little purpose for an art gallery to acquire a valuable painting then lock it away for safekeeping. It must be accessible to the viewing public, even though this accessibility is also a vulnerability that

[4] The first line illustrates the impact of a reduction in asset value, primarily a decrease in the severity of the outcome of a compromising threat event with a potential decline in the likelihood of certain deliberate threats due to a deterrent effect. The second line captures the impact of site selection to avoid certain threats, generally natural hazards, with the associated drop in the likelihood of a threat event actually occurring.

[5] Most preventive measures address vulnerabilities to reduce the probability of compromise should a threat event take place, but a few endeavour to restrict the capabilities of deliberate threat agents with a corresponding decrease in either the likelihood of occurrence or the probability of compromise.

[6] **Appendix B to the GSP, Glossary**.

exposes the asset to various threats, such as theft or vandalism. Thus, it would be more appropriate to define vulnerabilities as attributes, both positive and negative, that render assets more susceptible to compromise. Furthermore, vulnerabilities might be qualities of the asset itself or characteristics of the environment in which it is located. Thus, the portability of notebook computers, a positive feature of the asset, increases the likelihood of theft, whereas inadequate training for hydro employees, a negative trait in the surrounding environment, could increase both the probability of power outages and their duration.

4.1.3 Effects of Vulnerabilities

In general, all vulnerabilities contribute to risks in one or more of three different ways. Firstly, some attributes increase the probability that a threat event will actually occur. For example, the visibility of attractive items in a jewellery store window may encourage a higher rate of theft. Secondly, some vulnerabilities increase the likelihood that a threat event will compromise an asset. To continue the previous example, the visibility of valuable assets does not necessarily make them easier to steal, but a thief is more likely to succeed in the absence of bars or shatterproof glass. Finally, other vulnerabilities allow threat events to cause even greater damage. A faulty burglar alarm does not, in itself, increase either the likelihood of a break-in attempt or the probability of its success. It could, however, delay an effective response, thereby allowing the thieves to cause more harm. Of course, some vulnerabilities, such as insufficient training, may have two and even three of these side effects.

4.1.4 Vulnerabilities versus Safeguard Effectiveness

Although some safeguards alleviate risk by manipulating asset values or threats rather than vulnerabilities, as indicated in section 2.1 above, most security measures are intended to correct certain vulnerabilities either directly or indirectly. As safeguard effectiveness increases, the impacts of the associated vulnerabilities tend to decrease. In other words, vulnerabilities are inversely proportional to safeguard effectiveness as illustrated in Figure D-1. This relationship is the basis for vulnerability classes noted below.

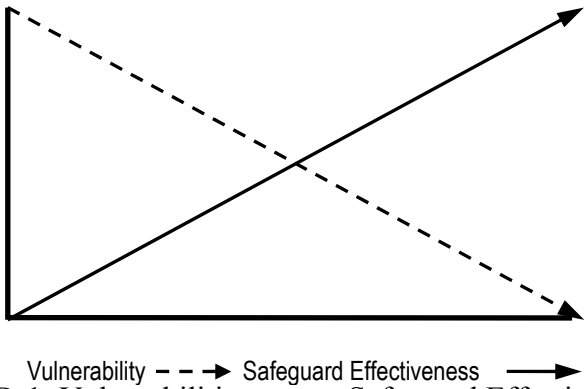

Figure D-1: Vulnerabilities versus Safeguard Effectiveness

4.1.5 Extended Definition

For purposes of the *Harmonized TRA Methodology*, the basic definition of vulnerability provided in the GSP is expanded to incorporate these three concepts, namely (1) vulnerabilities as attributes of assets or their environment; (2) their effects on the likelihood of threat events, the probability of compromise and the magnitude of the resulting injury; and (3) their inverse relationship with safeguard effectiveness.

Vulnerability *(vulnérabilité)* – an attribute of an asset or the environment in which it is located that increases the likelihood of a threat event, the probability of compromise or the severity of the outcome. Vulnerabilities are inversely proportional to safeguard effectiveness.

New Definition

4.2 Vulnerability Classes

4.2.1 General

Some safeguards, such as avoidance and deterrent mechanisms, do not address vulnerabilities directly. On the other hand, all vulnerabilities, even positive attributes, represent some inadequacy with the associated security measures. For example, a design flaw in a piece of machinery might be a vulnerability that could increase the likelihood of catastrophic failure. In turn, this fault might be attributed to some ineffective safeguards, such as insufficient review during the design process or inadequate stress testing. Given this fundamental relationship between vulnerabilities and safeguards, they might be categorized in broad classes related to the policy requirements in the GSP and the more detailed security measures prescribed in subordinate operational security standards and technical documentation as outlined below.

4.2.2 Security Program

Poorly defined roles and responsibilities for security, inadequate human and financial resources, and confusing or incomplete security policies and procedures are particularly serious vulnerabilities. While they may not increase the likelihood of occurrence for any given threat, these failings would almost inevitably increase the probability of compromise and the severity of the outcome should a threat arise, with potentially serious consequences for confidentiality, availability and integrity.

4.2.3 Sharing of Information and Assets

Inadequate arrangements for the sharing of information, facilities and IT infrastructure can introduce many vulnerabilities affecting both the probability of compromise and the severity of the outcome, again with adverse consequences for confidentiality, availability and integrity.

4.2.4 Security Outside Canada

Security risks vary considerably in other parts of the world so regular assessments are required to avoid potential vulnerabilities that might expose employees and assets to a greater probability of compromise and more severe outcomes. Once more, all three asset values (confidentiality, availability and integrity) might be affected. In the case of travel restrictions, ill-informed assessments might also lead Canadians to visit locations where the likelihood of certain threats is much greater.

4.2.5 Contracting

Ignorance regarding contract security and the associated procedures governing Security Requirements Check Lists (SRCLs)[7] and facility security clearances could increase the likelihood of compromise, especially unauthorized disclosure of classified or protected information.

4.2.6 Security Awareness and Training

Inadequate security awareness and training are amongst the most serious vulnerabilities because they can jeopardize virtually all assets, increasing the likelihood of threat events in the first place, as well as the probability of compromise and the severity of the outcome, affecting confidentiality, availability and integrity.

4.2.7 Identification of Assets

Improper categorization and marking of assets can introduce severe vulnerabilities leading to flawed risk management and the misapplication of other safeguards, thereby increasing the likelihood of compromise and the severity of the outcome with respect to confidentiality, availability or integrity, depending upon which asset values are involved.

4.2.8 Security Risk Management

Since the application of baseline security standards and continuous risk management are the two bases for the selection of all other safeguards, any faults with security risk management could have a cascading effect to cause many more vulnerabilities, increasing the likelihood of threat events occurring in the first place, as well as the probability of compromise and the severity of the outcome, affecting confidentiality, availability and integrity.

4.2.9 Access Limitations

Inadequate access limitations can increase both the probability of compromise and the severity of the outcome. The need to know principle applies primarily to confidentiality, while the other safeguards may protect all three asset values.

4.2.10 Security Screening

If the initial screening process is flawed, the likelihood of compromise may increase significantly. Conversely, vulnerabilities arising from inadequate review, revocation and release procedures can increase the severity of the outcome. Ineffective security clearances and site access clearances tend to jeopardize confidentiality, whereas weak reliability checks could put all three asset values at risk.

4.2.11 Protection of Employees

Vulnerabilities associated with ineffective measures for the protection of employees can increase both the likelihood and the severity of physical and psychological injuries, serious availability concerns.

[7] Form number TBS/SCT 350-103(2004/12) available at: http://www.tbs-sct.gc.ca/tbsf-fsct/350-103_e.asp.

4.2.12 Physical Security

Physical security measures perform a broad array of security functions, so the impacts of any associated vulnerabilities on the likelihood of occurrence, the probability of compromise and the severity of the outcome vary considerably, as do the asset values affected. Some, such as site selection, are essentially avoidance mechanisms to choose a location where threats are less likely to occur, so any weaknesses could increase the probability of threats actually materializing. Apart from exterior signs, which are largely deterrent in nature, most perimeter security measures are intended to prevent the compromise of assets by certain threats or detect them in progress to mitigate the amount of damage. Any related vulnerabilities could increase the probability of compromise or the severity of the outcome, with adverse consequences for confidentiality, availability and integrity. Other vulnerabilities related to access controls, facility management, secure storage and transport and transmittal may, with a few exceptions, affect all three asset values, but the primary impact on risk is an increased probability of compromise because they are essentially prevention mechanisms. Destruction safeguards are intended to prevent unauthorized disclosure, so any associated vulnerabilities are generally confidentiality concerns, with an increased probability of compromise.

4.2.13 IT Security

Like physical security measures, IT safeguards serve several different security functions including prevention, detection, response and recovery. Therefore, any related vulnerabilities could increase the probability of compromise or the severity of the outcome. Some IT security measures, such as management controls, affect all three asset values, while others are more specifically focused. Most technical safeguards are preventive in nature, so any weaknesses would increase the likelihood of compromise, but malicious code protection may also includes detection and response capabilities, so any failures could increase the severity of the outcome as well. Since intrusion detection and backup/recovery are detection and recovery mechanisms respectively, associated vulnerabilities would increase the severity of the outcome. Some technical safeguards, such as Public Key Infrastructure (PKI), can protect all three asset values while others concentrate on only one or two. For example, emanations security is purely a confidentiality control while backup and recovery are availability measures. Finally, any vulnerabilities related to operational safeguards may increase the probability of compromise or the outcome severity. Most affect all three asset values, but capacity planning, environmental protection, power conditioning and backup are essentially availability concerns.

4.2.14 Security in Emergencies

Without clearly established readiness levels and associated security procedures, the response to emergencies and increased threat situations may be too slow or incomplete, so the severity of the outcome could be much greater. In some cases, where there is some forewarning of the threat, these vulnerabilities could also increase the probability of compromise. While some emergencies may affect confidentiality or integrity, most involve the destruction of assets and the interruption of services, two availability concerns.

4.2.15 Business Continuity Planning

Any inadequacies related to business continuity planning could delay the resumption of critical services in the event of a loss, thereby increasing the severity of the outcome, a potentially serious availability issue.

4.2.16 Investigation of Incidents

Vulnerabilities arising from ineffective investigation and reporting procedures can increase the probability of further compromise if the root causes are not assessed correctly. Similarly, the ensuing injury could also increase with serious consequences for confidentiality, availability or integrity, depending upon the nature of the security incident.

4.2.17 Sanctions

Formal sanctions may deter repeat offenders, so their absence could possibly increase the likelihood of further infractions. Similarly a failure to remove or transfer serious wrongdoers as a preventive measure, could allow them to commit further offences, also increasing the probability of recurrence, with possible compromises to confidentiality, availability or integrity depending upon the nature of the security breaches or violations.

4.3 Sources of Vulnerability Data

4.3.1 Information Sharing

Vulnerability data are often more difficult to collect and assess than the other risk variables because many organizations are reluctant to admit to any flaws or weaknesses in the security posture of their products, programs or facilities for fear of censure or legal liability. Therefore, as indicated in section 2 of Annex A, the Preparation Phase, senior management commitment to the TRA process is crucial to break down these barriers and promote information sharing in the best interests of the entire organization.

4.3.2 Departmental Resources

Once these issues are addressed, however, departmental managers and security authorities have much to offer. A clear understanding of the relevant business processes can help uncover certain vulnerabilities, especially with respect to the overall security program. A careful review of design documentation, schematics and floor plans can be another useful source of information. Facility managers and systems administrators will know the kinds of problems that have occurred in the past and, therefore, the security weaknesses that have exposed assets or employees to injury. Departmental security authorities will understand most of the safeguards implemented to date and know many of their inherent shortcomings. In the case of IT systems in particular, security testing and evaluation can reveal many, but not all flaws. Internal audits and reviews frequently focus on the adequacy of management controls. Finance, human resources, and occupational health and safety authorities may also provide details on specific vulnerabilities affecting financial systems and employees respectively.

4.3.3 External Resources

Certain security lead departments offer extensive advice and guidance on an array of safeguards and at least some of the associated vulnerabilities. Several professional associations explore different aspects of security, providing assessments of different safeguards and related

vulnerabilities. Many journals review security products and comment on their effectiveness. A number of web sites contain current information on technical vulnerabilities associated with IT systems and products.

4.3.4 Summary

Appendix D-1 lists a variety of potential sources for vulnerability data, and the types of information they might provide to a TRA team.

4.4 Data Collection Techniques

As with the asset identification process described in section 2 of Annex B, the collection of vulnerability data should begin with a careful review of relevant documentation. Material of interest could range from departmental business plans and security policies for general orientation to more specific records directly related to the subject of the TRA project, including installation manuals and operating instructions, some of which are listed in Appendix D-1. Findings from this research should be confirmed through interviews with knowledgeable program, project, facility management, IT and security authorities, depending upon the nature of the assessment. While much of the information may be accepted at face value, it is usually preferable to corroborate the results with on-site inspections and security testing. Independent verification and validation may be advisable for particularly sensitive assets at higher risk, in order to ensure a comprehensive and impartial vulnerability assessment. Finally, the *Harmonized TRA Methodology* includes a substantial list of vulnerabilities in Appendix D-2 as an aide-mémoire during the vulnerability identification process.

4.5 Vulnerability Listing

4.5.1 Structure

The Vulnerability Listing in Appendix D-2 is presented as a hierarchical table with a structure much like the Asset and Threat Listings in Appendices B-2 and C-2 respectively. From the 16 vulnerability classes described in section 4.2, the list branches out to encompass more detailed vulnerability groups and discrete vulnerabilities. Each of these levels is defined below, and the actual structure is illustrated in Figure D-2:

- **Vulnerability Class.** A generic group of vulnerabilities based upon the broad security policy requirements defined in the GSP and supporting documentation.
- **Vulnerability Group.** A subdivision of vulnerability class, intended to capture all vulnerabilities associated with a related group of security measures.
- **Specific Vulnerability.** An actual flaw or inadequacy related to a specific safeguard that could expose employees, assets or service delivery to compromise.

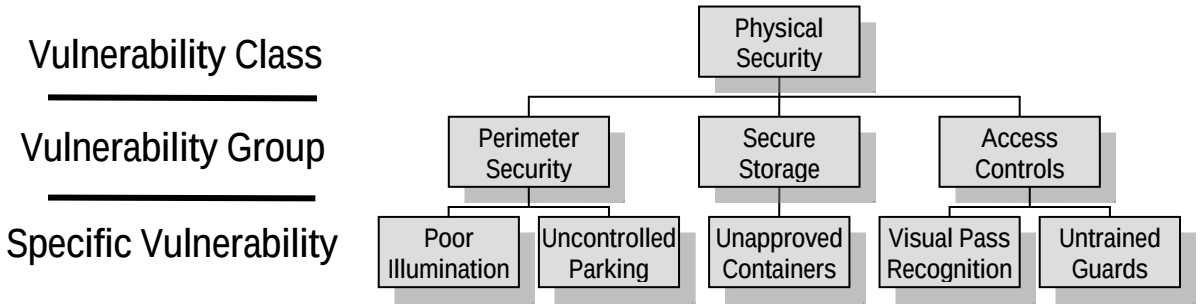

Figure D-2: Vulnerability Listing Hierarchical Structure

4.5.2 Benefits

Like the Asset and Threat Listings, the hierarchically structured Vulnerability Listing offers several important advantages when conducting a TRA project:

- **Consistency.** The use of common data structures and definitions for vulnerability identification facilitates communications within and between TRA projects to achieve consistent results that can be replicated by different practitioners assessing the same or similar vulnerabilities. It also promotes interoperability with the sharing of vulnerability data between organizations.
- **Completeness.** Important vulnerabilities are less likely to be overlooked with the use of a comprehensive list to guide TRA teams.
- **Flexibility and Scalability.** The Vulnerability Listing offers fewer benefits for flexibility and scalability than the corresponding Asset and Threat Listings because most inadequacies must be assessed at the lowest level of detail. On the other hand, entire branches of the tree-like structure might be ignored for any vulnerability class falling outside the scope of the assessment. For example, vulnerabilities related to the protection of employees might be excluded in cases where personnel are not an issue.
- **Currency.** The Vulnerability Listing is easily updated as new vulnerabilities are identified. Furthermore, given the logical groupings of similar vulnerabilities, it is much simpler to categorize new or emerging problems.

4.5.3 Caveat

Again, as with the Asset and Threat Listings, the Vulnerability Listing must be used with caution. It is not and cannot be complete because new vulnerabilities, especially with respect to IT security, are encountered on a regular basis due, in part, to rapidly changing technologies and evolving threat agent capabilities. **Thus, Appendix D-2 should be employed as an aide-mémoire and guide to help organize and structure the collection and collation of relevant vulnerability data, rather than a check-list to be followed without question.**

5 Vulnerability Impact Analysis

5.1 Vulnerability Metrics

As indicated in section 4.1 above, all vulnerabilities contribute to risk in one or more of three different ways. A few, such as adverse location or the visibility of valuable assets, may increase the possibility that a threat event will actually occur. Therefore, vulnerabilities of this nature are normally factored into the likelihood assessment within the Threat Assessment Phase of a TRA project, examined in section 3 of Annex C. The other potential effects of any vulnerability, namely an increase in either the probability of compromise or the severity of the outcome, provide the basis for suitable metrics to permit comparative analysis of different vulnerabilities that expose varied assets to harm.

5.2 Probability of Compromise

5.2.1 General

Effective preventive measures reduce the likelihood that a threat event will compromise an asset. Any vulnerabilities or inadequacies associated with these safeguards have the opposite effect, increasing the probability of unauthorized disclosure, destruction, removal, modification, interruption or use of assets depending upon the nature of the threat.

5.2.2 Basic Assessment Criteria

Some important factors to consider when assessing the impact of vulnerabilities related to inadequate or ineffective preventive measures include:

- **Likelihood of Prevention.** If there were no preventive measures in place, or they were largely ineffective, the associated probability of compromise would be High, approaching absolute certainty in the worst case scenario. Moderately effective prevention mechanisms would thwart at least some threats while allowing others to cause harm, so the related probability of compromise would fall in the Medium range. Very effective safeguards could prevent injuries in most cases, thereby reducing the probability of compromise to a Low level.
- **Ease of Exploitation.** Vulnerabilities that expose assets to deliberate threats may be rated according to their ease of exploitation. Those that are simple to abuse, that require little specialized knowledge, skill or resources to manipulate successfully, are particularly dangerous because the associated probability of compromise would be High. Others that call for moderate knowledge, skill or resources are more likely to foil some threats, so the probability of compromise would fall into the Medium range. Finally, very obscure vulnerabilities that are difficult to understand, or require extensive skills and resources to exploit, would have only a Low impact on the probability of compromise. For analytical purposes when assessing vulnerabilities on this basis, the knowledge required to circumvent a safeguard could be derived from either formal training, mentoring or practical experience. If, for example, an assailant required a graduate degree in a specialized field of study to understand a weakness, its impact on the probability of compromise is likely to be Low. Skills include

manual or mental dexterity, aural or visual acuity, and other personal attributes of prospective threat agents. Resources range from financial backing to the availability of specialized attack tools, such as supercomputers to decrypt high-grade ciphers.

- **Relevant Asset Attributes.** Some weaknesses in preventive measures are clearly related to various attributes of assets or their environment. For example, easy accessibility can facilitate many different threats, with a corresponding increase in the probability of compromise. Fragile items are more likely to break. Complex mechanisms are more likely to fail. Small, portable objects are easier to conceal and remove. As assets become less accessible, more robust, simpler and firmly attached, the probability of compromise tends to decrease.
- **Employee Awareness/Training.** Poorly trained, unaware employees are less likely to prevent many deliberate and accidental threats, so the probability of compromise would increase. Conversely, well-informed, properly trained and highly motivated employees are more likely to prevent threats from compromising assets.

5.2.3 Impact on Probability of Compromise

For each vulnerability exposing assets within the scope of the assessment, determine the impact on the probability of compromise based upon the relative effectiveness of associated prevention mechanisms, the ease of exploitation, the potential effects of adverse asset attributes, or the extent of employee awareness and training. Assign a level of Low, Medium or High from Table D-2, the Vulnerability Impact on Prevention, or Not Applicable if the vulnerability relates only to detection, response and recovery measures.

Safeguard Effectiveness	Associated Vulnerabilities	Probability of Compromise
No Safeguard Safeguard Largely Ineffective Probability of Compromise > 75%	Easily Exploited Needs Little Knowledge/Skill/Resources Assets Highly Accessible Assets Very Complex/Fragile/Portable Employees Ill-Informed/Poorly Trained	High
Safeguard Moderately Effective Probability of Compromise 25-75%	Not Easily Exploited Needs Some Knowledge/Skill/Resources Assets Moderately Accessible Assets Fairly Complex/Fragile/Portable Moderate Employee Awareness/Training	Medium
Safeguard Very Effective Probability of Compromise < 25% (Safeguard Performs Only Detection, Response or Recovery Functions)	Difficult to Exploit Needs Extensive Knowledge/Skill/Resources Access to Assets Tightly Controlled Assets Very Simple/Robust/Static Employees Well-Informed/Trained	Low (Not Applicable)

Table D-2: Vulnerability Impact on Probability of Compromise (Prevention)

5.3 Severity of Outcome

5.3.1 General

Effective detection, response and recovery measures reduce the amount of damage arising from a compromising threat event. Any vulnerabilities or inadequacies associated with these safeguards have the opposite effect, increasing the severity, either the magnitude or the duration, of the unauthorized disclosure, destruction, removal, modification, interruption or use of assets.

5.3.2 Basic Assessment Criteria

Some important factors to consider when assessing the impact of vulnerabilities that increase the severity of a compromise include:

- **Detection.** The effectiveness of any detection mechanism is generally a measure of two attributes, namely: the degree of certainty that it will expose certain threat events; and the efficiency with which it operates to prompt an early response. Inadequacies or vulnerabilities associated with these safeguards could increase the severity of a compromise by allowing it to continue unnoticed and unchecked. With no safeguards or largely ineffective detection measures, the impact on the severity of the outcome would be High. Where there is a significant probability that threat events will be detected over time, the impact would fall in the Medium range. Where immediate detection is almost certain, the vulnerability would have a Low impact.
- **Response.** Once a compromising threat event has been detected, response mechanisms might be activated to limit or contain the associated injury. For example, heat or smoke sensors (two detection devices) might trip a sprinkler system (a fire suppression safeguard). Any inadequacies or vulnerabilities related to these security measures could increase the severity of the compromise with impacts ranging from Low (damage tightly contained) to High (little intervention to limit injuries).
- **Recovery.** As with detection mechanisms, the effectiveness of recovery measures may be assessed in two dimensions, namely: the time required to reinstate affected assets or services; and the level of restoration. More effective safeguards tend to promote an earlier return to normal operations, while any associated vulnerabilities could introduce delays or prevent full recovery, thereby increasing the severity of the compromise. In an IT environment, for example, a fully equipped and tested hot site might allow almost immediate resumption of full services following a disruption, so the impact on the severity of the outcome would be considered Low. Conversely, a complete lack of backup data might prevent any meaningful recovery, so the impact of this vulnerability on the severity of compromise would be rated High.
- **Relevant Asset Attributes.** Once again, some vulnerabilities associated with detection, response and recovery mechanisms are related to certain attributes of assets or their environment. Complexity is a particular concern because it may be more difficult to detect the compromise of complicated equipment and IT systems. For example, recognizing even accidental errors amongst the millions of lines of code in a typical operating system is an exceptionally daunting challenge. Appropriate response and recovery measures may be more difficult to assess and take longer to implement so the resulting injuries may be harder to contain while the restoration of normal

services may be equally problematic. Depending upon the degree of complexity, the impact on the severity of the compromise may range from Low to High. The effects of fragility, or any other inadequacies related to structural integrity, may be hard to control and, in the worst case scenario, they may permit such extensive damage that any realistic recovery is rendered almost impossible.

- **Employee Awareness/Training.** With inadequate training and awareness, even conscientious employees are less likely to recognize and respond to threat events, so the injury arising from a compromise is likely to increase. When provided adequate training, well-informed personnel will notice many problems and take appropriate action to limit the damage and expedite an early recovery.

5.3.3 Impact on Severity of Outcome

For each vulnerability exposing assets within the scope of the assessment, determine the impact on the severity of the compromise based upon the relative effectiveness of associated detection, response and recovery mechanisms, the potential effects of adverse asset attributes, or the extent of employee awareness and training. Assign a level of Low, Medium or High from Table D-3, the Vulnerability Impact on Detection, Response and Recovery, or Not Applicable if the vulnerability relates only to prevention measures.

Safeguard Effectiveness	Associated Vulnerabilities	Severity of Outcome
No Safeguard Safeguards Largely Ineffective Assets Exposed to Extensive Injury	Unlikely to Detect Compromise Damage Difficult to Contain Prolonged Recovery Times/Poor Service Levels Assets Very Complex/Fragile Employees Ill-Informed/Poorly Trained	High
Safeguard Moderately Effective Assets Exposed to Moderate Injury	Compromise Probably Detected Over Time Damage Partially Contained Moderate Recovery Times/Service Levels Assets Fairly Complex/Fragile Moderate Employee Awareness/Training	Medium
Safeguard Very Effective Assets Exposed to Limited Injury (Safeguard Performs Only a Prevention Function)	Compromise Almost Certainly Detected Quickly Damage Tightly Contained Quick and Complete Recovery Assets Very Simple/Robust Employees Well-Informed/Trained	Low (Not Applicable)

Table D-3: Vulnerability Impact on Severity of Outcome (Detection, Response or Recovery)

6 Vulnerability Assessment

6.1 Vulnerability Levels

6.1.1 Basic Vulnerability Assessment

Once the impact of a vulnerability on the probability of compromise and the severity of the outcome have been determined based upon Tables D-2 and D-3 respectively, the two values may be entered in Table D-4 to establish an overall rating, from Very Low to Very High, for each vulnerability that exposes assets within the scope of the assessment to threats identified during the Threat Assessment Phase.

Impact on Severity of Outcome (Detection, Response & Recovery)	Impact on Probability of Compromise (Prevention)		
	Low (N/A)	**Medium**	**High**
High	Medium	High	Very High
Medium	Low	Medium	High
Low (N/A)	Very Low	Low	Medium

Table D-4: Basic Vulnerability Assessment

6.1.2 Related Vulnerabilities

Unfortunately, there are some fundamental limitations with the Basic Vulnerability Assessment. A single weakness that affects both the probability of compromise and the severity of outcome might be assigned any one of the five levels depending upon its actual or anticipated impacts, but inadequacies related to a single safeguard function (prevention, or detection, response and recovery), no matter how severe their effects in that one dimension would be capped at the Medium level in Table D-4. In some cases, this is not a serious concern because, for example, strong detection, response and recovery mechanisms can frequently offset inadequate or ineffective preventive measures. Similarly, less satisfactory detection, response and recovery safeguards may be fully acceptable in situations where the related preventive measures are particularly effective. The real problem arises when there are different but complementary weaknesses related to both prevention, and detection, response and recovery. Since this is frequently the case, the Basic Vulnerability Assessment should be extended to examine the cascading effects of related vulnerabilities.

6.1.3 Extended Vulnerability Assessment

To address this important phenomenon, an Extended Vulnerability Assessment should be applied to all vulnerabilities that are rated Not Applicable for either prevention, or detection, response and recovery. In each case, any related vulnerabilities affecting the Not Applicable dimension, either the impact on probability of compromise or severity of the outcome, should be identified to calculate their combined impact as follows:

- **Simple Scenario.** Frequently, one of the related vulnerabilities will affect only the probability of compromise (weak prevention) and the other only the severity of the

outcome (weak detection, response and recovery). The Extended Vulnerability Assessment is simply calculated by entering the two values in Table D-4.

- **Compound Scenario.** On occasion, this simple process may be complicated when the related vulnerability affects both the probability of compromise and the severity of the outcome, giving two ratings for one of these values, one for each of the related vulnerabilities. Where the ratings are the same (either Low, Medium or High), calculation of their combined impact is essentially the same as the simple scenario noted above. Should the two values differ, however, one should be selected for the Extended Vulnerability Assessment based on the following rationale –
  - if the more serious vulnerability is offset by the more effective safeguard with the lower vulnerability rating, use the lower value, and
  - if the more serious vulnerability undermines the effectiveness of the less vulnerable safeguard, use the higher value.

6.1.4 Sample Assessment

Two concrete examples serve to illustrate the Extended Vulnerability Assessment:

- **Simple Scenario.** An inexpensive lockset on the door to a warehouse will do little to prevent unauthorized access and theft. On the other hand, it has no direct bearing on the severity of the outcome because the lock does not perform a detection, response or recovery function. Therefore, according to the Basic Vulnerability Assessment, this weakness would warrant only a Medium rating. If at the same time there were neither guards nor intrusion alarms to detect unauthorized entry, the absence of any detection mechanism would be rated High for its impact on the severity of the outcome, but it still achieves only a Medium level on Table D-4. Considering the two together, however, and re-applying the Basic Vulnerability Assessment in Table D-4 generates a Very High result overall, a much more realistic conclusion.
- **Compound Scenario.** If the warehouse with ineffective locks (as noted above, a Medium vulnerability according to the Basic Vulnerability Assessment) were provided with a well-trained security guard, the related vulnerability might be assessed as Low, if the guard provided moderately effective prevention and a very effective detection and response capabilities. Faced with two different values for the impact on the probability of compromise (High for the lockset and Medium for the guard), one must be selected for the Extended Vulnerability Assessment. If the weak lock is unlikely to affect the guard's ability to perform a moderately effective prevention function, the lower rating for the impact on the probability of compromise (Medium) should be employed. If the lock might be exploited, however, to avoid intervention by the guard, thereby undermining his or her effectiveness, the higher rating for impact on the probability of compromise (High) should be used. Thus, the Extended Vulnerability Assessment would be either Low or Medium for the related vulnerabilities, depending upon their most likely interaction.

6.2 Practical Application

6.2.1 General

In order to apply the Extended Vulnerability Assessment and facilitate the computation of residual risk during the second segment of the Risk Assessment Phase of a TRA project, it is necessary to determine which assets and asset values are affected by each vulnerability, and which threats are facilitated.

6.2.2 Assets Affected

Some vulnerabilities have far-reaching effects on many different assets and asset values, while the impacts of others are more tightly constrained. For instance, weak security policies and procedures can expose virtually all assets and asset values to compromise, whereas unapproved shredders for the destruction of classified documents only facilitate unauthorized disclosure of sensitive information, a confidentiality rather than an availability or integrity concern. Establishing explicit linkages between vulnerabilities and the assets they expose, generally at the group or subgroup levels, is an important aspect of the Vulnerability Assessment that serves three analytical purposes:

- firstly, to limit the scope of the TRA project and concentrate on the greater risks, in other words the more serious vulnerabilities affecting more valuable assets;
- secondly, to determine whether an Extended Vulnerability Assessment is warranted in accordance with section 6.1.3 above for related inadequacies affecting the same assets; and
- thirdly, to organize data regarding the three risk variables (asset values, threats and vulnerabilities) in preparation for the computation of residual risk.

6.2.3 Threats Facilitated

In a similar vein, some vulnerabilities facilitate many different threats while others are exploited by relatively few. From a physical security perspective, for example, weak access controls would increase the probability of compromise by almost all deliberate threats and many accidents, with adverse consequences for confidentiality, availability and integrity. On the other hand, inadequate emanations security is unlikely to be exploited by anything other than a sophisticated intelligence service. Establishing potential connections between vulnerabilities and the associated threats offers comparable benefits for concentrating on the most significant risks, essentially those arising from the more serious threats interacting with the most severe vulnerabilities that expose the assets of greatest value.

6.2.4 Practical Cross-References

To ensure a structured and systematic approach to the identification of vulnerabilities and the associated assets and threats, some practical guidance may be found in:

- **Appendix D-2**, the **Vulnerability Listing**, which identifies the asset values exposed to compromise by each vulnerability;
- **Section 4.2 of Annex B**, the **Asset Identification and Valuation Phase**, which examines the asset values associated with different asset classes;

- **Section 2.6 of Annex C**, the **Threat Assessment Phase**, which provides some indication of the asset categories and asset values affected by each threat activity as well as the types of compromise.

6.3 Summary

The determination of vulnerability levels based upon their impact on the probability of compromise (inadequacies related to prevention measures) and the severity of the outcome (inadequacies related to detection, response or recovery mechanisms) is fundamental to the *Harmonized TRA Methodology* to establish common metrics and to permit comparative analysis. The five processes in the Vulnerability Assessment are listed with detailed instructions and examples in Appendix D-3.

7 Prioritized Vulnerability Assessment Table

As indicated above, all vulnerabilities exposing assets within the scope of an assessment to threats identified in the third phase of a TRA project must be assigned relative levels based upon their impact on the likelihood of compromise and the severity of the outcome. A single vulnerability may jeopardize one or more assets and facilitate one or more threats. This information should be recorded in the Vulnerability Assessment Table, the final output of the Vulnerability Assessment segment of the Risk Assessment Phase of a TRA project. Simply sorting by vulnerability levels, from Very Low to Very High, can quickly prioritize individual vulnerabilities and identify those of greatest significance.

This table is illustrated in Table D-5 and amplified in Appendix D-4.

Vulnerability Class	Vulnerability Group	Vulnerability	Related Vulnerabilities	Level	Asset(s) Exposed	Threat(s) Facilitated

Table D-5: Sample Vulnerability Assessment Table

Appendix D-1 - Sources of Vulnerability Data

Departmental Resources	
Data Source/Documentation	**Vulnerability Classes/Groups**
Program Managers • Business Plans • Standard Operating Procedures	• Security Program o Roles and Responsibilities o Human Resources o Financial Resources o Security Procedures • Sharing Information and Assets o Information • Contracting • Identification of Assets • Sanctions
Material/Asset Managers • Asset Inventories • Standard Operating Procedures	• Contracting • Physical Security o Secure Storage
Facility Managers • Floor Plans/Building Schematics • Guard Reports • Access Control Procedures • Emergency Plans • Incident Reports	• Sharing Information and Assets o Facilities • Protection of Employees o Management Response/Protective Measures • Physical Security o Perimeter Security o Access Controls o Facility Management
Human Resources • Incident Reports	• Protection of Employees
Finance • Standard Operating Procedures	• Access Limitations o Availability/Integrity/Separation of Duties
Chief Information Officer • Service Level Agreements • Asset Sharing Arrangements • IT Security Standards/Orders	• Sharing Information and Assets o IT Infrastructure • IT Security o Management Controls o (Some) Technical Safeguards o Operational Safeguards
Systems (Security) Administrator • System Schematics • Standard Operating Procedures • Security Test/Evaluation Reports • Incident Logs/Reports	• IT Security o (Some) Management Controls o Technical Safeguards o Operational Safeguards
Departmental Security Officer	• Security Program

Departmental Resources	
Data Source/Documentation	**Vulnerability Classes/Groups**
• Departmental Security Orders • Standard Operating Procedures • Security Inspection Reports • Investigation Reports	• Contracting • Security Awareness/Training • Identification of Assets • Security Risk Management • Security Screening • Protection of Employees • Physical Security • Security in Emergencies • Investigation of Incidents • Sanctions
IT Security Coordinator • Product Reviews/Evaluations • Incident Reports	• IT Security Incidents/Investigations
BCP Coordinator • Business Continuity Plans • BCP Exercise/Test Results	• Business Continuity Planning
Internal Audit/Review • Security Audits/Reviews	• Security Program (any management controls subject to audit or review)
Occupational Health and Safety • Standard Operating Procedures • Incident/Investigation Reports	• Protection of Employees o Incident Management

External Resources: Security Lead Departments	
Data Source/Documentation	**Types of Vulnerabilities**
Communications Security Establishment http://www.cse-cst.gc.ca/publications/publications-e.html • IT Security Guides • IT Security Alerts • IT Security Bulletins http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html • Product Evaluation Certification Reports	• IT Security Vulnerabilities
Public Safety and Emergency Preparedness Canada http://www.psepc-sppcc.gc.ca/prg/em/ccirc/anre-en.asp • Analytical Releases/Advisories	• IT Security Vulnerabilities
Royal Canadian Mounted Police http://www.rcmp.ca/tsb/home_e.htm • Security Guides/Reports	• Physical Security Vulnerabilities • IT Security Vulnerabilities

External Resources: Private Sector	
Data Source	**Types of Vulnerabilities**
CERT Vulnerability Notes Database http://www.kb.cert.org/vuls	• Technical Vulnerabilities
Common Criteria http://www.commoncriteriaportal.org/public/consumer	• Evaluated IT Security Products • Associated Vulnerabilities
SANS Critical Vulnerability Analysis Archive http://www.sans.org/newsletters/cva/index.php	• Technical Vulnerabilities
Product Vendors	• Technical Vulnerabilities

Notes:

1. The foregoing list of vulnerability sources is not complete. Other material will be added from time to time. Any suggestions for further references or contacts may be submitted to the offices identified in the Foreword.
2. The inclusion of any web site should not be construed as an endorsement. Similarly, the exclusion of other potentially useful sources is not a rejection. The list is merely intended to illustrate the wealth of information that is readily available to security practitioners and risk managers.

This page intentionally left blank.

Appendix D-2 - Vulnerability Listing

Vulnerability Class	Vulnerability Group	Specific Vulnerability	Impact			Values Affected		
			O_{Prob}	C_{Prob}	O_{Sev}	C	A	I
Security Program	Roles and Responsibilities	Executives		√	√	√	√	√
		Program Managers		√	√	√	√	√
		Project Managers		√	√	√	√	√
		Chief Information Officer		√	√	√	√	√
		Employees		√	√	√	√	√
		DSO		√	√	√	√	√
		IT Security Coordinator		√	√	√	√	√
		COMSEC Custodian		√	√	√	√	√
		BCP Coordinator		√	√		√	
	Human Resources	Effective Establishment		√	√	√	√	√
		Classification Levels		√	√	√	√	√
	Financial Resources	Departmental Operations		√	√	√	√	√
		Projects		√	√	√	√	√
	Security Policy/Procedures	Sharing Information/Assets		√	√	√	√	√
		Contracting		√	√	√	√	√
		Security Awareness/Training		√	√	√	√	√
		Identification of Assets		√	√	√	√	√
		Security Risk Management		√	√	√	√	√
		Access Limitations		√	√	√	√	√
		Security Screening		√	√	√	√	√
		Protection of Employees		√	√	√	√	√
		Physical Security		√	√	√	√	√
		IT Security		√	√	√	√	√
		Security in Emergencies		√	√	√	√	√
		Business Continuity Planning		√	√	√	√	√
		Security Program Audit		√	√	√	√	√
		Investigation of Incidents		√	√	√	√	√
		Sanctions		√	√	√	√	√
Sharing Information/Assets	Information	Arrangements		√	√	√	√	√
	Facilities	Arrangements		√	√	√	√	√
	IT Infrastructure	Arrangements		√	√	√	√	√
Security Outside Canada	Special Standards	TRAs by Location		√	√	√	√	√
	Travel Restrictions	By Location	√	√	√	√	√	√
Contracting	Roles and Responsibilities	Project/Technical Authority		√		√		
	SRCL			√		√		
	Facility Security Clearance	Personnel Assigned		√		√		
		Document Safeguarding		√		√		
	International Contracts			√		√		
Security Awareness/Training	Roles and Responsibilities	Training/Awareness Officer	√	√	√	√	√	√
	Security Training	Security Practitioners	√	√	√	√	√	√
	Security Awareness	Initial Briefings	√	√	√	√	√	√
		Regular Updates	√	√	√	√	√	√
Identification of Assets	Confidentiality	Categorization: Classified		√	√	√		

Vulnerability Class	Vulnerability Group	Specific Vulnerability	Impact			Values Affected		
			O_{Prob}	C_{Prob}	O_{Sev}	C	A	I
		Marking: Classified		√	√	√		
		Categorization: Protected		√	√	√		
		Marking: Protected		√	√	√		
	Availability	Categorization		√	√		√	
		Marking		√	√		√	
	Integrity	Categorization		√	√			√
		Marking		√	√			√
Security Risk Management	TRAs	Initial Assessment	√	√	√	√	√	√
		Continuous Monitoring	√	√	√	√	√	√
Access Limitations	Classified/Protected Assets	Need to Know		√	√	√		
		Security Screening		√	√	√	√	√
	Availability/Integrity	Separation of Duties	√	√	√	√	√	√
Security Screening	Reliability Status	Establishing Requirements		√		√	√	√
		Initial Screening		√		√	√	√
		Evaluating Results		√		√	√	√
		Regular Updating		√		√	√	√
		Review for Cause			√	√	√	√
		Revocation			√	√	√	√
		Release Procedures			√	√	√	√
	Security Clearance	Establishing Requirements		√		√		
		Initial Screening		√		√		
		Evaluating Results		√		√		
		Regular Updating		√		√		
		Review for Cause			√	√		
		Revocation/Downgrading			√	√		
		Release Procedures			√	√		
	Site Access Clearance	Establishing Requirements		√		√		
		Initial Screening		√		√		
		Evaluating Results		√		√		
		Regular Updating		√		√		
		Review for Cause			√	√		
		Revocation			√	√		
		Release Procedures			√	√		
Protection of Employees	Identify Employees at Risk	TRA		√	√	√		
	Management Response	Protective Measures		√	√	√		
		Support Mechanisms		√	√	√		
		Training and Counselling		√	√	√		
	Incident Management	Incident Reporting			√	√		
		Incident Investigation			√	√		
		Remedial Action			√	√		
Physical Security	Planning Factors	Building Codes		√	√	√	√	√
		Security Zones		√	√	√	√	√
	Site Selection	Easements Through Site	√				√	
		Emergency Lanes	√				√	
		Building Location/Topography	√				√	
		Emergency Services	√				√	
		Adjacent Occupants	√			√	√	
	Perimeter Security	Control of Site Perimeter		√	√	√	√	√

Vulnerability Class	Vulnerability Group	Specific Vulnerability	Impact			Values Affected		
			O_{Prob}	C_{Prob}	O_{Sev}	C	A	I
		Illumination of Site	√		√	√	√	√
		Exterior Signs	√			√	√	√
		Landscape Design		√	√	√	√	√
		Parking		√	√	√	√	√
	Entry Security	Pedestrian Entrances/Lobbies		√		√	√	√
		Service/Utility Openings		√		√	√	√
		Shipping/Receiving Areas		√		√	√	√
	Interior Security Planning	Circulation Routes		√	√		√	
		Elevator Lobbies		√	√		√	
		Daycare Centres		√	√		√	
		Conference Rooms/Boardrooms		√	√	√	√	
		Stairwells/Elevators		√	√		√	
		Washrooms		√	√		√	
		Amenity Spaces		√	√		√	
		Mailrooms		√	√	√	√	
		Telecommunications/Wiring		√	√	√	√	√
		HVAC Spaces		√	√		√	
		Server Rooms		√	√	√	√	√
	Access Controls	Identification Cards		√		√	√	√
		Electronic Access Controls		√		√	√	√
		Electronic Intrusion Detection			√	√	√	√
		Closed Circuit Video Equipment			√	√	√	√
		Security Control Centre		√	√	√	√	√
		Sensitive Discussion Areas		√		√		
		Secure Rooms		√		√	√	√
		Security Guards		√	√	√	√	√
	Facility Management	Leasing Contracts		√		√	√	√
		Maintenance Services		√		√	√	√
		Cleaning Services		√		√	√	√
		Interior Signs	√			√	√	√
		Locking Hardware/Key Control		√		√	√	√
		Renovation Work		√		√	√	√
		Facility Security Committee		√		√	√	√
	Secure Storage	Security Containers		√		√	√	√
		Keys/Combinations		√		√	√	√
		Maintenance of Containers		√		√	√	√
		Disposal of Containers		√		√	√	√
		Secure Rooms/Vaults		√		√	√	√
	Transport/Transmittal	Transport		√		√	√	√
		Transmittal		√		√	√	√
	Destruction	Storage Pending Disposal		√		√		
		Destruction Equipment: Paper		√		√		
		Destruction Equipment: IT Media		√		√		
		Equipment Marking		√		√		
		Equipment Maintenance		√		√		
		Contracted Services		√		√		
		Emergency Destruction		√		√		
IT Security	Management Controls	System Development Life Cycle		√	√	√	√	√

Vulnerability Class	Vulnerability Group	Specific Vulnerability	Impact			Values Affected		
			O_{Prob}	C_{Prob}	O_{Sev}	C	A	I
		IT Security Resources for Projects		√	√	√	√	√
		Certification and Accreditation		√	√	√	√	√
		Contracting		√	√	√	√	√
		Outsourcing		√	√	√	√	√
	Technical Safeguards	Evaluated Products		√	√	√	√	√
		Identification and Authentication		√		√	√	√
		Authorization/Access Control		√		√	√	√
		Cryptography		√		√		√
		Public Key Infrastructure (PKI)		√		√	√	√
		Perimeter Defence		√		√	√	√
		Mobile Computing/Telework		√		√	√	√
		Wireless Devices		√		√	√	√
		Emanations Security		√		√		
		Telecommunications Cabling		√		√	√	
		Software Integrity		√		√	√	√
		Software Security Configuration		√		√	√	√
		Malicious Code Protection		√	√		√	√
		Intrusion Detection			√	√	√	√
		Backup/Recovery			√		√	
	Operational Safeguards	Help Desk/Problem Resolution		√	√	√	√	√
		Incident Management		√	√	√	√	√
		Vulnerability Assessments		√		√	√	√
		Patch Management		√		√	√	√
		IT Continuity Planning			√	√	√	√
		IT Security Assessment/Audit		√	√	√	√	√
		Configuration Management		√		√	√	√
		Change Control		√		√	√	√
		Capacity Planning		√			√	
		Hardware Maintenance		√	√	√	√	√
		Environmental Protection			√		√	
		Power Conditioning/Backup			√		√	
Security in Emergencies	Plans and Procedures	Departmental Plans		√	√		√	
		Testing		√	√		√	
		Coordination with Other Plans		√	√		√	
		Resourcing for Sustainability		√	√		√	
Business Continuity Planning	Governance Structure	Authorities			√		√	
		Responsibilities			√		√	
	Business Impact Analysis				√		√	
	Plans/Arrangements				√		√	
	BCP Program Readiness				√		√	
	Review, Testing and Audit				√		√	
Investigation of Incidents	Incident Investigation			√	√	√	√	√
	Incident Reporting			√	√	√	√	√
Sanctions	Security Violations		√			√	√	√
	Security Breaches		√			√	√	√

Notes:

1. The primary effect(s) of vulnerabilities related to inadequacies associated with any given safeguard are indicated in the foregoing table under Impact as:
    - **O_{Prob}** – an increase in the likelihood that a threat event will actually occur, usually arising from weak deterrence or avoidance mechanisms;
    - **C_{Prob}** – an increase in the probability of compromise should a threat event actually materialize, generally attributed to inadequate prevention measures; and
    - **O_{Sev}** – an increase in the severity of the outcome of a threat event due to ineffective detection, response or recovery measures.
2. The asset values most likely to be affected are identified in the last three columns with the abbreviations: C (confidentiality); A (availability); and I (integrity).
3. This listing is not an absolute arbiter of impacts or asset values affected, but rather a general indicator to facilitate analysis during the Vulnerability Assessment.

This page intentionally left blank.

Appendix D-3 - Vulnerability Metrics

1 Instructions

For each vulnerability exposing assets to threats within the scope of the TRA project, determine the appropriate levels as follows:

- **Step 1.** Identify all existing and, in the case of a project environment, proposed safeguards that protect assets within the scope of the assessment using the Safeguard Listing in Appendix F-2 as a guide.
- **Step 2.** Determine the security functions (avoidance, deterrence, prevention, detection, response and recovery) performed by each safeguard.
- **Step 3.** Identify potential vulnerabilities associated with each safeguard that has been, will be or should have been implemented in accordance with baseline security standards using the Vulnerability Listing in Appendix D-2 as a guide.
- **Step 4a.** Assess the impact of each vulnerability on the probability of compromise, ranging from Low to High, or Not Applicable if it does not perform a prevention function, in accordance with Table D3-1 below.

Safeguard Effectiveness	Associated Vulnerabilities	Probability of Compromise
No Safeguards Safeguards Largely Ineffective Probability of Compromise > 75%	Easily Exploited Needs Little Knowledge/Skill/Resources Assets Highly Accessible Assets Very Complex/Fragile/Portable/ Employees Ill-Informed/Poorly Trained	High
Safeguards Moderately Effective Probability of Compromise 25-75%	Not Easily Exploited Needs Some Knowledge/Skill/Resources Assets Moderately Accessible Assets Fairly Complex/Fragile/Portable Moderate Employee Awareness/Training	Medium
Safeguards Very Effective Probability of Compromise < 25% (Safeguard Performs Only Detection, Response or Recovery Functions)	Difficult to Exploit Needs Extensive Knowledge/Skill/Resources Access to Assets Tightly Controlled Assets Very Simple/Robust/Static Employees Well-Informed/Trained	Low (Not Applicable)

Table D3-1: Vulnerability Impact on Probability of Compromise (Prevention)

- **Step 4b.** Assess the impact of each vulnerability on the severity of the outcome, ranging from Low to High, or Not Applicable if it does not perform a detection, response or recovery function, in accordance with Table D3-2 below.

Safeguard Effectiveness	Associated Vulnerabilities	Severity of Outcome
No Safeguards Safeguards Largely Ineffective Assets Exposed to Extensive Injury	Unlikely to Detect Compromise Damage Difficult to Contain Prolonged Recovery Times/Poor Service Levels Assets Very Complex/Fragile Employees Ill-Informed/Poorly Trained	High
Safeguards Moderately Effective Assets Exposed to Moderate Injury	Compromise Probably Detected Over Time Damage Partially Contained Moderate Recovery Times/Service Levels Assets Fairly Complex/Fragile Moderate Employee Awareness/Training	Medium
Safeguards Very Effective Assets Exposed to Limited Injury (Safeguard Performs Only a Prevention Function)	Compromise Almost Certainly Detected Quickly Damage Tightly Contained Quick and Complete Recovery Assets Very Simple/Robust Employees Well-Informed/Trained	Low (Not Applicable)

Table D3-2: Vulnerability Impact on Severity of the Outcome (Detection, Response or Recovery)

- **Step 5a.** Determine level of each vulnerability from Very Low to Very High by correlating its impact on the probability of compromise in the horizontal axis with the impact on outcome severity in the vertical axis of Table D-3, the Basic Vulnerability Assessment.

Impact on Severity of Outcome (Detection, Response & Recovery)	Impact on Probability of Compromise (Prevention)		
	Low (N/A)	**Medium**	**High**
High	Medium	High	Very High
Medium	Low	Medium	High
Low (N/A)	Very Low	Low	Medium

Table D3-3: Basic Vulnerability Assessment

- **Step 5b.** For vulnerabilities rated Low, Medium or High in Step 5a, apply the Extended Vulnerability Assessment as follows:
  - for vulnerabilities rated Low, Medium or Not Applicable for their impact on the probability of compromise, determine whether any related vulnerabilities regarding weak prevention measures are rated Medium or High;
  - if a related vulnerability has a higher impact on the probability of compromise, recalculate the overall vulnerability in Table D3-3 using the higher values;

  - for vulnerabilities rated Low, Medium or Not Applicable for their impact on the severity of the outcome, determine whether any related vulnerabilities regarding weak detection, response and recovery measures are rated Medium or High; and
  - if a related vulnerability has a higher impact on the severity of the outcome, recalculate the overall vulnerability in Table D3-3 using the higher values.
- **Step 5c.** Determine which assets identified during the Asset Identification and Valuation Phase of the TRA project (Annex B) are exposed and which threats identified during the Threat Assessment Phase (Annex C) are facilitated by each vulnerability, or pair of related vulnerabilities in the case of the Extended Vulnerability Assessment.
- **Step 5d.** Whenever doubts remain regarding the actual vulnerability level, both the high and low values may be entered in the Vulnerability Assessment and used for the calculation of residual risk during the Risk Assessment Phase to determine if this uncertainty has any impact on the assessed residual risk.
- **Step 5e.** Vulnerabilities that fall close to the threshold between two levels should be flagged for subsequent analysis during the Risk Assessment Phase of the TRA project, using arrows (↑↓) to indicate whether they fall near the high or low end of the range. For example, if a compromise were likely to be detected in 24 to 48 hours, in the severity of the outcome might be rated Low, but at the higher end of the range, near Medium, so the entry in the Vulnerability Assessment Table should be marked (↑) accordingly.
- **Step 6.** Enter the results under the appropriate columns in the Vulnerability Assessment Table at Appendix D-4.

2 Examples

2.1 Poor Perimeter Lighting

The analytical processes outlined above might be applied as follows to determine the vulnerability levels associated with inadequate perimeter lighting:

- **Safeguard Identification.** Section 7.3.6 of the *Operational Security Standard on Physical Security* states in part "Lighting should provide sufficient illumination in and around facilities to allow the detection and observation of people approaching the facility". This baseline security requirement is amplified in *RCMP Guide G1-002, Security Lighting*.
- **Security Functions.** As indicated in the operational security standard, proper illumination might discourage certain types of deliberate attacks, such as theft or vandalism, thereby decreasing the likelihood of a threat event. This deterrent effect could be factored into the Threat Assessment Phase of a TRA project, in accordance with section 5.1 of Annex D. For purposes of the Vulnerability Assessment, however, it is necessary to determine whether perimeter lighting performs prevention, detection, response or recovery functions. In this regard, lights by themselves cannot stop anything, so they are not a prevention measure. On the other hand, it is much easier to detect an intruder in a well-lit space. Therefore, perimeter lighting is an important detection mechanism to initiate a response that might help to contain the injury or reduce the severity of the outcome in the event of a compromise.

- **Associated Vulnerabilities.** Inadequate security lighting, the relevant vulnerability, would have the opposite effect, increasing the amount of damage that might be expected by allowing threat agents to continue their unauthorized activities without interruption.
- **Vulnerability Impact on Probability of Compromise (Prevention).** Since perimeter lighting is not a preventive measure, any associated weaknesses will have no impact on the probability of compromise. Hence, this vulnerability should be assigned a Low or, more precisely, N/A level in Table D3-1, Vulnerability Impact on Prevention.
- **Vulnerability Impact on Severity of the Outcome (Detection, Response and Recovery).** If there were absolutely no lights or they were very dull and dirty, the impact on outcome severity might be rated High in accordance with Table D3-2, Vulnerability Impact on Detection, Response or Recovery. Low intensity lights that offer some illumination and, therefore, moderate prospects for detecting anyone loitering in the area might warrant a Medium rating, whereas high intensity mercury-vapour lamps situated at regular intervals around the entire perimeter might increase the probability of detection significantly and, therefore, reduce the impact on outcome severity to a Low level.
- **Basic Vulnerability Assessment.** With a Low or N/A impact on the probability of compromise the Basic Vulnerability Assessment level would be selected from the first column in Table D3-3, with a result of Very Low, Low or Medium depending upon the impact on outcome severity determined in the previous step.
- **Extended Vulnerability Assessment.** The impact on the probability of compromise is rated N/A, so Extended Vulnerability Assessment procedures should be invoked to determine if there are related vulnerabilities due to inadequate prevention measures, such as poor access controls, unprotected glass windows or unapproved locks on exterior doors. If any of these weaknesses were rated Medium or High for their impact on the probability of compromise, the extended vulnerability might be rated High or Very High.
- **Assets Exposed/Threats Facilitated.** Depending upon the scope of the TRA project, inadequate perimeter lighting might expose any number of assets to increased risk. Some of the more obvious examples include any employees frequenting the area and the contents of the facility. The threats that might exploit poor lighting conditions range from vandals spraying graffiti on exterior walls to burglars targeting equipment or supplies, and even predators stalking pedestrian traffic.

2.2 Outdated Malicious Code Protection

The vulnerability levels associated with outdated anti-virus software may be determined following the same procedures.

- **Safeguard Identification.** Section 16.4.12 of the *Operational Security Standard: Management of Information Technology Security (MITS)* states in part "Departments must install, use and regularly update antivirus software and conduct malicious code scans on all electronic files from external systems."
- **Security Functions.** While the capabilities and features of anti-virus software vary considerably, most products perform two or more security functions: early identification of malicious code before it can execute is actually a prevention measure, whereas the

recognition of suspicious activities or behavioural patterns is a true detection mechanism that may initiate a response to shut down the infected machine or block further infection.

- **Associated Vulnerabilities.** Anti-virus software must be updated regularly; otherwise it may not recognize and respond to newer threats, potentially serious vulnerabilities which could increase both the probability of compromise and the severity of the outcome.
- **Vulnerability Impact on Probability of Compromise (Prevention).** If the software were updated automatically in real time, the safeguard should be very effective and the impact on the likelihood of compromise would be Low. If several days or weeks were to elapse between upgrades, the likelihood of preventing an infection would decrease significantly, so the impact might be rated Medium. If the software were never renewed or perhaps improperly installed in the first place, the effects on the probability of compromise would be High.
- **Vulnerability Impact on Severity of the Outcome (Detection, Response and Recovery).** Outdated anti-virus software is also less likely to detect and respond to newer viruses and worms, so the impact on the severity of the outcome will increase over time from Low for the current release to High for truly obsolete versions.
- **Basic Vulnerability Assessment.** Depending upon the ratings assigned to the two dimensions of vulnerability (probability of compromise and severity of the outcome), the Basic Vulnerability Assessment might range from Very Low for very robust fully current software to Very High for badly outdated versions.
- **Extended Vulnerability Assessment.** In this case, the Enhance Vulnerability Assessment would only be applied if inadequacies related to older malicious code protection measures affects were rated Low or Medium for either prevention (probability of compromise) or detection and response (severity of the outcome).
- **Assets Affected/Threats Facilitated.** In this case, the vulnerabilities arising from inadequate malicious code protection tend to expose a smaller subset of assets to increased risk, specifically any electronic files on the system and those services that rely upon them. Quite clearly, the primary threat related to this vulnerability is sabotage by hackers, whether individuals, groups or state-sponsored organizations.

This page intentionally left blank.

Appendix D-4 - Vulnerability Assessment Table

Vulnerability Class	Vulnerability Group	Vulnerability	Related Vulnerabilities	Level	Asset(s) Exposed	Threat(s) Facilitated
Security Program						
Sharing Information/Assets						
Security Outside Canada						
Contracting						
Security Awareness/Training						
Identification of Assets						
Security Risk Management						
Access Limitations						
Security Screening						
Protection of Employees						
Physical Security						
IT Security						
Security in Emergencies						
Business Continuity Planning						
Investigation of Incidents						
Sanctions						

1 Instructions

Enter all vulnerabilities that expose assets within the scope of the TRA project to threats identified during the Threat Assessment Phase, using the Vulnerability Listing in Appendix D-2 as a guide.

Based upon the Vulnerability Metrics in Appendix D-3, determine the relevant levels for each ranging from Very Low through Very High (VL through VH) using either the Basic or Extended Vulnerability Assessment as appropriate.

Identify both the assets exposed by these vulnerabilities and the threats they facilitate.

2 Examples

The two examples explored in Appendix D-3, poor perimeter lighting and outdated malicious code detection, would generate the following entries:

Vulnerability Class	Vulnerability Group	Vulnerability	Related Vulnerabilities	Level	Asset(s) Exposed	Threat(s) Facilitated
Physical Security	Perimeter Security	Poor Perimeter Lighting	Weak Access Controls	H[1]	Employees Building Exterior	Stalkers Vandals
			Unprotected Windows	VH[2]	Building Content	Burglars
IT Security	Technical Safeguards	Outdated Anti-Virus Software	N/A	M[3]	Electronic Files Related Services	Hackers

[1] Assuming that the perimeter lighting were particularly bad or non-existent as a detection mechanism and, therefore, rated High for its impact on severity of the outcome, while the perimeter access controls were deemed moderately effective as a preventive measure and warranted a rating of Medium for their impact on the probability of compromise.

[2] Again assuming that the perimeter lighting were particularly bad or non-existent as a detection mechanism and, therefore, rated High for its impact on severity of the outcome, while the glass windows in the building were totally unprotected and, as a weak preventive measure, warranted a rating of High for their impact on the probability of compromise.

[3] Assuming that the anti-virus software were updated every few weeks rather than daily or, better still, in real time, so both the impact on the probability of compromise and the severity of the outcome would merit a medium rating which would generate an overall Medium level on the Basic Vulnerability Assessment table.

Annex E - Calculation of Residual Risks

1 Introduction

1.1 General

The second segment of the Risk Assessment Phase of a TRA project is the Calculation of Residual Risk which comprises a single process and one major output as follows:

- **Computation of Residual Risk** – to determine residual risk levels ranging from Very Low to Very High based upon the value of assets identified within the scope of the assessment, the associated threats that might compromise these assets, employees and services, and any related vulnerabilities; and
- **Prioritized List of Residual Risks** – to produce a comprehensive list of residual risks which may be ranked from the most serious to the least.

1.2 Aim

The aim of this annex is to describe the one process and single output of the Calculation of Residual Risk segment of the Risk Assessment Phase of a TRA project.

2 Computation of Residual Risk

2.1 General

Upon completion of the Asset Identification and Valuation Phase, the Threat Assessment Phase and the Vulnerability Assessment segment of the Risk Assessment Phase of a TRA project, the three risk variables (asset values, threats and vulnerabilities) have been assigned appropriate levels ranging from Very Low to Very High. Now, in the second segment of the Risk Assessment Phase, the three factors may be combined to identify and prioritize any residual risks, namely those that remain after the proposed and approved safeguards have been fully implemented.

Residual Risk (*Risque résiduel*) - The risk that remains after safeguards have been selected, approved and implemented.

New Definition.

2.2 Basic Risk Calculation

At this stage in a TRA project, all assets within the scope of the assessment have been identified and assigned values based upon the injuries that could reasonably be expected to arise in case of a compromise to their confidentiality, availability or integrity. The associated threats that might affect them have been rated according to the likelihood of occurrence and the potential gravity of

the results. Related vulnerabilities that might expose assets to harm have been assigned relative levels based on their impact on the likelihood of compromise and the severity of the outcome. As part of the analysis, each of the three variables has been assigned a level from Very Low to Very High. Now, to determine the residual risk arising from a threat exploiting a related vulnerability to compromise an asset, each of the three factors should be assigned a numeric score from one to five in accordance with Table E-1 below.

Asset Value, Threat and Vulnerability Levels	Very Low	Low	Medium	High	Very High
Scores for Risk Computation	1	2	3	4	5

Table E-1: Numeric Scores for Asset Value, Threat and Vulnerability Levels

As illustrated in Figure E-1, the assessed residual risks are calculated as the product of the three variables for each combination of asset, associated threat and related vulnerability taken from the Vulnerability Assessment Table presented in Table D-5 and amplified in Appendix D-4.

$$\text{Residual Risk} = \text{Asset Value} \times \text{Threat} \times \text{Vulnerability}$$

Figure E-1: Calculation of Residual Risk

Given numeric scores from one to five for each variable, the final results for residual risk may range from one to 125.

2.3 Risk Levels

Although the raw scores are immediately useful to prioritize residual risks, it is often helpful to group similar results in graduated levels ranging from Very Low to Very High. The thresholds between the Medium, High and Very High levels reflected in Table E-2 were selected with the underlying premise that where two of the three variables fall at one level, such as Medium, and the third in the next higher category, in this case High, it seems prudent to adopt the higher rating overall. The boundaries between Very Low, Low and Medium were adjusted upward slightly to achieve a more uniform distribution of results. As indicated in Table E-2, the Medium range encompasses the largest single grouping, with 43 possible combinations, while somewhat fewer fall in the High and Low ranges, and fewer still at the Very High and Very Low extremes. Finally, Tables E1-3 through E1-7 provide a complete breakdown of all possible results for every different combination of asset value, threat and vulnerability.

Basic Risk Score	1-4	5-12	15-32	36-75	80-125
Risk Level	Very Low	Low	Medium	High	Very High
Number of Outcomes in Range	13	34	43	28	7

Table E-2: Risk Levels and Ranges

2.4 Practical Application

2.4.1 General

To achieve more realistic results, the straightforward calculation of residual risk as the product of three variables (asset value, threat and vulnerability) must be tempered with some practical considerations under certain circumstances.

2.4.2. Borderline Values

In cases where two or more variables fall at either the high or low end of the range for their assessed values, it is generally prudent to raise or lower the level of one factor to better reflect the actual risk. To provide a concrete example, if an asset value were determined to be Medium based on an expected financial loss of $9.8 million in the event of compromise, the estimated injury lies very near the threshold between Medium and High asset values and should have been flagged (↑) accordingly in accordance with the instructions in Appendix B-4, the Expanded Injury Table. If either an associated threat or related vulnerability, or both, were also assessed to lie at the high end of the spectrum, on the borderline between two levels, then one of the three variables, normally the lowest, should be elevated one level for the purposes of calculating residual risk and annotated accordingly in the final Risk Assessment.

2.4.3 Uncertain Values

In a few cases, despite the best efforts of TRA team members to achieve consensus on realistic levels for asset values, threats and vulnerabilities, some legitimate disagreements can arise. In other situations, especially with respect to threats and vulnerabilities, the appropriate levels may be doubtful due to incomplete or contradictory evidence. Rather than force the assessment to a single unique solution, it is generally preferable to compute the residual risk using both of the disputed values. For example, based on current intelligence, it may not be entirely clear whether a deliberate threat agent possesses extensive or merely moderate knowledge, skill and resources and should, therefore, fall in the High or Medium range for threat agent capability and, therefore, impact or gravity. Given this uncertainty, two values should be computed for the assessed residual risk using the higher and lower threat levels.

2.4.4 Deliberate Threats

The likelihood of many threats, especially accidents and natural hazards, remain relatively constant, at least in the short run. Of course, changes can take place, but they generally come about quite gradually. For example, the probability of certain natural hazards, such as hurricanes, has increased significantly in the past fifty years due, in part, to global warming. Since most TRA projects are updated periodically, long-term variations of this nature are

unlikely to affect the findings for the duration of any given TRA report. Conversely, the likelihood of many deliberate threats can be far more volatile because threat agent intentions may change very quickly, literally overnight. To date, cases of extortion to recover encrypted data files have occurred quite regularly in some parts of the world, but they are almost unheard of in Canada. Thus, the likelihood of the threat would be rated as Low or Medium during Threat Assessment Phase in accordance with Table C-1. Should past intentions change, however, the probability and the overall threat might increase quickly, without warning, before suitable safeguards could be implemented. Therefore, when the intentions of a deliberate threat agent are rated as Low or Medium, it is only prudent to calculate two residual risks, one based on current intentions and capabilities and a second higher level based upon a High likelihood. If the two risk levels vary significantly, the difference may be noted during the Recommendation Phase of the TRA project to justify additional safeguards before the change occurs.

3 Prioritized List of Assessed Residual Risks

As indicated above, residual risks may be calculated based upon the three constituent elements, namely asset values, the associated threats and related vulnerabilities. Since one threat may affect several different assets and asset values, and one vulnerability may expose many assets to varied threats, the List of Residual Risks can become very long indeed for even a tightly focused TRA project. Therefore, to achieve more manageable results, assets and threats in particular should be rolled up wherever possible to the Group or Subgroup and Activity of Threat Agent Category levels respectively. This information should be recorded in the List of Residual Risks, the final output of the Calculation of Residual Risk segment of the Risk Assessment Phase of a TRA project. Simply sorting by assessed residual risk levels, from Very Low to Very High, or raw scores, from one to 125, can quickly prioritize individual risks and identify those of greatest concern.

This List of Assessed Residual Risks is illustrated in Table E-3 and amplified in Appendix E-2.

Asset (Group/Subgroup)	Asset Values			Associated Threat (Activity/Agent Category)	T	Related Vulnerability	V	Residual Risk ($A_{Val} \times T \times V$)	R
	C	A	I						

Table E-3: List of Assessed Residual Risks

Appendix E-1 - Residual Risk Tables

1 Instructions

Upon completion of the Asset Identification and Valuation Phase, the Threat Assessment Phase and the Vulnerability Assessment segment of the Risk Assessment Phase of a TRA project, residual risks may be calculated and assigned appropriate levels as follows:

- **Step 1a.** For all assets within the scope of the assessment, convert the values from Very Low to Very High captured in Appendix B-5, the Asset Valuation Table or Statement of Sensitivity, to a raw score of one to five in accordance with Table E1-1 below and enter the results in the relevant columns of the List of Assessed Residual Risks, Appendix E-2.
- **Step 1b.** If the assigned asset values fall near the boundary between two levels, flag the entries accordingly, either ↑ or ↓ to indicate their position in the high or low range of the spectrum respectively.
- **Step 2a.** For all threats associated with each asset, convert the levels from Very Low to Very High recorded in Appendix C-4, the Threat Assessment Table, to a raw score of one to five in accordance with Table E1-1 below and enter the results in the relevant columns of the List of Assessed Residual Risks, Appendix E-2.
- **Step 2b.** Where the assessed threats lie near a boundary between two levels, flag the entries accordingly, either ↑ or ↓ to indicate their position in the high or low range of the spectrum respectively.
- **Step 2c.** Where there is contradictory evidence regarding threat levels, record both the high and low values in separate lines.
- **Step 2d.** For deliberate threats with a Low or Medium likelihood of occurrence, consider the potential impact of changing threat agent intentions by re-computing the overall threat level with Table C-3, the Threat Levels Table, using a High rather than Low of Medium likelihood, and record the result as a second entry.
- **Step 3a.** For all vulnerabilities that expose assets to threats, convert the levels from Very Low to Very High recorded in Appendix D-4, the Vulnerability Assessment Table, to a raw score of one to five in accordance with Table E1-1 below and enter the results in the relevant columns of the List of Residual Risks, Appendix E-2.
- **Step 3b.** For vulnerabilities sitting near a boundary between two levels, flag the entries with either ↑ or ↓ to show their position near the higher or lower threshold respectively.
- **Step 3c.** In cases where some doubt exists regarding vulnerability levels, record both the high and low values in separate lines.

Asset Value, Threat and Vulnerability Levels	Very Low	Low	Medium	High	Very High
Scores for Risk Computation	1	2	3	4	5

Table E1-1: Numeric Scores for Asset Value, Threat and Vulnerability Levels

- **Step 4a.** Having recorded all assets, the associated threats and related vulnerabilities in Appendix E-2, the List of Assessed Residual Risks, along with the numeric scores derived from their levels, the product of the three variables may be computed and entered as either a raw score from one to 125 or the appropriate risk level from Table E1-2 below.
- **Step 4b.** If two or three of the risk factors fall in either the high or low range of their assessed levels, increase or decrease the raw score of the lowest rated variable by one level before computing the residual risk. This step may be omitted when one or two of the variables sit at one end of the spectrum and another lies at the opposite end, thereby offsetting each other.

Basic Risk Score	1-4	5-12	15-32	36-75	80-125
Risk Level	Very Low	Low	Medium	High	Very High
Number of Outcomes in Range	13	34	43	28	7

Table E1-2: Risk Levels and Ranges

2 Expanded Risk Assessment Tables

Tables E1-3 to E1-7 provide a break-out of all possible outcomes for the calculation of assessed residual risk. Simply select the table for the assigned asset value, and determine the residual risk by correlating the associated threat level on the horizontal axis with the related vulnerability level on the vertical.

Vulnerability Level	**Threat Level**				
	Very Low	Low	Medium	High	Very High
Very Low	VL	VL	VL	VL	L
Low	VL	VL	L	L	L
Medium	VL	L	L	L	M
High	VL	L	L	M	M
Very High	L	L	M	M	M

Table E1-3: Risk Table for Very Low Asset Values

Vulnerability Level	Threat Level				
	Very Low	Low	Medium	High	Very High
Very Low	VL	VL	L	L	L
Low	VL	L	L	M	M
Medium	L	L	M	M	M
High	L	M	M	M	H
Very High	L	M	M	H	H

Table E1-4: Risk Table for Low Asset Values

Vulnerability Level	Threat Level				
	Very Low	Low	Medium	High	Very High
Very Low	VL	L	L	L	M
Low	L	L	M	M	M
Medium	L	M	M	H	H
High	L	M	H	H	H
Very High	M	M	H	H	H

Table E1-5: Risk Table for Medium Asset Values

Vulnerability Level	Threat Level				
	Very Low	Low	Medium	High	Very High
Very Low	VL	L	L	M	M
Low	L	M	M	M	H
Medium	L	M	H	H	H
High	M	M	H	H	VH
Very High	M	H	H	VH	VH

Table E1-6: Risk Table for High Asset Values

Vulnerability Level	Threat Level				
	Very Low	Low	Medium	High	Very High
Very Low	L	L	M	M	M
Low	L	M	M	H	H
Medium	M	M	H	H	H
High	M	H	H	VH	VH
Very High	M	H	H	VH	VH

Table E1-7: Risk Table for Very High Asset Values

3 Example

3.1 Regional Medical Storage Facility

If $12 million worth of morphine were stored in a regional medical storage facility, the risk variables might be determined as follows to compute the assessed residual risk:

- **Asset Valuation.** The primary asset value in this case should reflect the injury that could reasonably be expected if the drugs were lost or stolen, an availability concern. The psychological impact of an accidental loss might be quite modest, but the theft of drugs from a public facility is far more likely to cause serious doubts and uncertainty in the community at large, probably a Medium Asset value in accordance with the Extended Injury Table in Appendix B-4. If the morphine were unavailable for any reason, the physical impact on some patients could be quite devastating, causing serious physical hardship for at least some if not many patients, certainly a Medium and quite probably a High asset value. Finally, the financial impact could be as much as $12 million to replace the entire supply, so the availability value would fall at the low end of the High level and might be annotated (↓) accordingly.
- **Threat Assessment.** Although outlaw motorcycle gangs have never robbed a regional medical storage facility in the past, they have broken into local pharmacies to steal drugs on average once every ninety days. Thus, the threat likelihood would be rated Medium, albeit at the lower end of the range, based on a past frequency of 10-100 days for similar assets from different venues, using column 3 in Table C3-1, Threat Likelihood Table. Given the knowledge, skill and resources available to organized gangs, threat agent capabilities are undoubtedly High, so the overall threat level would be assessed as High in accordance with Table C3-3. Since the actual frequency of once every ninety days falls near the lower end of the range, the threat level might also be annotated (↓).
- **Vulnerability Assessment.** With standard frame construction and brick facing, the building fabric offers little resistance to forceful entry, even with steel mesh grills in the windows and plywood reinforcement in the walls, so the impact on the probability of compromise must be rated at a High level in accordance with Table D3-1, Vulnerability Impact on Prevention. Although a high quality intrusion alarm has been installed to alert the local police to any unauthorized entry, but their response times are typically twenty minutes or more. In effect, a solid detection mechanism is undermined by a relatively slow response capability. Using Table D3-2, Vulnerability Impact on Detection, Response and Recovery, this weakness could be assigned a Medium rating because the safeguards are only moderately effective. Since the inadequacies regarding structural integrity and the police force, prevention and response measures respectively, are clearly related, the Extended Vulnerability Assessment should be applied in accordance with section 6.1.3 of Annex D to produce a High vulnerability level.

- **Risk Assessment.** In this example, all three risk variables (asset value, threat and vulnerability) have been assigned High levels, so the residual risk would be 64 (4×4×4). On the other hand, both the asset value and the threat lie at the low end of the High range, so the assessed residual risk should be adjusted accordingly, reducing the lower value variable by one level, to give a result of 48 (3×4×4). Despite this adjustment, both results indicate a High level residual risk.

This page intentionally left blank.

Appendix E-2 - List of Assessed Residual Risks

Asset (Group/Subgroup)	Asset Values			Associated Threat (Activity/Agent Category)	T	Related Vulnerability	V	Residual Risk ($A_{Val} \times T \times V$)	R
	C	A	I						

<u>Legend</u>

C – Confidentiality. A – Availability. I – Integrity.

T – Threat. V – Vulnerability. A_{Val} – Asset Value. R – Risk.

1 Instructions

Using the results of the Asset Identification Phase, the Threat Assessment Phase and the Vulnerability Assessment segment of the Risk Assessment Phase, specifically the Asset Valuation Table or Statement of Sensitivity, the Threat Assessment Table and the Vulnerability Assessment Table in Appendices B-5, C-4 and
D-4 respectively:

- **Step 1.** Record all assets within the scope of the assessment in the first column with separate entries for each relevant asset value, noting those that fall near the upper or lower boundaries of the injury level.
- **Step 2.** Record all associated threats that might compromise these assets and asset values in the fifth column and their levels in the sixth column, noting those that fall near the upper or lower boundaries of the assessed level. Where there is some question regarding the actual threat level due to conflicting evidence, include separate entries for the higher and lower values. For deliberate threats where threat agent intentions and, therefore, the likelihood of occurrence are rated Medium or Low, insert another line to reflect the higher threat level if threat agent intentions changed to High.
- **Step 3.** Record all related vulnerabilities that expose each asset to an associated threat in the seventh column and their levels in the eighth column, noting those that fall near the upper or lower boundaries of the assessed level. Where there is some question regarding the actual vulnerability level due to conflicting evidence, include separate entries for the higher and lower values.
- **Step 4.** Convert the assigned levels for each of the three variables (asset values, threats and vulnerabilities) to numeric scores from one to five and compute the product, entering the results in the ninth column. In cases where two or three of the factors fall at the high or low range of the assessed level, adjust the lower score up or down by one for the calculation of residual risk. Finally, the corresponding risk level from Very Low to Very High may be inserted in the tenth column.

2 Example

The example explained in Appendix E-1, a regional medical storage facility, would generate the following entry in the List of Residual Risks:

Asset (Group/Subgroup)	Asset Values			Associated Threat (Activity/Agent Category)	T	Related Vulnerability	V	Residual Risk ($A_{Val} \times T \times V$)	R
	C	A	I						
Medicine/Morphine		H↓		Motorcycle Gangs/Theft	H↓	Structural Integrity Slow Response	H	(4-1)[1] × 4 × 4 = 48	H

[1] Both asset value and threat level have been assessed at the low end of the High range (H↓), so the lower value is reduced by one level for the calculation of residual risk. In this particular case, either the asset value or the threat level might have been adjusted because both variables have the same value.

Annex F - Recommendations Phase

1 Introduction

1.1 General

The Recommendations Phase of a TRA project comprises four sequential processes and one major output as follows:

- **Identification of Unacceptable Risks** – to determine which of the assessed residual risks computed during the Risk Assessment Phase of a TRA project exceed the Target Risk Level specified in the TRA Work Plan;[1]
- **Selection of Potential Safeguards** – to identify an array of appropriate safeguards that could mitigate unacceptable residual risks and reduce them to an acceptable level;
- **Calculation of Costs** – to assess the cost and cost-effectiveness of proposed safeguards;
- **Assessment of Projected Residual Risks** – to forecast the remaining residual risks once the recommended safeguards have been approved and fully implemented; and
- **Final TRA Report** – to present the risk acceptance authority with the findings and recommendations of the TRA project.

1.2 Aim

The aim of this annex is to describe the four processes and single output of the Recommendations Phase of a TRA project.

2 Identification of Unacceptable Risks

2.1 General

Once residual risks have been calculated and prioritized in the fourth phase of an assessment, the TRA team should generally concentrate on those which exceed the target threshold, defined in the original TRA Work Plan and approved by the risk acceptance authority. Various options may then be examined in detail to develop suitable recommendations for senior managers to achieve an acceptable risk posture at an affordable cost.

2.2 Underlying Determinants

The actual level of risk that may be acceptable can vary between organizations based upon several underlying factors including:

[1] As indicated in **section 5 of Appendix A-6**, the **Sample TRA Work Plan**, the Target Risk Level should be identified explicitly in advance for each TRA project.

- **Corporate Culture.** Some agencies and individuals are more risk tolerant while others are more risk averse, largely based upon past experience and personal preference. While these factors should be rationalized as much possible, they cannot be eliminated entirely.
- **Statutory and Regulatory Obligations.** For some government services and business lines, acceptable risk levels may be governed, at least indirectly, by federal statutes. For example, the Privacy Act and related regulations require the protection of personal information.
- **Potential Opportunities.** In some cases, higher risks may be acceptable in order to achieve even greater benefits from the opportunities afforded by certain program or project choices. For instance, use of the Internet for electronic service delivery is inherently risky, but the advantages in cost reduction and client convenience frequently outweigh the increased dangers involved.
- **Operational Expediency.** On occasion, it may prove impossible to mitigate the assessed residual risks to an acceptable level because suitable safeguards are simply unavailable or they cannot be implemented in time. Under these circumstances, in order to achieve essential operational goals, it may be necessary to accept otherwise intolerable risk levels in either the short or the long term.
- **Cost Constraints.** From a practical perspective, the safeguards required to achieve an acceptable level of residual risk may be prohibitively expensive so, of necessity, elevated risks might be approved, albeit with serious reservations.

2.3 Risk Ranges

Although each of the foregoing factors may colour the assessment of residual risks, a common approach to the determination of acceptability is generally preferable to enhance interoperability and communications amongst different programs and TRA projects. With that aim in mind, the subdivision of all possible risk values in five bands ranging from Very Low to Very High, can provide a useful construct for decision making. As a general rule, any residual risks in the Very High range are definitely unacceptable and require recommendations for remedial action. Those at the other end of the spectrum, at the Very Low level, are definitely acceptable with no further consideration. While some additional analysis may be required, High residual risks are probably unacceptable while Low risks are probably acceptable. Those in the Medium range are likely to be more contentious, requiring very careful examination to determine their relative acceptability.

This logical progression is captured in Table F-1.

Assessed Residual Risk	Very Low	Low	Medium	High	Very High
Acceptability	Definitely Acceptable	Probably Acceptable	Possibly Unacceptable	Probably Unacceptable	Definitely Unacceptable

Table F-1: Acceptability of Assessed Residual Risks

2.4 Management Options

2.4.1 General

Quite clearly, the recommendations in a final TRA report can vary widely depending upon the relative risk levels and, more specifically, whether or not the assessed residual risks are entirely acceptable.

2.4.2 Acceptable Residual Risks

For those that are fully acceptable, generally risks at the Very Low, Low and possibly the Medium levels, responsible managers may be presented with the following options:

- **Retain Existing Safeguards.** Any existing safeguards that reduce residual risk to an acceptable level should be retained, unless other alternatives might achieve the same ends in a more cost-effective manner. Of course, any current safeguards that do not contribute to meaningful risk reduction should be highlighted or flagged for possible removal.
- **Implement Proposed Safeguards.** All proposed safeguards that were factored into the TRA to achieve an acceptable level of residual risk should be approved, funded, installed and tested to verify their effectiveness.
- **Remove Excessive Safeguards.** In a few cases, where residual risks have been reduced well below the acceptable threshold, to a Low or Very Low level, with expensive or inconvenient safeguards, it may be feasible to recommend their removal to achieve greater economies or efficiencies provided that the related risks do not increase beyond the acceptable range, usually the Low or Medium levels.

2.4.3 Unacceptable Residual Risks

For any residual risks that are not acceptable, generally those at the Very High, High and perhaps the Medium levels, recommendations to responsible authorities could include any combination of the following:

- **Propose Additional Safeguards.** In most cases, the TRA team will recommend additional safeguards to reduce asset values, threats or, more often, vulnerabilities in order to achieve acceptable levels of residual risk.
- **Revise the Original Requirements.** On occasion, when suitable safeguards are prohibitively expensive, technically impractical or simply unavailable, the entire project or system might have to be reviewed with a view to –
  - revising the original requirements and limiting asset values,
  - choosing a more secure location,
  - adopting a more robust architecture, or
  - accepting an elevated level of residual risk.
- **Reject the Proposal or Cancel the Project.** Only infrequently will some residual risks be entirely irreconcilable, so the TRA team may have to recommend rejection of the proposal or cancellation of the project depending upon the purpose of the assessment.

2.5 Basis for Recommendations

As part of the Vulnerability Assessment (Annex D), existing and proposed safeguards were identified and categorized according to the security functions they perform, namely avoidance, deterrence, prevention, detection, response or recovery. Then, to determine relative vulnerabilities, the effectiveness of these safeguards was assessed based upon three factors, specifically their impact on (1) the likelihood of occurrence of a threat event, (2) the probability of compromise should the threat event actually arise, and (3) the severity of the outcome or the extent of the injury that might be expected.[2] Given the inverse relationship between vulnerabilities and safeguard effectiveness, appropriate recommendations for cost-effective solutions to address unacceptable residual risks may be developed in the next three processes of the Recommendations Phase:

- **Safeguard Selection.** Determine which security measures might be implemented to mitigate unacceptable risks on the basis of explicit safeguard selection criteria.
- **Cost Estimate.** Assess the costs and cost-effectiveness of each alternative.
- **Projected Residual Risk.** Compute the projected residual risk once the recommendations have been approved and implemented.

3 Selection of Potential Safeguards

3.1 General

The List of Assessed Residual Risks completed at the end of the Risk Assessment Phase of a TRA project, illustrated at Appendix E-2, is both a logical point of departure and an invaluable tool for choosing appropriate safeguards to mitigate unacceptable risks. To ensure consistent results, however, several explicit selection criteria, some qualitative and others quantitative in nature, should govern the analysis supporting all recommendations in the final TRA report. These selection criteria provide an objective rationale for each safeguard based upon the risk variables mitigated by the proposed security measures and their overall effectiveness.

3.2 Safeguard Selection Criteria: Risk Variables

3.2.1 Assets Protected

As indicated in Appendix F-2, the Safeguard Listing, some security measures protect several different asset classes while others offer fewer benefits, covering only a few asset groups or subgroups within a single asset category. This is an important consideration when choosing suitable countermeasures for two reasons. Firstly, the recommended safeguards must protect all assets that contribute to unacceptable residual risks. Of course, this is easily determined by simply sorting entries in the List of Assessed Residual Risks by risk level, from Very High to Very Low, and examining the associated assets in the first column. Secondly, all things being

[2] See **section 2**, **Safeguard Identification**, and **section 3**, **Safeguard Effectiveness**, in **Annex D**, the **Vulnerability Assessment**.

equal, security mechanisms that protect multiple assets are preferable to those with more limited effects because they could mitigate a greater number of risks.

3.2.2 Asset Values Preserved

An examination of the asset values (confidentiality, availability and integrity) at greatest risk is a logical extension of the first selection criterion. Clearly, safeguards must be chosen to protect both the assets and, more specifically, the asset values that contribute to unacceptable residual risks. This is also useful because some safeguards may be counterproductive in certain circumstances, given the inherent tension between confidentiality and availability mechanisms. For example, file encryption, a confidentiality measure, generally serves little purpose in cases where availability is the primary concern. Worse still, it might actually impede the exchange of data with adverse effects on availability.

3.2.3 Threat Activities Moderated

As noted in section 3.3 of Annex D, the Vulnerability Assessment, most safeguards mitigate risk by reducing vulnerabilities rather than threats. That being said, all threats that contribute to unacceptable residual risks should be identified explicitly to ensure that proposed safeguards address them directly or, more often, indirectly by moderating the related vulnerabilities. Again, this can be achieved by sorting entries in the List of Assessed Residual Risks according to risk levels. Finally, safeguards that moderate multiple threats are preferable to ones with more focused effects because they may deal with several different risks.

3.2.4 Vulnerabilities Alleviated

In a similar vein, safeguards should be selected to ease vulnerabilities associated with unacceptable residual risks. As with assets protected and threats moderated, security measures that relieve several vulnerabilities are generally preferable.

3.2.5 Security Functions Performed

The security functions performed by different safeguards (avoidance, deterrence, prevention, detection, response and recovery) and their impact on risk variables (asset values, threats and vulnerabilities) are examined in some detail in section 3 of Annex D, the Vulnerability Assessment. Security measures should be selected with these functions in mind because no safeguard is absolutely foolproof. Therefore, the final recommendations in a TRA report should normally present a balanced approach with linked detection, response and recovery mechanisms to complement any avoidance, deterrent and, more frequently, preventive measures in order to achieve defence in depth with an active security strategy, illustrated in Figure F-1. In a few cases, this may not be feasible where, for example, a natural hazard cannot be avoided or prevented, so early detection, response and recovery methods must receive greater emphasis. On the other hand, prevention may assume greater importance where confidentiality is the primary concern, simply because it may be difficult, if not impossible, to recover from a compromise and restore the original secrecy in the event of unauthorized disclosure. Finally, all detection measures must have an associated response and probably a recovery mechanism.

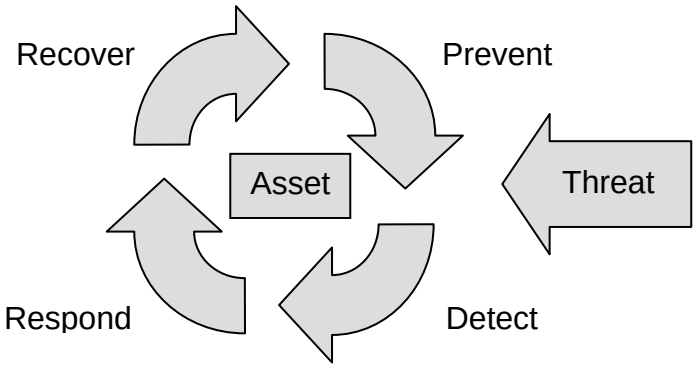

Figure F-1: Active Security Strategy

3.3 Safeguard Selection Criteria: Safeguard Effectiveness

3.3.1 Basic Considerations

As noted above, potential security measures to address all unacceptable risks are identified in the first stage of the safeguard selection process on the basis of their capacity to: (1) protect assets and asset values at greatest risk; (2) mitigate the most serious threats; (3) alleviate the most severe vulnerabilities; and (4) afford a balance between avoidance, deterrence or prevention, and detection, response and recovery. Now, in the second stage, the effectiveness of different alternatives is assessed based upon their impact on the three risk variables: asset values, threats and vulnerabilities. For example, a preventive measure that reduces an associated vulnerability from a High to a Low level is clearly more effective than another that achieves only a Medium level. Some other factors, such as the sensitivity, visibility and acceptability of a safeguard, its own vulnerability, any interdependence with other security measures, the maturity of the product or process, and its conformity with national or international security standards are also useful albeit less precise indicators of safeguard effectiveness.

3.3.2 Impact on Asset Values

Placing a ceiling or cap on asset values, an avoidance mechanism, can effectively mitigate risks in certain circumstances. The difference in asset values may be measured precisely in accordance with the injury tests explained in section 3 of Annex B, the Asset Identification and Valuation Phase. Thus, a transaction limit of $1,000 is more effective than one of $1 million for it reduces asset values from a Medium to a Low level.

3.3.3 Impact on Threats

Some deterrent mechanisms may dissuade deliberate threat agents, thereby reducing the likelihood of a threat event occurring in the first place. Choosing locations less susceptible to certain natural hazards can have the same effect. A few preventive measures, such as restrictions on the possession of lock-picking tools, may reduce threat agent capabilities and, therefore, the gravity of a threat event. In each case, the level of the threat may be recomputed to reflect the impact of the recommended safeguards. Those that generate a greater reduction in threat levels are more effective.

3.3.4 Impact on Vulnerabilities

As indicated in section 3.3 of Annex D, the Vulnerability Assessment, most safeguards address vulnerabilities rather than asset values and threats to mitigate unacceptable risks. For example, most preventive measures reduce the probability of compromise should a threat event actually arise, whereas detection, response and recovery mechanisms aim to limit or contain the damage, and moderate the severity of the outcome. As with asset values and threats, the vulnerability levels may be revised to capture the impact of the proposed security measures: again, the greater the difference, the more effective the safeguard.

3.3.5 Acceptability

Safeguard effectiveness frequently depends upon user and operator acceptance. In this regard, convenience and ease of operation are important issues, so simpler, user-friendly security measures are often preferable to more capable but complex solutions. For example, an access control mechanism based on multiple, unpronounceable passwords can be frustrating and, therefore, counterproductive. Other factors affecting the acceptability of a prospective countermeasure might include real or imagined safety concerns with certain biometric devices, like retinal scanners, and social or cultural resistance to intrusive searches or surveillance. All too often, the absolute effectiveness of a security mechanism may be unattainable in practice due to employee or client opposition. On the other hand, where this reluctance can be overcome with sympathetic leadership and sound training, well informed and highly motivated users can enhance the effectiveness of many safeguards.

3.3.6 Visibility

Highly visible safeguards, such as chain link fences or patrolling guards, may be more effective deterrents, but there can be negative side effects. Too much visibility may attract unwanted attention, increasing the likelihood of certain deliberate threats. Exposure like this may also provide adversaries with an opportunity to study the situation for exploitable vulnerabilities.

3.3.7 Safeguard Vulnerability

Like any other assets, safeguards may be vulnerable in their own right. Reliability, robustness, complexity, other maintenance issues and ease of use (or misuse) are real considerations affecting the susceptibility of a countermeasure to accidental failure or deliberate evasion. Each of these concerns should be assessed in relation to asset values and threats within the scope of the TRA project. In other words, safeguards that may be exploited by known threat agents to compromise assets identified in the Statement of Sensitivity are probably less effective than ones with no discernable or relevant vulnerabilities.

3.3.8 Safeguard Interdependence

Some safeguards act independently, but most rely upon other supporting or complementary security features for successful operation. For example, the effectiveness of even the best deadbolt lock depends upon the structural integrity of the door and doorframe in which it is installed, and it is easily undermined by adjacent, unprotected windows. The negative implications of safeguard interdependence reflect the old adage that a chain is only as strong as its weakest link. From a positive perspective, however, tightly integrated, mutually supporting security measures are often more effective than the sum of the parts with a defence in depth. Both factors merit consideration during the safeguard selection process.

3.3.9 Human Intervention

In a related issue, safeguards that depend upon human intervention or interpretation are frequently less reliable than fully automated mechanisms, especially if they are awkward or inconvenient to manage. Human nature being what it is, only the most conscientious individuals will remain alert over time and respond quickly, especially after a number of false alarms. Others are more likely to ignore or disable the sensor or alarm. That being said, properly trained and motivated personnel can enhance the effectiveness of certain safeguards with intelligent interpretation of conflicting data and a measured response to various threat events. Both possibilities should be examined during the assessment of safeguard effectiveness.

3.3.10 Sensitivity

Like other assets, security mechanisms may be sensitive to unauthorized disclosure and, therefore, require categorization as either classified or protected if the injuries that could reasonably be expected to arise in the event of a compromise were to affect the national or other interests respectively. Typically, this is a significant factor with respect to cryptographic devices and the associated keying material. Since classified and protected safeguards normally require further protection to maintain their confidentiality, they are frequently less desirable than completely unclassified countermeasures.

3.3.11 Mature/Proven Technology

Mature security products tend to be more effective than the latest technologies to hit the market. In practice, however, the actual difference can be difficult to measure unless the safeguard has undergone a formal evaluation of some kind. Nevertheless, when faced with a choice between two comparable solutions, the more stable product is usually preferable.

3.3.12 Security Standards

Various standards organizations, both national and international, develop common practices and procedures for the selection, installation or application and operation of security products and processes. In some cases, they also accredit laboratories to conduct formal tests and evaluations.[3] Some of these standards present broad security guidelines, others capture commonly accepted best practices, and a few establish formal methods for the evaluation of security equipment and products. As a general rule, safeguards that conform to one or more of these standards are likely to be more effective than others that do not. With a few noteworthy exceptions, such as the *Common Criteria for the Evaluation of Information Technology Security Products*,[4] conformity with approved standards offers little indication of relative safeguard effectiveness for the purposes of comparative analysis amongst different options. All the same, security measures based on recognized standards are generally preferable to other alternatives

---

3 A number of these standards bodies are listed in **Appendix F-1**, **Sources of Safeguard Data**.

4 An evaluation under the Common Criteria Scheme provides an explicit rating of the level of assurance associated with the security features of an IT security product. This Evaluated Assurance Level (EAL) can be translated directly into a relative assessment of safeguard effectiveness. CSE currently offers a one-day course, CSE755, Selecting the Right Security Technologies: Mapping Threat and Risk Assessment to Common Criteria, to explain the process. Further details may be found at: http://www.cse-cst.gc.ca/training/courses/755-e.html.

provided, of course, that they are fully implemented and carefully configured to meet all provisions of the relevant standard.

3.4 Summary

In summary, the safeguard selection process comprises two successive stages.

Firstly, security measures must be identified to address all unacceptable residual risks. To that end, the List of Assessed Residual Risks produced during the previous phase of the TRA project may be sorted on different fields to confirm which assets, threats and vulnerabilities contribute to the greatest risks. Clearly, safeguards must be selected to protect these assets and the related asset values, and mitigate the associated threats and related vulnerabilities.

Knowing which security measures afford the right kind of protection in a qualitative sense is not sufficient, however, to achieve acceptable levels of residual risk. It is also necessary to determine the level of protection required to drive all risks into the acceptable range. Therefore, the second activity in the safeguard selection process comprises an assessment of safeguard effectiveness, a quantitative measure of their impact on asset values, threats and vulnerabilities tempered with some other more subjective considerations.

At the end of this process, the TRA team should have identified at least one, but preferably several different options to address each unacceptable risk.

Appendix F-3 provides a checklist of safeguard selection criteria with step-by-step instructions for their application.

4 Identification of Associated Costs

4.1 Primary Objective

Once an array of potential safeguards has been identified to address all unacceptable residual risks, it is incumbent on the TRA team to determine which options provide the best value for money. To that end, all costs associated with each safeguard, both direct and indirect, should be captured as accurately as possible to support informed decision making and justify the final recommendations to the risk acceptance authority.

4.2 Direct Costs

Most direct costs, or at least reasonable estimates, are readily available from project managers and design offices, procurement authorities, product vendors, and many of the sources listed in Appendix F-1. Some of the more important issues to consider include:

- **Design and Development.** Although most safeguards, both security equipment and procedures, may be purchased directly, some might have to be designed and developed in house or through a commercial contractor. This is usually the case with new facilities,

sizeable renovations, complex IT systems and major Crown projects where security considerations typically account for something between five and ten percent of the total budget. Even recommendations for specific solutions in smaller TRA projects may incur some architectural and engineering costs for feasibility studies, design and development.

- **Acquisition.** The most obvious costs associated with any recommendations will be the purchase price or licensing fees for security hardware, software or procedural documents. In most cases, precise estimates are readily available from the original vendor or reseller.
- **Integration.** Almost invariably, some effort will be required to integrate recommended safeguards with existing facilities, hardware, software or procedures. Related costs are very similar to those for major projects, with salaries for design, development and testing generally accounting for the largest expenditures.
- **Installation.** While installation costs may be included with integration expenses, they might be calculated separately, especially when the recommended safeguards must be deployed regionally and, therefore, require an extensive travel budget.
- **Documentation.** With many safeguards, a full suite of documentation, such as user guides, installation instructions and operator manuals, is included with the purchase price. On the other hand, it is often necessary to document the actual configuration of new security equipment and prepare site-specific standard operating procedures. Updating this documentation is also an ongoing expense that is frequently overlooked.
- **Training.** New security equipment and procedures generally entail some training costs if they are to be installed and operated correctly. This too can be an ongoing expense as personnel move between positions and organizations.
- **Ongoing Operation.** Operating costs for the recommended safeguards cover a variety of expenditures including salaries and benefits for security guards and other personnel, expendable materiel and supplies, renewable licenses and other fees, regular upgrades, audits and reviews, and updating of both training and documentation if they are not captured separately, as noted above.
- **Maintenance.** Routine maintenance costs might be captured under operating expenses, but separate funds might be earmarked to repair or replace defective equipment based upon the assessed mean-time-between-failure.

4.3 Indirect Costs/Benefits

In most cases, indirect costs or benefits associated with potential safeguards are far more difficult to predict with any degree of accuracy because the full impact of their implementation may not be evident without operational experience. Nevertheless, some effort should be made to project the following indirect costs and benefits wherever possible:

- **Reduced Productivity.** Some safeguards can cause delays or distractions and otherwise impede productivity. For example, rigorous access controls and random spot checks can slow pedestrian and vehicular traffic at the entrances to secure facilities. Audit functions, both manual and automated, impose an overhead on personnel and IT equipment with an attendant impact on throughput. In general, these costs are relatively minor irritants that are fully offset by other advantages or benefits, but they should be identified explicitly wherever possible to ensure a balanced assessment.

- **Improved Efficiency.** In theory, most safeguards should have a positive impact on efficiency by reducing the likelihood and gravity of any compromise to acceptable levels commensurate with established business requirements. Availability safeguards, such as business continuity planning, provide perhaps the clearest examples because the costs of any interruption and the benefits of early resumption can be measured quite precisely.

4.4 Cost-Effectiveness

4.4.1 Basic Approach

Having identified an array of potential safeguards based upon explicit safeguard selection criteria (section 3.2) and determined the total cost of ownership for every option (sections 4.2 and 4.3), the TRA team may face some difficult choices between viable alternatives. Therefore, the actual cost-effectiveness of each proposal should be calculated to provide an objective justification for the final recommendations. In this regard, the two most important considerations are the amortized annual cost of the recommended security measures and their overall impact on residual risk, the cost and effectiveness dimensions respectively, but some other issues may also arise in practice.

4.4.2 Amortized Annual Cost

The total cost of ownership is significant in absolute terms, especially because many of the expenditures, such as acquisition and installation expenses, are front-end loaded. This figure must be tempered, however, by the life expectancy of the proposed safeguards. Some, such as physical security features built into the fabric of a building, have a long life expectancy, while others, such as security software, usually have a shorter life span. In practical terms, an expensive but long-lasting countermeasure may be a better bargain than a cheaper option that will require early replacement. Thus, the amortized annual cost, simply calculated as the quotient of the total cost of ownership divided by the life expectancy, illustrated in Figure F-2, is the first analytical factor to substantiate the final recommendations.

$$\frac{\text{Total Cost of Ownership (\$)}}{\text{Life Expectancy (years)}} = \text{Amortized Annual Cost (\$/year)}$$

Figure F-2: Calculation of Amortized Annual Cost

4.4.3 Total Risk Reduction

As noted in section 3.3.1, all safeguards mitigate risk by reducing one or more of the three variables: asset values, threats or vulnerabilities. Furthermore, some security measures, such as physical access controls, protect many different assets and asset values from a variety of threats, thereby addressing a broad array of risks. Others, such as paper shredders, concentrate on a single asset value (confidentiality) for a limited number of assets (classified and protected documents) to thwart a narrow range of threats (threat activities causing unauthorized disclosure). While both may be necessary in any given situation, security measures like the former that reduce more risks to an acceptable level generally represent a better value for money.

Total risk reduction, the second criterion for determining the relative cost-effectiveness of different options, may be compiled as follows:

- select from the List of Assessed Residual Risks (Appendix E-2) all unacceptable risk combinations (asset value, threat and vulnerability) that are moderated by the proposed safeguard;
- re-compute the residual risk for each of these entries, based upon the lower asset value, threat or vulnerability achieved with the proposed safeguard;
- determine the number of levels between the assessed and projected residual risks for each combination affected by the proposed safeguard; and
- calculate the total risk reduction, namely the sum of all the changes in risk levels.

4.4.4 Recommended Safeguards

Ideally, recommendations in the final TRA report, when approved and implemented, should reduce all unacceptable residual risks to acceptable levels at the least or most reasonable cost. To achieve this goal, where there are alternative solutions, each of the options identified during the safeguard selection process in section 3 above should be ranked according to their relative cost-effectiveness, namely the quotient of amortized annual cost divided by the total risk reduction, illustrated in Figure F-3. The most cost-effective suite of safeguards may then be identified and recommended to address unacceptable residual risks. These recommendations should be summarized in the tabular form at Appendix F-5.

$$\frac{\text{Amortized Annual Cost (\$/year)}}{\text{Total Risk Reduction (levels)}} = \text{Cost-Effectiveness (\$/year/level)}$$

Figure F-3: Calculation of Safeguard Cost-Effectiveness

4.4.5 Practical Considerations

In a few cases, the calculation of cost-effectiveness may be moot because only one safeguard exists to mitigate a particular residual risk, or the actual solution may be dictated by approved government standards. Occasionally, the most effective solution may be prohibitively expensive. If affordable alternatives cannot achieve the targeted risk levels, it may be necessary to recommend a review of the original requirements, rejection of the proposal or cancellation of the project, as discussed in section 2.4.3. More often than not, however, the real difficulty will be choosing from several options, all of which achieve suitable risk reduction, albeit in different ways and at different costs. In any event, the calculation of cost-effectiveness for competing safeguards outlined above and amplified in Appendix F-4 provides an objective basis for the final recommendations to address unacceptable residual risks or identify those which cannot be resolved.

5 Assessment of Projected Residual Risk

To illustrate the impact of these recommendations in the final TRA report, all unacceptable risks from the List of Assessed Residual Risks at Appendix E-2 should be transferred to the appropriate columns under the offsetting safeguards in the Recommendations Table. Then, the residual risks remaining after the approval and implementation of all proposals should be calculated and entered in the table, as explained in the detailed instructions with Appendix F-5.

6 Final TRA Report

6.1 Format of a TRA Report

At this point, the outputs from each of the preceding phases of the TRA project may be combined and summarized in a logical narrative with supporting material to explain and justify the final recommendations. Brevity is crucial, however, to promote and facilitate management review, so each section should focus on the most important issues, leaving much of the detail to summary tables and supporting annexes. While the format of a TRA report can be quite flexible depending upon the purpose of the assessment, typical contents include:

- **Executive Summary.** All but the shortest TRA reports should commence with an Executive Summary of one or two pages describing the purpose and subject of the assessment, any assessed residual risks that are unacceptable, major recommendations, the total cost of all proposals and the projected residual risks once the recommendations have been approved and implemented.
- **Background.** As indicated in section 1 of Appendix A-6, the Sample TRA Work Plan, identify the organization and provide some background material to situate the assessment within a departmental context. Depending upon the purpose of the TRA, this might include –
    - a short description of the business line and its operating environment,
    - any service delivery levels or obligations relevant to the assessment,
    - the rationale for a new or upgraded facility or IT system, and
    - the nature of any specific security concerns to be addressed.
- **Aim.** As explained in section 2 of Appendix A-6, the Sample TRA Work Plan, state the purpose of the assessment in a single sentence like the following examples –
    - "The aim of this TRA is to assess the risks associated with upgrades planned for *[facility name]* and to recommend suitable safeguards."
    - "The aim of this TRA is to assess the risks associated with *[name of new IT system]* and to recommend suitable safeguards in support of system certification and accreditation."
    - "The aim of this TRA is to assess the need for safeguards beyond baseline security requirements for *[identify facility or IT system]*."
- **Mandate.** Briefly review the authority of the TRA team established in accordance with section 3 of Annex A, the Preparation Phase. Attach a copy of any written instructions and the TRA Work Plan described in Appendix A-6 as annexes.

- **Scope.** As indicated in section 4 of Annex A, the Preparation Phase, identify the subject of the assessment and provide a general description of the facility or IT system under assessment. Maps, charts, floor plans and system schematics can be particularly useful to delineate the boundaries of a TRA project. Note any related TRA reports and explain their relationship with the current project. Lists of what falls within the scope of the assessment and what does not might be attached as annexes.
- **Asset Identification and Valuation.** Once all assets, both tangible and intangible, employees and services within the scope of the assessment have been identified and assigned values based on the injury tests explained in Annex B, the findings should be attached to the TRA report in the form of an Asset Valuation Table or Statement of Sensitivity illustrated in Appendix B-5. The body of the text should provide a short summary, concentrating on the most important assets and asset values, and their relationship with the business lines or operational objectives of the organization.
- **Threat Assessment.** A complete list of threats and threat levels should be attached as an annex to the TRA report in the form shown at Appendix C-4, the Threat Assessment Table. Only the more serious threats affecting more valuable assets, typically those in the High and Very High ranges, should be examined briefly in the body of the TRA report.
- **Vulnerability Assessment.** Like the Statement of Sensitivity and the Threat Assessment, the Vulnerability Assessment should comprise a short explanation of the more serious security weaknesses in the main report with an attachment in the form of Appendix D-4, the Vulnerability Assessment Table, listing all of the problems.
- **Risk Assessment.** The Risk Assessment can be the longest and most complex portion of many TRA reports because every unacceptable residual risk must be explained in terms meaningful to the risk acceptance authority. Of course, the results should be compressed and summarized as much as possible with details relegated to an annex like Appendix E-2, the List of Assessed Residual Risks, but the text must clarify the relationships amongst asset values, threats and vulnerabilities, and their impact on residual risks. This can be a challenge when the worst risks arise from elevated threats and vulnerabilities to assets of lower value, since many managers tend to focus on the most important assets rather than the risks to which they are exposed.
- **Recommendations.** From a management perspective, the Recommendations are the most important part of a TRA report. The costs associated with each recommendation and the projected residual risk should be explained carefully in non-technical terms to solicit management support and approval. As with earlier sections, most of the detailed analysis of safeguard costs and effectiveness should be captured in an annex based upon Appendix F-5, the Recommendations Table.
- **Attachments.** To streamline the main narrative, supporting material for a TRA report should be presented in a series of attachments or annexes, including –
    - TRA Mandate,
    - TRA Work Plan,
    - Scope of Assessment,
    - Related TRA Reports,
    - Asset Valuation Table or Statement of Sensitivity,
    - Threat Assessment Table,

- Vulnerability Assessment Table,
- Residual Risks Table,
- Recommendations Table, and
- Reference Documents, to list all manuals, schematics, incident reports and other material consulted during the TRA project that collectively comprise the TRA record in support of the TRA report.

Appendix F-6 provides an Outline TRA Report with explanatory notes and cross-references to relevant sections in the body of the *Harmonized TRA Methodology* as an aide-mémoire or checklist for security analysts, while Appendix F-7 presents a complete Sample TRA Report.

6.2 TRA Report versus TRA Record

As noted throughout the *Harmonized TRA Methodology*, from the Preparation Phase through to the final Recommendations Phase, many different sources of information must be consulted to identify assets within the scope of the assessment, determine their values, capture relevant threat data, uncover associated vulnerabilities and select cost-effective safeguards.[5] In fact, for all but the simplest TRA projects, the list of reference material can become quite extensive. Although these references are absolutely crucial to support the analytical processes, they should not normally accompany the final TRA report. They should be cited in an annex, however, and retained on file for future examination as part of the permanent TRA record.

[5] Some of these data sources are enumerated in:

- section 8 of **Appendix A-6**, the **Sample TRA Work Plan**;
- **Appendix B-1**, **Sources of Asset Data**;
- **Appendix C-1**, **Sources of Threat Data**;
- **Appendix D-1**, **Sources of Vulnerability Data**; and
- **Appendix F-1**, **Sources of Safeguard Data**.

This page intentionally left blank.

Appendix F-1 - Sources of Safeguard Data

Departmental Resources	
Data Source/Documentation	**Safeguard Classes/Groups**
Program Managers • Business Plans • Standard Operating Procedures	• Security Program o Roles and Responsibilities o Human Resources o Financial Resources o Security Procedures • Sharing Information and Assets o Information • Contracting • Identification of Assets • Sanctions
Material/Asset Managers • Asset Inventories • Standard Operating Procedures	• Contracting • Physical Security o Secure Storage
Facility Managers • Floor Plans/Building Schematics • Guard Force Instructions • Access Control Procedures • Emergency Plans • Incident Response Procedures	• Sharing Information and Assets o Facilities • Protection of Employees o Management Response/Protective Measures • Physical Security o Perimeter Security o Access Controls o Facility Management
Human Resources • Incident Response Procedures	• Protection of Employees
Finance • Standard Operating Procedures	• Access Limitations o Availability/Integrity/Separation of Duties
Chief Information Officer • Service Level Agreements • Asset Sharing Arrangements • IT Security Standards/Orders	• Sharing Information and Assets o IT Infrastructure • IT Security o Management Controls o (Some) Technical Safeguards o Operational Safeguards
Systems (Security) Administrator • System Schematics • Standard Operating Procedures • Security Test/Evaluation Reports • Incident Logs/Reports	• IT Security o (Some) Management Controls o Technical Safeguards o Operational Safeguards

Departmental Resources	
Data Source/Documentation	**Safeguard Classes/Groups**
Departmental Security Officer • Departmental Security Orders • Standard Operating Procedures • Security Inspection Reports • Investigation Reports	• Security Program • Contracting • Security Awareness/Training • Identification of Assets • Security Risk Management • Security Screening • Protection of Employees • Physical Security • Security in Emergencies • Investigation of Incidents • Sanctions
IT Security Coordinator • Product Reviews/Evaluations • Incident Reports	• IT Security Incidents/Investigations
BCP Coordinator • Business Continuity Plans • BCP Exercise/Test Results	• Business Continuity Planning
Internal Audit/Review • Security Audits/Reviews	• Security Program (any management controls subject to audit or review)
Occupational Health and Safety • Standard Operating Procedures • Incident/Investigation Reports	• Protection of Employees o Incident Management

External Resources: Security Lead Departments	
Data Source/Documentation	**Types of Safeguards**
Communications Security Establishment http://www.cse-cst.gc.ca/publications/publications-e.html • IT Security Guides and Directives • IT Security Alerts and Bulletins http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html • Product Evaluation Certification Reports	• IT Security
Public Safety and Emergency Preparedness Canada http://www.psepc-sppcc.gc.ca/prg/em/index-en.asp • Analytical Releases/Advisories	• Critical Infrastructure Protection • Cyber Security • Disaster Mitigation • Emergency Preparedness
Royal Canadian Mounted Police http://www.rcmp.ca/tsb/pubs/index_e.htm • Security Guides/Reports	• Physical Security • IT Security
Public Works and Government Services Canada http://www.ciisd.gc.ca/text/ISM/toc-e.asp • **Industrial Security Manual**	• Contract Security

External Resources: Government Standards Organizations	
Data Source	**Types of Safeguards**
National Research Council http://www.nationalcodes.ca/ncd_home_e.shtml • National Building Code of Canada • National Fire Code of Canada	• Physical Security and Safety
Standards Council of Canada http://www.scc.ca/en/index.shtml • Many Safety/Security Standards	• Various

External Resources: Other Standards Organizations	
Data Source	**Types of Safeguards**
American National Standards Institute http://www.ansi.org/	• IT Security Standards
Canadian Standards Association http://www.csa.ca/about/Default.asp?language=english	• Health/Safety Standards
International Organization for Standardization http://www.iso.org/iso/en/ISOOnline.frontpage	• Many Safety/Security Standards • IT Security Standards
International Telecommunications Union http://www.itu.int/ITU-T/	• IT and IT Security Standards
National Institute of Standards and Technology http://www.nist.gov/	• IT and IT Security Standards
Organization for Economic Cooperation and Development http://www.oecd.org/home/	• Privacy and IT Security Standards

External Resources: Other Private Sector Organizations	
Data Source	**Types of Safeguards**
CERT Coordination Center http://www.cert.org/nav/index_green.html	• Technical Vulnerabilities
Common Criteria http://www.commoncriteriaportal.org/public/consumer	• IT Security Guidelines
SANS Information and Computer Security Resources http://www.sans.org/resources/resources.php	• IT Security Safeguards
Product Vendors	• Technical Security Features

Notes:

1. The foregoing list of safeguard sources is not complete. Other material will be added from time to time. Any suggestions for further references or contacts may be submitted to the offices identified in the Foreword.
2. The inclusion of any web site should not be construed as an endorsement. Similarly, the exclusion of other potentially useful sources is not a rejection. The list is merely intended to illustrate the wealth of information that is readily available to security practitioners and risk managers.

Appendix F-2 - Safeguard Listing

Safeguard Class Safeguard Group Safeguard	Impact			Assets Protected	Values Protected			Threats Mitigated	Reference(s)
	A_{Val}	T	V		C	A	I		
Security Program									GSP 10.1
Roles and Responsibilities									
Executives	√		√	All	√	√	√	All	MITS 9.2
Program Managers	√		√	All	√	√	√	All	MITS 9.6
Project Managers	√		√	All	√	√	√	All	MITS 9.6 & 9.10
Chief Information Officer	√		√	All	√	√	√	All	MITS 9.4
Employees			√	All	√	√	√	All	MITS 9.8
DSO			√	All	√	√	√	All	GSP 10.1 & MITS 9.3
IT Security Coordinator			√	I, T, S	√	√	√	All	MITS 9.1
COMSEC Custodian			√	I	√		√	E, C, A	MITS 9.9
BCP Coordinator			√	All		√		S, T, C, A, N	MITS 9.5
Human Resources									
Effective Establishment			√	All	√	√	√	All	
Classification Levels			√	All	√	√	√	All	
Financial Resources									
Departmental Operations			√	All	√	√	√	All	
Projects			√	All	√	√	√	All	MITS 9.2
Security Policy/Procedures									
Sharing Information/Assets	√		√	I, T, F, S	√	√	√	E, S, C, A	GSP 10.2
Contracting	√		√	I, S	√	√	√	E, S, C	GSP 10.4
Security Awareness/Training			√	All	√	√	√	All	GSP 10.5
Identification of Assets	√		√	I	√	√	√	All	GSP 10.6
Security Risk Management			√	All	√	√	√	All	GSP 10.7
Access Limitations			√	All	√	√	√	E, S, s, T, C, A	GSP 10.8
Security Screening			√	All	√	√	√	E, S, s, T, C, A	GSP 10.9
Protection of Employees			√	P		√		S, s, T,C, A, N	GSP 10.10
Physical Security			√	All	√	√	√	All	GSP 10.11
IT Security			√	I, T, S	√	√	√	All	GSP 10.12, MITS 10, MG-01 Appendix C & MG-09 5
Security in Emergencies			√	All	√	√	√	S, T, A, N	GSP 10.13
Business Continuity Planning			√	All		√		S, T, C, A, N	GSP 10.14
Security Program Audit			√	All	√	√	√	All	GSP 11
Investigation of Incidents			√	All	√	√	√	All	GSP 10.15
Sanctions		√	√	All	√	√	√	E, S, s, T, C, A	GSP 10.16
Sharing Information/Assets									GSP 10.2
Information									
Arrangements	√		√	I, S	√	√	√	E, S, C, A	
Facilities									G1-027
Arrangements	√		√	F, S	√	√	√	E, S, C, A	
IT Infrastructure									MITS 12.10
Arrangements	√		√	I, T, S	√	√	√	E, S, C, A	

Safeguard Class Safeguard Group Safeguard	Impact			Assets Protected	Values Protected			Threats Mitigated	Reference(s)
	A_{Val}	T	V		C	A	I		
Security Outside Canada									GSP 10.3
Special Standards									
TRAs by Location			√	All	√	√	√	All	
Travel Restrictions									
By Location		√	√	P, I	√	√		E, T, C, N	DFAIT
Contracting									GSP 10.4, SCM & ISM
Roles and Responsibilities									SCM 4-6
Project/Technical Authority			√	I	√			E, S, C	
SRCL	√		√	I	√			E, C	SCM 7
Facility Security Clearance									SCM 8
Personnel Assigned		√	√	I	√			E, C	
Document Safeguarding			√	I	√			E, C	
International Contracts			√	I	√			E, S, C	SCM 10
Security Awareness/Training									GSP 10.5, MITS 12.12-12.13, MG-01 Appendix F, MG-09 13 & G1-030
Roles and Responsibilities									STA 3
Training/Awareness Officer	√	√	√	All	√	√	√	E, S, s, T, C, A	
Security Training									STA 4.1
Security Practitioners	√	√	√	All	√	√	√	E, S, s, T, C, A	
Security Awareness									STA 4.2
Initial Briefings	√	√	√	All	√	√	√	E, S, s, T, C, A	STA 4.3
Regular Updates	√	√	√	All	√	√	√	E, S, s, T, C, A	STA 8
Identification of Assets									GSP 10.6 & IoA
Confidentiality									IoA 6.5
Categorization: Classified	√		√	I	√			E, C	
Marking: Classified			√	I	√			E, C	IoA 7.1 & MG-09 14.5
Categorization: Protected	√		√	I	√			E, C	
Marking: Protected			√	I	√			E, C	IoA 7.1 & MG-09 14.5
Availability									IoA 6.6
Categorization	√		√	All		√		S, T, C, A, N	
Marking			√	All		√		S, T, C, A, N	
Integrity									IoA 6.7
Categorization	√		√	I			√	S, s, C, A	
Marking			√	I			√	S, s, C, A	
Security Risk Management									GSP 10.7 & SRM
TRAs									SRM 6 & MG-09 7
Initial Assessment	√		√	All	√	√	√	All	
Continuous Monitoring	√		√	All	√	√	√	All	
Access Limitations									GSP 10.8
Classified/Protected Assets									
Need to Know		√	√	I	√			E, C	
Security Screening		√	√	All	√	√	√	E, S, s, T, C, A	
Availability/Integrity									
Separation of Duties	√	√	√	All	√	√	√	S, s, T, C, A	

Safeguard Class Safeguard Group Safeguard	Impact			Assets Protected	Values Protected			Threats Mitigated	Reference(s)
	A_{Val}	T	V		C	A	I		
Security Screening									GSP 10.9 & SS
Reliability Status									SS 7
Establishing Requirements			√	All	√	√	√	E, S, s, T, C, A	
Initial Screening		√	√	All	√	√	√	E, S, s, T, C, A	
Evaluating Results		√	√	All	√	√	√	E, S, s, T, C, A	
Regular Updating		√	√	All	√	√	√	E, S, s, T, C, A	
Review for Cause		√	√	All	√	√	√	E, S, s, T, C, A	
Revocation		√	√	All	√	√	√	E, S, s, T, C, A	
Release Procedures		√	√	All	√	√	√	E, S, s, T, C, A	
Security Clearance									SS 9-10
Establishing Requirements	√		√	I	√			E, C	
Initial Screening		√	√	I	√			E, C	
Evaluating Results		√	√	I	√			E, C	
Regular Updating		√	√	I	√			E, C	
Review for Cause		√	√	I	√			E, C	
Revocation/Downgrading		√	√	I	√			E, C	
Release Procedures		√	√	I	√			E, C	
Site Access Clearance									SS 10.2
Establishing Requirements	√		√	I	√			E, C	
Initial Screening		√	√	I	√			E, C	
Evaluating Results		√	√	I	√			E, C	
Regular Updating		√	√	I	√			E, C	
Review for Cause		√	√	I	√			E, C	
Revocation		√	√	I	√			E, C	
Release Procedures		√	√	I	√			E, C	
Protection of Employees									GSP 10.10, OSHP
Identify Employees at Risk									
TRA			√	P		√		S, s, T, C, A, N	
Management Response									
Protective Measures			√	P		√		S, s, T, C, A, N	
Support Mechanisms			√	P		√		S, s, T, C, A, N	
Training and Counselling			√	P		√		S, s, T, C, A, N	
Incident Management									
Incident Reporting			√	P		√		S, s, T, C, A, N	
Incident Investigation			√	P		√		S, s, T, C, A, N	
Remedial Action			√	P		√		S, s, T, C, A, N	
Physical Security									GSP 10.11 & PS
Planning Factors									G1-005
Building Codes			√	All	√	√	√	All	G1-010
Security Zones			√	All	√	√	√	E, S, s, T, C	PS, 6.2 & G1-026
Site Selection									PS 7
Easements Through Site		√	√	All		√		E, S, s, T, C	
Emergency Lanes			√	All		√		All	
Building Location/Topography		√	√	All		√		All	
Emergency Services			√	All		√		All	
Adjacent Occupants		√	√	All	√	√	√	E, S, C	
Perimeter Security									PS 7.3
Control of Site Perimeter		√	√	All	√	√	√	E, S, s, T, C	

Safeguard Class Safeguard Group Safeguard	Impact			Assets Protected	Values Protected			Threats Mitigated	Reference(s)
	A_{Val}	T	V		C	A	I		
Illumination of Site		√	√	All	√	√	√	E, S, s, T, C, A	G1-002
Exterior Signs		√	√	All	√	√	√	E, S, s, T, C, A	
Landscape Design		√	√	All	√	√	√	E, S, s, T, C, A	
Parking		√	√	All	√	√	√	E, S, s, T, C, A	
Entry Security									PS 7.4
Pedestrian Entrances/Lobbies			√	All	√	√	√	E, S, s, T, C	G1-017 & G1-018
Service/Utility Openings			√	All	√	√	√	E, S, s, T, C	
Shipping/Receiving Areas			√	All	√	√	√	E, S, s, T, C	G1-015
Interior Security Planning			√						PS 7.5
Circulation Routes			√	P, F		√		S, s, T, C, A	
Elevator Lobbies			√	P		√		S, s, T, C	
Daycare Centres			√	P		√		S, T, C, A	
Conference Rooms/Boardrooms			√	P, I	√	√		E, S, s, T, C	
Stairwells/Elevators			√	P		√		S, s, T, C	
Washrooms			√	P		√		S, s, T, C	
Amenity Spaces			√	P		√		S, s, T, C	
Mailrooms			√	P, I, F	√	√		E, S, s, T, C	
Telecommunications/Wiring			√	I	√	√	√	E, S, T, C, A	
HVAC Spaces			√	F		√		S, s, T, C, A	
Server Rooms			√	I, T, S	√	√	√	E, S, s, T, C, A	G1-031
Access Controls									PS 7.6 & G1-025
Identification Cards			√	All	√	√	√	E, S, s, T, C	G1-005
Electronic Access Controls			√	All	√	√	√	E, S, s, T, C	
Electronic Intrusion Detection		√	√	All	√	√	√	E, S, s, T, C	
Closed Circuit Video Equipment		√	√	All	√	√	√	E, S, s, T, C, A	
Security Control Centre			√	All	√	√	√	All	G1-013
Sensitive Discussion Areas			√	I	√			E, C	G1-004
Secure Rooms			√	I	√	√	√	E, S, s, T, C	G1-029
Security Guards		√	√	All	√	√	√	All	G1-008
Facility Management									PS 7.7 & G1-027
Leasing Contracts	√		√	All	√	√	√	E, S, s, T, C, A	
Maintenance Services			√	All	√	√	√	E, S, s, T, C, A	
Cleaning Services			√	All	√	√	√	E, S, s, T, C, A	
Interior Signs		√		All	√	√	√	E, S, s, T, C, A	
Locking Hardware/Key Control			√	All	√	√	√	E, S, s, T, C	G1-007 & G1-016
Renovation Work			√	All	√	√	√	All	
Facility Security Committee	√		√	All	√	√	√	All	
Secure Storage									PS 8
Security Containers			√	I	√	√	√	E, C	G1-001
Keys/Combinations			√	I	√	√	√	E, S, T, C	G1-007 & G1-016
Maintenance of Containers			√	I	√	√	√	E, S, T, C	
Disposal of Containers			√	I	√			E, C	
Secure Rooms/Vaults			√	I	√	√	√	E, C	G1-019 & G1-029
Transport/Transmittal									PS 9 & G1-009
Transport	√		√	I	√		√	E, C	
Transmittal	√		√	I	√		√	E, C	
Destruction									PS 10
Storage Pending Disposal			√	I	√			E, C, A	

Safeguard Class Safeguard Group Safeguard	Impact			Assets Protected	Values Protected			Threats Mitigated	Reference(s)
	A_{Val}	T	V		C	A	I		
Destruction Equipment: Paper			√	I	√			E, C, A	
Destruction Equipment: IT Media			√	I	√			E, C, A	MITS 16.2, DSX-G , G2-003 & ITSG-06
Equipment Marking			√	I	√			E, C, A	
Equipment Maintenance			√	I	√			E, C	
Contracted Services			√	I	√			E, C	
Emergency Destruction			√	I	√			E, C	
IT Security									GSP 10.12 & MITS
Management Controls									
System Development Life Cycle	√		√	I, T, S	√	√	√	All	MITS 12.1, MG-02, MG-09 8 & ITSA-09
IT Security Resources for Projects			√	I, T, S	√	√	√	All	MITS 11
Certification and Accreditation	√	√	√	I, T, S	√	√	√	All	MITS 12.2.3 & MG-04
Contracting			√	I, T, S	√	√	√	E, S, C	MITS 12.7
Outsourcing			√	I, T, S	√	√	√	E, S, C	
Physical and Personnel Security									G2-002
Physical Security			√	I, T, S	√	√	√	All	G1-031 & MITS 16.1
Personnel Security		√	√	I, T, S	√	√	√	E, S, s, T, C, A	MITS 16.3
Technical Safeguards									
Evaluated Products			√	I, T, S	√	√	√	All	MITS 16.4.1
Identification and Authentication			√	I, T, S	√	√	√	E, S, s, T, C, A	MITS 16.4.2, MG-09 16 & R2-001
Authorization/Access Control			√	I, T, S	√	√	√	E, S, s, T, C, A	MITS 16.4.3 & MG-09 17
Cryptography			√	I	√		√	E, C	MITS 16.4.4, ITSD-01 Annex C, ITSB-013, ITSG-10, ITSG-13 & MG-09 19
Public Key Infrastructure (PKI)			√	I, S	√	√	√	E, C	MITS 16.4.5
Perimeter Defence			√	I, T, S	√	√	√	E, S, s, T, C	MITS 16.4.6, ITSD-02, MG-01 &
Mobile Computing/Telework	√		√	I, T, S	√	√	√	E, S, s, T, C, A	MITS 16.4.7 & ITSPSR-14
Wireless Devices	√		√	I, S	√	√	√	E, S, s, T, C, A	MITS 16.4.8, ITSB-02, ITSB-03, ITSB-06, ITSB-12, ITSB-15, ITSB-19, ITSB-29, ITSPSR-16, ITSPSR-17 ITSPSR-18, ITSPSR-21
Emanations Security			√	I	√			E	MITS 16.4.9, ITSD Annex E & ITSB-18
Telecommunications Cabling			√	I, S	√	√		E	MITS 16.4.10
Software Integrity			√	I, T, S	√	√	√	E, S, s, T, C, A	MITS 16.4.11
Software Security Configuration			√	I	√	√	√	E, S, s, T, C	MITS 16.4.11, G2-004, G2-005, ITSPSR-19 & ITSG-20
Technical Safeguards (continued)									
Malicious Code Protection			√	I, S		√	√	E, S, s, T, C	MITS 16.4.12 & R2-002

Safeguard Class Safeguard Group Safeguard	Impact			Assets Protected	Values Protected			Threats Mitigated	Reference(s)
	A_{Val}	T	V		C	A	I		
Intrusion Detection			√	I, S	√	√	√	E, S, s, T, C	MITS 17-18
Backup/Recovery			√	I, T, S		√		S, s, T, C, A, N	MITS 18.5, ITSB-09 MG-01 Appendix E & MG-09 11 & 14.4
Operational Safeguards									
Help Desk/Problem Resolution			√	I, T, S	√	√	√	All	MITS 14.2 & MG-09 14.1
Incident Management			√	I, T, S	√	√	√	All	MITS 12.4 & 18, MG-09 12 & ITSA-10
Vulnerability Assessments			√	I, T, S	√	√	√	E, S, s, C	MITS 12.5
Patch Management			√	I, T, S	√	√	√	E, S, s, C, A	MITS 12.5.2
IT Continuity Planning			√	I, T, S		√		S, T, A, N	MITS 12.8
IT Security Assessment/Audit			√	I, T, S	√	√	√	All	MITS 12.11 & MG-09 18
Configuration Management			√	I, T, S	√	√	√	All	MITS 14.1 & MG-09 14.3
Change Control			√	I, T, S	√	√	√	All	MITS 14.1
Capacity Planning			√	I, T, S		√		S, A	MITS 14.3
Hardware Maintenance			√	I, T, S	√	√	√	A	MG-09 14.7
Environmental Protection			√	I, T, S		√		A, N	
Power Conditioning/Backup			√	I, T, S		√		S, T, A, N	
Security in Emergencies									GSP 10.13 & RL
Plans and Procedures									
Departmental Plans	√		√	All		√		S, T, A, N	
Testing			√	All		√		S, T, A, N	
Coordination with Other Plans			√	All		√		S, T, A, N	
Resourcing for Sustainability			√	All		√		S, T, A, N	
Business Continuity Planning									GSP 10.14 & BCP
Governance Structure									BCP 3.1 & BCPTD 3
Authorities			√	All		√		S, T, C, A, N	
Responsibilities			√	All		√		S, T, C, A, N	
Business Impact Analysis			√	All		√		S, T, C, A, N	BCP 3.2 & BCPTD 4
Plans/Arrangements			√	All		√		S, T, C, A, N	BCP 3.3 & BCPTD 5
BCP Program Readiness			√	All		√		S, T, C, A, N	BCP 3.4 & BCPTD 6
Review, Testing and Audit			√	All		√		S, T, C, A, N	BCP 3.4 & BCPTD 6
Investigation of Incidents									GSP 10.15 & SIS
Incident Investigation			√	All	√	√	√	All	
Incident Reporting			√	All	√	√	√	All	
Sanctions									GSP 10.16 & SIS
Security Violations		√	√	All	√	√	√	E, S, s, T, C, A	
Security Breaches		√	√	All	√	√	√	E, S, s, T, C, A	

Notes:

1. To help with the selection of suitable security measures, the Safeguard Listing provides a general indication of the risk variables affected by each countermeasure and some useful references as follows:
   - **Column 1** lists Safeguards within Safeguard Groups and Safeguard Classes;
   - **Columns 2-4** indicate which of the three risk variables might be lowered by the safeguard, asset values (A_{Val}), threats (T) or, most frequently, vulnerabilities (V);
   - **Column 5** identifies which classes or categories of assets might be protected by the safeguard, namely personnel (P), information (I), IT systems (T), facilities (F), services (S) or intangible assets (i);
   - **Columns 6-8** suggest which asset values might be protected by the safeguard, specifically confidentiality (C), Availability (A) or integrity (I);
   - **Column 9** points to some of the threat activities or classes mitigated by each safeguard, such as espionage (E), sabotage (S), subversion (s), terrorism (T), criminal acts (C), accidents (A) and natural hazards (N); and
   - **Column 10** provides some references to the GSP, Operational Security Standards and technical documentation that describe the safeguard and its intended use. The entries are keyed to the titles listed below, and some contain pointers to specific sections of the cited reference. For example, GSP 10.1 refers to section 10.1 of the GSP while BCPTD 3 indicates section 3 of the BCP Technical Documentation issued by PSEPC. Sources for this documentation may be found in Appendix G-3, References.

     - **GSP** – Government Security Policy.
     - **OSHP – Occupational Safety and Health Policy**.
     - **Operational Security Standards** –
       - **BCP** – Business Continuity Planning (BCP) Program,
       - **IoA** – Identification of Assets,
       - **MITS** – Management of Information Technology Security,
       - **PS** – Physical Security,
       - **RL** – Readiness Levels for Federal Government Facilities,
       - **SCM** – Security in Contracting Management,
       - **SIS** – Security Investigations and Sanctions,
       - **SS** – Security Screening,
       - **STA** – Security Training and Awareness,
     - **CSE IT Security Alerts, Bulletins, Directives and Guidelines –**
       - **ITSA-09** – COMSEC Equipment Disposal.
       - **ITSA-10** – COMSEC Incident Reporting.
       - **ITSB-02** – Government of Canada Wireless Vulnerability Assessment.
       - **ITSB-03** – Trends in Wireless Technology and Security.
       - **ITSB-06** – CSE Approves Secure BlackBerry.
       - **ITSB-09** – STU-III Operation during a Power Outage.
       - **ITSB-12** – Procurement of the Blackberry Security Module.
       - **ITSB-13** – Key Ordering for STE.
       - **ITSB-15** – Security Vulnerability - Wireless Local Area Network (WLAN) Capable Laptops.

- **ITSB-18** – NATO Recommended Products List (NRPL) - TEMPEST Approved Products.
- **ITSB-19** – Security Measures - Wireless Electronic Devices.
- **ITSB-29** – SECTERA Global System for Mobile Communication Security Module (SGSM) Wireless Standing Offer.
- **ITSD-01** – Directives for the Application of Communications Security in the Government of Canada.
- **ITSD-02** – IT Security Zones Baseline Security Requirements.
- **ITSG-06 –** Clearing and Declassifying Electronic Data Storage Devices.
- **ITSG-10 –** COMSEC Material Control Manual.
- **ITSG-13 –** Cryptographic Key Ordering Manual.
- **ITSG-20** – Windows Server 2003 Recommended Baseline Security.
- **ITSPSR-14 –** Telework Project.
- **ITSPSR-16 –** Personal Communications Services (PCS) and Cellular System Vulnerability Assessment.
- **ITSPSR-17 –** Bluetooth Vulnerability Assessment.
- **ITSPSR-18 –** Personal Digital Assistant Vulnerability Assessment.
- **ITSPSR-19 –** Windows 2000 Pro and Windows XP Pro Recommended Baseline Security.
- **ITSPSR-21 –** 802.11 Wireless LAN Vulnerability Assessment.
- **MG-1 –** Network Security, Analysis and Implementation.
- **MG-2 –** A Guide to Security Risk Management for Information Technology Systems.
- **MG-4 –** A Guide to Certification and Accreditation for Information Technology Systems.
- **MG-9 –** Canadian Handbook on Information Technology Security.

▪ **DFAIT** – Foreign Affairs Travel Warnings.

▪ **Public Safety and Emergency Preparedness Canada –**
- **BCPTD** – Business Continuity Planning Program Technical Documentation.

▪ **Public Works and Government Services Canada –**
- **ISM** – Industrial Security Manual.

▪ **RCMP Physical Security and IT Security Guides, Bulletins and Reports** –
- **G1-001** – Security Equipment Guide,
- **G1-002** – Security Lighting,
- **G1-003** – Glazing,
- **G1-004** – Construction of Special Discussion Areas,
- **G1-005** – Preparation of Physical Security Briefs,
- **G1-006** – Identification Cards/Access Badges,
- **G1-007** – Security Sealing of Building Emergency/Master Keys or Cypher Lock Codes,
- **G1-008** – Guidelines for Guard Services,
- **G1-009** – Standard for the Transport and Transmittal of Sensitive Information and Assets,
- **G1-010** – Security Connotations of the 1995 National Building Code,

- **G1-011** – Overhead Door Specifications,
- **G1-013** – Security Control Room Space Requirements,
- **G1-014** – Exterior Fixed Ladder Barrier Specification
- **G1-015** – Entry Controls for Overhead Doors,
- **G1-016** – Master Key Systems,
- **G1-017** – Hardware,
- **G1-018** – Doors and Frames,
- **G1-019** – Vaults,
- **G1-024** – Control of Access,
- **G1-025** – Protection, Detection and Response,
- **G1-026** – Application of Physical Security Zones,
- **G1-027** – Tenant and Custodian Departments Physical Security Responsibilities,
- **G1-029** – Secure Rooms,
- **G1-030** – Security Awareness Guide,
- **G1-031** – Server Rooms.
- **G2-002** – Guide to Minimizing Computer Theft,
- **G2-003** – Hard Drive Secure Information Removal and Destruction Guidelines,
- **G2-004** – Windows 2000 Professional Advanced Security Configuration Guide,
- **G2-005** – Windows 2000 Active Directory Security Configuration Guide,
- **B2-001** – Suggested DSX Replacement Products,
- **R2-001** – Biometric Technologies,
- **R2-002** – Future Trends in Malicious Code,
- **DSX-G** – RCMP Hard Disk Overwrite Software (DSX) User Manual.

2. The Safeguard Listing should be employed with caution for it cannot be complete and there are exceptions to many entries. It is intended, however, to provide a useful point of departure for analysis during the safeguard selection process in the Recommendations Phase of a TRA project. With that in mind, other material will be added from time to time. Any suggestions for further references may be submitted to the offices identified in the Foreword.

This page intentionally left blank.

Appendix F-3 - Selection of Potential Safeguards

1 General

In order to determine an appropriate array of security measures for the final recommendations in a TRA report several safeguard selection criteria may be applied in two stages:

- firstly, to identify potential solutions for all unacceptable assessed residual risks; and
- secondly, to evaluate their relative effectiveness as risk reduction mechanisms.

Then, in the next TRA process, summarized in Appendix F-4, comparative costs will be calculated to determine the most cost effective options.

2 Identify Potential Solutions

Possible safeguards are identified in six steps as follows:

- **Step 1.** Extract all unacceptable residual risks from the List of Assessed Residual Risks, Appendix E-2.
- **Step 2.** Determine which assets are jeopardized, usually at the asset group or subgroup level, but occasionally considering specific components or individuals, and their values.
- **Step 3.** Determine which threats, normally at the threat activity or threat agent category levels, cause unacceptable risks, and their levels.
- **Step 4.** Determine which vulnerabilities expose these assets to compromising threats, and their levels.
- **Step 5.** To facilitate further analysis, copy these data in an Abbreviated List of Assessed Residual Risks illustrated at Table F3-1. Enter all assets at unacceptable risk in the first column and their values in the second. Then, for each asset, list all associated threats that cause unacceptable risks and their levels in columns three and four respectively. For each of these threats, insert all related vulnerabilities that expose the asset to unacceptable risks and their levels in columns five and six. Finally, unacceptable assessed residual risk levels should be entered in column seven. This task may be accomplished quickly and efficiently by sorting the List of Assessed Residual Risks, Appendix E-2, on the Asset, Associated Threat and Related Vulnerability columns successively.

Assets at Unacceptable Risk		**Threats Causing Unacceptable Risks**		**Vulnerabilities Exposing Assets to Unacceptable Risks**		**R**
Asset	**A_{Val}**	**Threat**	**T**	**Vulnerability**	**V**	

Table F3-1: Abbreviated List of Assessed Residual Risks

- **Step 6.** Knowing which assets, threats and vulnerabilities cause unacceptable residual risks, the Safeguard Listing at Appendix F-2 may be examined to identify potential security measures on the basis of the assets they protect, the threats they address and the vulnerabilities they mitigate.

3 Assess Safeguard Effectiveness

The effectiveness of each prospective safeguard is then assessed in six steps as follows:

- **Step 1.** For certain avoidance mechanisms, specifically those that limit asset values, calculate the difference in levels between the original and the reduced asset values.
- **Step 2.** For any avoidance measures that reduce the likelihood of a threat event, for all deterrent mechanisms that affect threat agent intentions and for any preventive measures that affect threat agent capabilities, assess the overall impact on threat levels.
- **Step 3.** For most preventive measures and all detection, response and recovery mechanisms, determine their effects upon the associated vulnerabilities, either the probability of compromise or the severity of the outcome.
- **Step 4.** Using the revised levels for asset values, threats and vulnerabilities, re-compute residual risks in the Abbreviated List of Assessed Residual Risks to determine whether or not the proposed safeguards achieve acceptable risk levels.
- **Step 5.** For each safeguard that helps reduce unacceptable risks to acceptable levels, consider the implications of secondary selection criteria, specifically its acceptability, visibility, vulnerability, interdependence with other security measures, reliance on human intervention, sensitivity, maturity and conformity to security standards. Any one or more of these factors may influence the final choice between two otherwise acceptable options.
- **Step 6.** All acceptable choices that help achieve target risk levels are then subject to the cost benefit analysis in the next TRA process outlined in Appendix F-4.

4 Example

4.1 Staff Relations Offices

If four staff relations officers in a small government agency were responsible for investigating grievances submitted by employees and recommending appropriate solutions to senior managers, several risks might be identified in a TRA report based upon the following asset values, threats and vulnerabilities:

- **Asset Values.** By definition, the four staff members warrant a High intrinsic value when considering possible threats of violence. Their investigation reports would likely be categorized Protected B, a Medium confidentiality value. Unauthorized modification or tampering with the evidence in these reports would likely cause serious embarrassment to some individuals, so the files would also have a Medium integrity value.
- **Threats.** If other employees had harassed or physically threatened the staff relations officers during subject interviews on two or three occasions during the past year, the threat might be assessed at the Medium level based on the past frequency (100-1,000

days) and threat agent capabilities (moderate knowledge, skill and resources). If other employees had tried to read the files surreptitiously and tamper with their content in the same time frame, the two threats would also be rated at the Medium level.

- **Vulnerabilities.** If the interviews were conducted in open offices, readily accessible to all other employees, the complete ease of access would constitute a very weak preventive mechanism. If this vulnerability were coupled with inadequate detection and response measures, such as poor emergency communications or the lack of an alarm system, unescorted visitors wandering freely through the offices, and a security guard force some distance away, the overall vulnerability rating might be Very High with respect to threats of harassment or assault. The open office and unescorted access would also facilitate the threats of snooping and tampering with sensitive files. If the staff relations officers were prone to leave the offices unattended or unsupervised, the likelihood of detecting unauthorized disclosure might be quite small. Without some integrity checks, it might be equally difficult to detect unauthorized modification of the reports and recommendations. In both cases, the inability to detect and respond to possible threats linked with inadequate access controls, would constitute Very High level vulnerabilities.
- **Assessed Residual Risks.** In each case, the assessed residual risks associated with these asset values, threats and vulnerabilities fall within the High range, an unacceptable level. This assessment should be presented in a Safeguard Selection Worksheet as explained in Steps 1 through 5 of the first stage of the safeguard selection process and illustrated in Table F3-2, a List of Unacceptable Assessed Residual Risks.

Assets at Unacceptable Risk				**Threats Causing Unacceptable Risks**		**Vulnerabilities Exposing Assets to Unacceptable Risks**		**R**
Asset	**A_{Val}**			**Threat**	**T**	**Vulnerability**	**V**	
	C	**A**	**I**					
Staff Relations Officers		H		Harassment/Assault	M	Open Office	VH	H
		H			M	No Alarm	VH	H
		H			M	No Response Force	VH	H
Grievance Files	M			Employee Snooping	M	Open Office	VH	H
	M				M	Unsupervised Access	VH	H
			M	Evidence Tampering	M	Open Office	VH	H
			M		M	Unsupervised Access	VH	H
			M		M	Weak Integrity Checks	VH	H

Table F3-2: List of Unacceptable Assessed Residual Risks

4.2 Identify Potential Solutions

Once the unacceptable assessed residual risks have been isolated for examination, the Safeguard Listing at Appendix F-2 might be examined to identify possible security measures to protect the assets at risk, namely staff relations officers (personnel) and grievance files (documents with both confidentiality and integrity values), against the known threats of violence in the workplace, eavesdropping and evidence tampering, and address the related vulnerabilities. In this particular case, relevant considerations include:

- **Asset Values.** Given the nature of the assets, both personnel and sensitive documents, avoidance measures cannot be introduced to limit asset values.
- **Threats.** Some safeguards, such as warning signs, might deter violent employees and those seeking to read or modify grievance files, but little can be done to affect their capabilities based on their knowledge, skills and resources.
- **Vulnerabilities.** Quite clearly, in this case, the most profitable approach is to address the varied vulnerabilities, the weak prevention, detection and response mechanisms that contribute to unacceptable residual risks.
- **Potential Safeguards.** Some options might include safeguards listed in Table F3-3, and described below during the evaluation of safeguard effectiveness.

4.3 Evaluate Safeguard Effectiveness

The presence of security guards on site might have some deterrent value, even though the actual impact on threat agent intentions may be difficult to measure accurately. Otherwise, the prospective safeguards do not reduce asset values or threats, only vulnerabilities, either the probability of compromise or the severity of the outcome. Thus, the overall reduction in vulnerability levels is the primary indicator of safeguard effectiveness in this particular scenario. Furthermore, to achieve projected residual risks in the Medium range, a generally acceptable level, proposed safeguards should reduce all Very High vulnerabilities with respect to harassment and assault to a Low level and those for snooping and tampering to a Medium level. The expected impact of each security measure is explored briefly below.

- **Locked Entry.** A locked door at the entrance to the staff relations office space is a moderately effective preventive measure, limiting access to both personnel and grievance files. Without a complementary improvement in detection, response and recovery, however, this simple access control mechanism might reduce the overall vulnerability from Very High (High probability of compromise and High outcome severity) to High (Medium probability of compromise, but still a High outcome severity). When coupled with other safeguards, especially staff training, a duress alarm and a qualified response force, the overall vulnerability could drop to a Medium or possibly a Low level.
- **Escorted Access.** The locked entrance can only be moderately effective as a prevention mechanism because legitimate clients must be admitted to the area for interviews and counselling, where they might harass the staff or try to access the grievance files. Escorting all guests throughout their visits could prevent most snooping and tampering, but probably not harassment or threats of violence. Supervised access also provides an effective detection and response capability to all three threats. Therefore, as a detection and response measure, this safeguard alone could reduce the vulnerability to harassment and assault from a Very High level (High probability of compromise and High outcome severity) to High or possibly Medium (still a High probability of compromise, but now a Medium or perhaps Low outcome severity). Since it serves as a preventive measure as well as a detection and response mechanism with respect to snooping and tampering, escorted access is even more effective against these threats, reducing the associated vulnerabilities to a Very Low level (Low likelihood of compromise and Low outcome severity). Of course, the effectiveness of this safeguard might diminish over time if the escorts were to relax their vigilance.

- **Staff Training.** Staff training and awareness to recognize, report and counter real and potential problems is essential to ensure effective application of other safeguards, such as a locked entrance, escorted access and a clear desk policy. Therefore, the ultimate impact of this training on vulnerability levels is best reflected in an assessment of the relative effectiveness of other safeguards that depend upon staff intervention and implementation.

Safeguard Options	Security Functions	Assets Protected	Threats Mitigated	Vulnerabilities Addressed
Locked Entry	Prevention	Employees	Harassment/Assault	Open Office
		Grievance Files	Snooping	Open Office
		Grievance Files	Tampering	Open Office
Escorted Access	Prevention	Grievance Files	Snooping	Unsupervised Access
		Grievance Files	Tampering	Unsupervised Access
	Detection	Employees	Harassment/Assault	No Alarm
		Grievance Files	Snooping	Unsupervised Access
		Grievance Files	Tampering	Unsupervised Access
	Response	Employees	Harassment/Assault	No Response Force
		Grievance Files	Snooping	No Response Force
		Grievance Files	Tampering	No Response Force
Staff Training	Prevention	Employees	Harassment/Assault	Unsupervised Access
		Grievance Files	Snooping	Unsupervised Access
		Grievance Files	Tampering	Unsupervised Access
	Detection	Employees	Harassment/Assault	No Alarm
		Grievance Files	Snooping	Unsupervised Access
		Grievance Files	Tampering	Unsupervised Access
	Response	Employees	Harassment/Assault	No Response Force
		Grievance Files	Snooping	No Response Force
		Grievance Files	Tampering	No Response Force
Clear Desk Policy	Prevention	Grievance Files	Snooping	Unsupervised Access
		Grievance Files	Tampering	Unsupervised Access
Secure Interview Rooms	Prevention	Employees	Harassment/Assault	Open Office
Duress Alarm	Detection	Employees	Harassment/Assault	No Alarm
Security Guard On Site	Deterrence	Employees	Harassment/Assault	Unsupervised Access
		Grievance Files	Snooping	Unsupervised Access
		Grievance Files	Tampering	Unsupervised Access
	Prevention	Employees	Harassment/Assault	Unsupervised Access
	Detection	Employees	Harassment/Assault	No Alarm
	Response	Employees	Harassment/Assault	No Response Force
		Grievance Files	Snooping	No Response Force
		Grievance Files	Tampering	No Response Force
Security Guard On Call	Response	Employees	Harassment/Assault	No Response Force
		Grievance Files	Snooping	No Response Force
		Grievance Files	Tampering	No Response Force
Close Circuit TV	Detection	Employees	Harassment/Assault	No Alarm
File Folio Numbers	Detection	Grievance Files	Tampering	Weak Integrity Checks
Duplicate Files	Recovery	Grievance Files	Tampering	Weak Integrity Checks

Table F3-3: List of Potential Safeguards

- **Clear Desk Policy.** A clear desk policy, requiring employees to lock sensitive files in security containers when not in immediate use, is a simple but effective means to prevent unauthorized access for snooping or tampering. Even without complementary detection and response measures, this safeguard could reduce the vulnerability from Very High (High probability of compromise and High outcome severity) to Medium (a Low probability of compromise, but still a High outcome severity). Since it does impose some inconvenience, staff may baulk at these procedures, or fail to comply conscientiously, thereby undermining their effectiveness.
- **Secure Interview Rooms.** With shatterproof glass partitions and separate entrances for clients and staff, secure interview rooms are very effective safeguards to prevent physical abuse. Their solid construction also helps contain the damage in the event of a confrontation, a partial response mechanism, thereby reducing the vulnerabilities to harassment and assault from Very High (High probability of compromise and High outcome severity) to Low (a Low probability of compromise, and a Medium outcome severity). If a duress alarm were also installed to alert a rapid response force, the ultimate vulnerabilities might be rated Very Low.
- **Security Guard on Site.** Installing a security guard in the staff relations office space could address several vulnerabilities related to threats of harassment and assault. With proper training, for example, the guard might recognize potentially dangerous situations and stop suspicious individuals or help calm agitated visitors, very effective preventive measures. The guard could also perform detection and response functions to mitigate any injuries arising from abusive or violent clients. Thus, the overall vulnerabilities could be reduced from Very High (High probability of compromise and High outcome severity) to Low or perhaps Very Low (a Low probability of compromise, and a Medium or Low outcome severity).
- **Security Guard on Call.** Clearly a security guard on call is less effective than one located in the staff relations office area for several reasons. Firstly, a remote guard serves neither prevention nor detection functions. Secondly, the guard only provides a response capability, if there is some other detection mechanism to raise an alert. Finally, the response is likely to be slower and less effective, depending upon the location of the guard post. If it were implemented in conjunction with a moderately effective prevention measure, such as a locked entrance, and a detection mechanism, such as a duress alarm, the response from a centralized security guard post could help reduce the overall vulnerability to violence in the workplace from Very High (High probability of compromise and High outcome severity) to the Medium level (a Medium probability of compromise, and a Medium outcome severity).
- **Closed Circuit TV.** Provided that it is monitored from a central guard post, a closed circuit television (CCTV) system could provide a very effective detection mechanism, especially with respect to agitated or potentially abusive clients. Coupled with a rapid response capability, the two safeguards would not prevent cases of harassment or assault, but they could help contain the any incident, reducing the severity of the outcome from a High to a Medium or perhaps even a Low level. If a complementary preventive measure, such as the locked entrance, were to reduce the probability of compromise from a High to a Medium level, the overall vulnerability might drop from Very High to Medium or Low. Notwithstanding the potential effectiveness of CCTV equipment, privacy concerns and employee resistance to continuous monitoring may mitigate against its installation.

- **File Folio Numbers.** The use of sequential folio numbers for each entry in the grievance files cannot prevent tampering, but the practice could help detect certain alterations, such as the removal of important evidence. Without matching preventive measures, however, this moderately effective safeguard could only reduce the associated vulnerability from Very High (High probability of compromise and High outcome severity) to High (still a High probability of compromise, with a Medium outcome severity). Furthermore, staff relations officers may find the procedures cumbersome and time-consuming, and resist their implementation.
- **Duplicate Files.** While folio numbers may help detect unauthorized modification of grievance files, they do little to facilitate recovery after an incident actually arises. The maintenance of parallel or duplicate files could be reasonably effective as a backup and recovery strategy. Again, like folio numbers, their impact on the associated vulnerability would be limited without a corresponding preventive measure. Duplicate files are also susceptible to integrity problems, where the two versions do not match, if they are not scrupulously maintained.

4.4 Summary of Options

In order to achieve the target risk levels, a significant reduction in vulnerabilities will be necessary, from Very High to at least Medium, as noted above. With this aim in mind, complementary safeguards should be selected to reduce both the probability of compromise with preventive measures, and the severity of the outcome with detection, response and perhaps recovery mechanisms. The following combinations of security measures from Table F3-3, all of which must include relevant security training, could satisfy these requirements:

- **Locked Entrance with Escorted Access.** Working together, these safeguards would be moderately effective as preventive measures against harassment and assault (Medium probability of compromise) and very effective with respect to snooping and tampering (Low probability of compromise). At the same time, the escorted access and security training could provide effective detection and response capabilities for all threats (Low outcome severity) with the possible exception of harassment and assault where an employee might be reluctant to intervene beyond calling for help. In that case, the vulnerability would revert to the Medium level (Medium probability of compromise and Medium outcome severity). Taking each of these issues into consideration, overall vulnerabilities to harassment and assault would drop to the Low or Medium range and those to snooping and tampering to Very Low. The projected residual risks if these safeguards were approved and implemented are summarized in Table F3-4.

Assets at Unacceptable Risk		Threats Causing Unacceptable Risks		Vulnerabilities Exposing Assets to Unacceptable Risks		R
Asset	**A_{Val}**	**Threat**	**T**	**Vulnerability**	**V**	
Staff Relations Officers	H	Harassment/Assault	M	Open Office	L-M	M-H
	H		M	No Alarm	L-M	M-H
	H		M	No Response Force	L-M	M-H
Grievance Files	M	Employee Snooping	M	Open Office	VL	L
	M		M	Unsupervised Access	VL	L
	M	Evidence Tampering	M	Open Office	VL	L
	M		M	Unsupervised Access	VL	L

Table F3-4: Projected Residual Risks with a Locked Entrance and Escorted Access

- **Adding a Duress Alarm and Security Guard on Call.** If employee intervention in the event of harassment or assault were a significant concern with the previous option, a duress alarm might be added to alert a trained security guard and provide a more effective response capability, reducing vulnerabilities to a Low level (Medium probability of compromise and Low outcome severity), with the results noted in Table F3-5.

Assets at Unacceptable Risk		Threats Causing Unacceptable Risks		Vulnerabilities Exposing Assets to Unacceptable Risks		R
Asset	**A_{Val}**	**Threat**	**T**	**Vulnerability**	**V**	
Staff Relations Officers	H	Harassment/Assault	M	Open Office	L	M
	H		M	No Alarm	L	M
	H		M	No Response Force	L	M
Grievance Files	M	Employee Snooping	M	Open Office	VL	L
	M		M	Unsupervised Access	VL	L
	M	Evidence Tampering	M	Open Office	VL	L
	M		M	Unsupervised Access	VL	L

Table F3-5: Projected Residual Risks Adding a Duress Alarm and Security Guard on Call

- **Security Guard On Site, Clear Desk Policy and Folio Numbers.** A properly trained security guard could address all vulnerabilities related to harassment and assault very effectively as both a prevention, and a detection and response mechanism, to reduce the level from Very High (High probability of compromise and High outcome severity) to Very Low (Low probability of compromise and Low outcome severity). The clear desk policy could prevent most snooping and tampering with grievance files, while folio numbering might be moderately effective to detect unauthorized modifications, so the vulnerabilities related to snooping could drop from Very High (High probability of compromise and High outcome severity) to Medium (Low probability of compromise but still High outcome severity) and those for tampering from Very High (High probability of compromise and High outcome severity) to Low (Low probability of compromise and Medium outcome severity). These impacts are reflected in Table F3-6.

Assets at Unacceptable Risk		Threats Causing Unacceptable Risks		Vulnerabilities Exposing Assets to Unacceptable Risks		R
Asset	**A_{Val}**	**Threat**	**T**	**Vulnerability**	**V**	
Staff Relations Officers	H	Harassment/Assault	M	Open Office	VL	L
	H		M	No Alarm	VL	L
	H		M	No Response Force	VL	L
Grievance Files	M	Employee Snooping	M	Open Office	M	M
	M		M	Unsupervised Access	M	M
	M	Evidence Tampering	M	Open Office	L	M
	M		M	Unsupervised Access	L	M

Table F3-6: Projected Residual Risks with Security Guard, etc.

- **Secure Interview Rooms.** A secure interview room might replace the security guard in the previous option with the same impact on vulnerabilities related to harassment and assault, namely a reduction from Very High (High probability of compromise and High outcome severity) to Very Low (Low probability of compromise and Low outcome severity). A clear desk policy and folio numbering could address vulnerabilities related to snooping and tampering. This combination would achieve the same overall impact on vulnerabilities and projected residual risks as the previous option in Table F3-6.
- **Closed Circuit Television (CCTV) Equipment.** As a detection measure, CCTV equipment could not reduce the vulnerabilities to harassment and assault without a complementary response mechanism, such as a trained guard force. The duress alarm in the second option achieves the same results with greater reliability, so CCTV monitoring need not be considered during the subsequent assessment of safeguard cost effectiveness.

4.5 Conclusion

The four options described above represent reasonable groupings of safeguards, both preventive measures and detection and response mechanisms. Clearly, these are not the only possibilities, but simply realistic combinations, all of which achieve or surpass the targeted range for residual risks, namely a Medium level or lower. The best choice will be determined during the next process in the Recommendations Phase of a TRA project, the identification of associated costs and assessment of cost effectiveness, amplified in Appendix F-4.

This page intentionally left blank.

Appendix F-4 - Calculation of Safeguard Cost Effectiveness

1 General

In order to determine which of the options identified in the preceding TRA process, the Selection of Potential Safeguards, provides the best value for money, a cost benefit analysis may be applied in two stages:

- firstly, to estimate the total cost of ownership for each combination of safeguards; and
- secondly, to calculate their cost effectiveness based upon the overall risk reduction for every dollar expended.

Then, the most cost-effective solutions may be presented in the final recommendations for management consideration and approval, funding and subsequent implementation as described in Appendix F-5.

2 Determine Total Cost of Ownership

The total cost of ownership for each viable option is projected in three steps as follows:

- **Step 1.** Calculate the direct costs associated with proposed safeguards, including design and development, acquisition, integration, installation, documentation, training, ongoing operation and maintenance expenses, as appropriate.
- **Step 2.** Estimate the indirect costs and benefits attributed to the proposed security measures based upon reduced productivity and improved efficiency respectively.
- **Step 3.** Compute the sum of all direct and indirect costs or benefits as the total cost of ownership for each proposal.

3 Assess Safeguard Cost Effectiveness

Compute the comparative cost effectiveness of each of these options in three steps, as follows:

- **Step 1.** Assess the life expectancy of the proposed safeguard and compute the amortized annual cost, the quotient of total cost of ownership divided by life expectancy.
- **Step 2.** Calculate the total risk reduction for each potential security measure by –
  - selecting all unacceptable risk combinations (asset value, threat and vulnerability) from Appendix E-2 that are moderated by the proposed safeguard;
  - re-computing the residual risk for each of these entries, based upon the lower asset value, threat or vulnerability achieved with the proposed safeguard;
  - determining the number of levels between the assessed and projected residual risks for each combination affected by the proposed safeguard; and
  - calculating the total risk reduction, namely the sum of all the changes in risk levels.

- **Step 3.** Compute the cost effectiveness of each proposal, the quotient of amortized annual cost divided by total risk reduction.

4 Example

4.1 Staff Relations Offices

The example presented in Appendix F-3 to illustrate the selection of potential safeguards to protect staff relations officers and their grievance files may be completed with the following assessment of the associated costs and cost effectiveness for each of the following options:

- **Option 1.** Locked entrance with escorted access and security training.
- **Option 2.** Adding a duress alarm and security guard on call to Option 1.
- **Option 3.** Security guard on site with clear desk policy and folio numbers.
- **Option 4.** Substitute secure interview rooms for the security guards in Option 3.

4.2 Total Cost of Ownership

Typical and representative costs associated with each of the four options are summarized in Table F4-1 below.

Costs	Option 1	Option 2	Option 3	Option 4
Design/Development	–	–	–[1]	$5,000[2]
Acquisition	$500[3]	$1,300[4]	$750[5]	$10,400[6]
Integration	–	–	–	–
Installation	$250[7]	$850[8]	$150[9]	$16,300[10]
Documentation	$300[11]	$500[12]	$300[13]	$200[14]
Training	$400[15]/$100[16]	$500[17]/$125[18]	$200[19]/$100[20]	$100[21]/$25[22]

1 Assuming there is space at the entrance to set up a guard station and no redesign is necessary.
2 To produce architectural plans and designs.
3 To purchase an electronic key pad door lock to facilitate access by staff relations officers.
4 To purchase both an electronic key pad door lock and four duress alarms.
5 To purchase a desk, chair, telephone and other office equipment for the security guard.
6 To purchase two duress alarms and the material to construct two secure interview rooms.
7 To install the key pad electronic door lock.
8 To install the key pad electronic door lock and four duress alarms.
9 To connect the telephone and move the furniture.
10 To construct two secure interview rooms and install two duress alarms.
11 Salary for a security analyst to document the access control and emergency response procedures.
12 Salary for a security analyst to document the access control and added emergency response procedures.
13 Salary for a security analyst to document the access control and emergency response procedures.
14 Salary for a security analyst to document emergency response procedures.
15 Salaries for security analyst and staff relations officers for initial training on equipment and procedures.
16 Annual training costs for new employees, assuming complete turnover every four years.
17 Salaries for a security analyst and staff relations officers for initial training on equipment and procedures.
18 Annual training costs for new employees, assuming complete turnover every four years.
19 Salaries for a security analyst and the security guards for initial training on emergency procedures.
20 Annual training costs for new security guards, assuming complete turnover every other year.
21 Salaries for a security analyst and staff relations officers for initial training on emergency procedures.

Ongoing Operation	–	–[23]	$37,500[24]	–
Maintenance	$100[25]	$200[26]	–	$300[27]
Reduced Productivity	–[28]	–[29]	$2,800[30]	–
Improved Efficiency	–	–	–[31]	–[32]
Total One-Time Costs	$1,450[33]	$3,150[34]	$1,400[35]	$32,000[36]
Recurring Annual Costs	$200[37]	$325[38]	$40,400[39]	$325[40]

Table F4-1: Initial and Recurring Direct and Indirect Costs

4.3 Safeguard Cost Effectiveness

The relative cost effectiveness of each option is calculated in three steps as follows:

- **Amortized Annual Costs.** While durable items, such as the secure interview rooms might be expected to last almost indefinitely, organizational changes occur rather more frequently, so a ten year life span for each of the options seems more realistic, perhaps even slightly optimistic, to calculate the amortized annual costs in Table F4-2. It is noteworthy that, as the projected life span of the safeguards increases, the amortized annual cost for option 4 decreases significantly because it is capital intensive with larger initial expenditures. On the other hand, the total cost of ownership for option 3 continues to increase steadily due to the ongoing annual salaries.

- **Total Risk Reduction.** The total risk reduction for each option may be calculated very easily by comparing the projected residual risks in Tables F3-4 to F3-6 of Appendix F-3

22 Annual training costs for new employees, assuming complete turnover every four years.
23 Assuming that a central guard post already exists in the building, there are no incremental salary costs for one of the guards to respond to any alarms.
24 Based on an hourly wage of $15 for a security guard from 7:30 a.m. to 5:30 p.m. daily every workday.
25 Annual maintenance check for the electronic key pad door lock.
26 Annual maintenance check for the electronic key pad door lock and duress alarms.
27 Annual maintenance check for the secure interview rooms and duress alarms.
28 While the requirement to escort visitors will have some adverse impact on productivity, it is likely to be offset by improved morale due to an increased sense of security.
29 Again, the requirement to escort visitors will have some adverse impact on productivity, but it is likely to be offset by improved morale due to an increased sense of security.
30 Imposing a clear desk policy and the use of folio numbers will increase the workload for the staff relations officers by a small amount, in the order of one percent.
31 While productivity might increase due to improved morale and a better sense of security, the actual benefits are difficult to project.
32 While productivity might increase due to improved morale and a better sense of security, the actual benefits are difficult to project.
33 The acquisition, installation, documentation and initial training costs.
34 The acquisition, installation, documentation and initial training costs.
35 The acquisition, installation, documentation and initial training costs.
36 The design and development, acquisition, installation, documentation and initial training costs.
37 The annual maintenance checks and training costs for new employees.
38 The annual maintenance checks and training costs for new employees.
39 The security guard's salary and benefits, annual training costs for new employees and lost productivity due to the imposition of a clear desk policy and the use of folio numbers.
40 The annual maintenance checks and training costs for new employees.

with the initial assessed residual risks in Table F3-2. The decrease is then entered in Table F4-2 below.

- **Safeguard Cost Effectiveness.** The relative cost effectiveness of each option is measured as the annual expenditure for every level of risk reduction listed in the final row of Table F4-2.

Cost Effectiveness	Option 1	Option 2	Option 3	Option 4
Life Expectancy	10 years	10 years	10 years	10 years
Amortized Annual Cost	$345	$640	$40,540	$3,525
Total Risk Reduction	8/11[41]	11	10	10
Cost Effectiveness	$43.13/$31.36	$58.18	$4,054.00	$352.50

Table F4-2: Calculation of Safeguard Cost Effectiveness

4.4 Conclusion

Although Option 1 provides a more cost effective solution than the other three, there remains some doubt about its effectiveness with respect to the threats of harassment and assault, because employees might be reluctant to intervene. If that were the case, this option could not achieve the targeted residual risk, namely a Medium level. Therefore, prudence dictates the selection of Option 2 which is only marginally less cost effective, but does achieve the requisite risk reduction. Options 3 and 4 also achieve acceptable results but at much greater costs for each level of risk reduction. For the final TRA report, the data captured above for Option 2 should be transferred to a Recommendations Table illustrated at Appendix F-5.

Note:

The costs presented in this example are not necessarily complete or definitive. They are offered rather as examples to illustrate the calculation of cost effectiveness in support of the final recommendations in a TRA report.

[41] The lower number (8) represents a more cautious assessment where other employees may be reluctant to intervene in cases of harassment or assault, while the second number (11) reflects the greater risk reduction if they were to provide an effective response capability.

Appendix F-5 - Recommendations Table

Recommendation No. 1:													
Related Costs													
Direct Costs					**Indirect Costs/Benefits**		**Total Cost of Ownership**						
Design	**Acquisition**	**Installation**	**Operation**	**Other**	**Reduced Productivity**	**Increased Efficiency**							
Life Expectancy	**Amortized Annual Cost**	**Safeguard Interdependencies**	**1.**										
			2.										
			3.										
Unacceptable Assessed Residual Risks								**Projected Residual Risks**					
Asset	**A_{Val}**	**Threat**	**T**	**Vulnerability**	**V**	**R**		**Asset**	**A_{Val}**	**Threat**	**T**	**Vulnerability**	**V**	**R**
Safeguard Cost Effectiveness														
Total Risk Reduction (Levels)								**Cost Effectiveness ($/Level)**						
Other Considerations														

1 Instructions

The Recommendations Table provides a convenient form to capture the analysis supporting each of the proposals intended to reduce unacceptable residual risks to an acceptable level. The relevant information should be entered as follows:

- **Step 1.** Prepare a separate form for each recommendation, numbered in sequence from the most cost effective to the least. Provide a brief description in the first cell of the table, something like: "Install an intrusion alarm with magnetic sensors on all doors and windows, and infrared motion detectors and glass break sensors in each room."
- **Step 2.** Itemize all related costs, both direct and indirect, and compute the total cost of ownership in accordance with sections 4.2 and 4.3 of Annex F.
- **Step 3.** Assess the life expectancy of the proposed safeguard in years.
- **Step 4.** Calculate the amortized annual cost of the recommended safeguard in accordance with section 4.4.2 of Annex F. **Note:** If any dependencies are identified in Step 5 and there are costs associated with the implementation and operation of the related safeguard(s), the amortized annual cost of the two, or more, linked security measures should be combined to compute their overall cost effectiveness in Step 9.
- **Step 5.** List any interdependencies with other existing or proposed safeguards in accordance with section 3.3.8 of Annex F. This is particularly important because the effectiveness of one recommendation may be contingent on the implementation of another related security measure. If it were not approved, the resulting residual risks may not be acceptable. To continue with the example of an intrusion alarm noted above, the presence of a response force, either security guards or the local police would be an essential interdependency.
- **Step 6.** Transfer all of the unacceptable risk combinations that would be addressed by the recommended safeguard from the List of Assessed Residual Risks at Appendix E-2.
- **Step 7.** Enter the revised asset values or threat and vulnerability levels achieved with the recommended safeguard, and compute the projected residual risk in accordance with section 5 of Annex F.
- **Step 8.** Compare the assessed and projected residual risk levels for each entry and count the total risk reduction in levels in accordance with section 4.4.3 of Annex F.
- **Step 9.** Compute the relative cost effectiveness of the recommended safeguard in accordance with section 4.4.4 of Annex F.
- **Step 10.** Note any additional considerations, such as the availability of the proposed safeguard, its acceptability, any training concerns and its compliance with mandatory standards or recognized best practices.

2 Example

If the installation of an intrusion alarm system were proposed to protect bearer bonds and sensitive financial records in a government registry from thieves and industrial spies respectively, the relevant Recommendation Table entry might be completed as follows:

Recommendation No. 1:

Install an intrusion alarm with magnetic sensors on all doors and windows in the central registry office. Install infrared motion detectors and glass break sensors in rooms A-101 and A-103.

Related Costs

Direct Costs					Indirect Costs/Benefits		Total Cost of Ownership
Design	**Acquisition**	**Installation**	**Operation**	**Other**	**Reduced Productivity**	**Increased Efficiency**	
-	$2,000	$1,500	$750/yr[1]	$250[2]			

Life Expectancy	**Amortized Annual Cost**	**Safeguard Interdependencies**
10[6]	$1,125[7]	1. Registry walls are already solidly constructed.[3] 2. Recommend doors be reinforced/windows barred.[4] 3. Bearer bonds and sensitive documents are stored in safes.[5] 4. Local police can respond in 10 minutes or less.[8]

Unacceptable Assessed Residual Risks							**Projected Residual Risks**						
Asset	**A_{Val}**	**Threat**	**T**	**Vulnerability**	**V**	**R**	**Asset**	**A_{Val}**	**Threat**	**T**	**Vulnerability**	**V**	**R**
bonds	H	thieves	H	accessibility no detection	H	H	bonds	H	thieves	H	accessibility no detection	L	M
sensitive documents	M	industrial espionage	H	accessibility no detection	H	H	sensitive documents	M	industrial espionage	H	accessibility no detection	L	M

Safeguard Cost Effectiveness

Total Risk Reduction (Levels)	4	**Cost Effectiveness ($/Level)**	$381[9]

Other Considerations

1. Although the intrusion alarm system might be expected to last for more than ten years, it is assumed that the registry is likely to be reorganized or moved at least that often, thereby necessitating a replacement system.

1 Assuming a monthly monitoring fee of $60 and an annual maintenance inspection at $150.

2 One time training costs for ten employees.

3 This related safeguard is a preventive measure to slow down forceful entry. It is already in place, so there are no additional expenses to affect the overall amortized annual cost of the recommendation.

4 The doors and windows are not currently reinforced so a determined intruder could break in and make off with either bearer bonds or sensitive documents in a few minutes. In this case, the added cost of $4,000 to install these preventive measures should be included in the final calculation of cost effectiveness.

5 The safes, another preventive measure, could be expected to delay unauthorized access to the contents for about fifteen minutes after unauthorized entry. Again, there is no added cost because they already exist.

6 Although the intrusion alarm system might last for more than ten years, it is assumed that the registry is likely to be reorganized or moved every ten years, necessitating a replacement system. These assumptions might be stated under Other Considerations.

7 Calculated as follows: acquisition, installation and other costs plus ten times the annual operating costs divided by the life expectancy; or $2,000 + $1,500 + $250 = $3,750 + (10 × $750) ÷ 10 = $1,125.

8 Local police provide the necessary response capability, without which the installation of an intrusion alarm system, a detection mechanism, would be virtually useless.

9 Based on the original amortized annual cost of $1,125 adjusted by $400 to reflect the cost of reinforcing the doors and windows divided by the four levels of risk reduction.

This page intentionally left blank.

Appendix F-6 - Outline TRA Report

Outline TRA Report	Cross-References

Executive Summary
 	
• Recommended for all but the shortest TRA reports.
• Presented in one or two pages to describe:
  o the purpose and subject of the assessment;
  o assessed residual risks that are unacceptable;
  o the primary recommendations;
  o the estimated cost of all recommendations; and
• the projected residual risks once the recommendations have been approved and implemented.	

Background
 	
• Identify the organization or department.
• Provide some context for the TRA project with a description of:
  o the business line and its operating environment;
  o service delivery levels and obligations;
  o the rationale for a new facility or IT system; or
  o the specific security problem to be addressed.
• The actual content will vary according to the subject and purpose of the assessment.
	Appendix A-6, Section 1, Background.

Aim • State the purpose of the TRA project in a single sentence.	Annex A, Section 4.2.2, Purpose of the Assessment.
Mandate • Briefly summarize the authority of the TRA team. • Attach a copy of any written instructions. • Attach a copy of the approved TRA Work Plan.	Annex A, Section 3, Mandate of the TRA Project. Appendix A-6, Sample TRA Work Plan.

Scope
 	
• Identify the subject of the TRA project.
• Define the bounds of the assessment, indicating:
  o what falls within the scope of the TRA project; and
  o which related assets do not.
• Use schematic diagrams or floor plans to illustrate the scope.
	Annex A, Section 4, Scope of Assessment.

Outline TRA Report	Cross-References

• Note any related TRA reports:
  o describe their relationship with the current assessment; and
  o list them in an attachment.	

Asset Identification and Valuation
 	
• Describe the more important:
  o assets, both tangible and intangible, normally at the group or subgroup level;
  o employees who rely upon these assets to perform their jobs;
  o the services they provide; and
  o the injuries that might arise in the event of compromise.
• In general, a short paragraph should suffice for each entry.
• Summarize other items in the Asset Valuation Table/Statement of Sensitivity, which should be attached as an annex.
	Annex B, Asset Identification and Valuation Phase.
	
	Appendix B-5, Asset Valuation Table.

Threat Assessment • Describe the more serious threats, normally at the activity or agent category level of detail. • Indicate the assets affected and the likely types of compromise. • Again, a short paragraph should suffice for each entry. • Summarize other items in the Threat Assessment Table, which should be attached as an annex.	Annex C, Threat Assessment Phase. Appendix C-4, Threat Assessment Table.
Vulnerability Assessment. • Describe serious vulnerabilities, usually at the group level. • Indicate the assets affected and the threats facilitated. • Avoid too much technical detail in the body of the report. • Again, a short paragraph should suffice for each entry. • Summarize other items in the Vulnerability Assessment Table, which should be attached as an annex.	Annex D, Vulnerability Assessment. Appendix D-4, Vulnerability Assessment Table.

Risk Assessment.
• Describe all assessed residual risks that are unacceptable
• To streamline the assessment:
  o concentrate on the more serious risks; and
  o consolidate as many as possible into broad groupings.
• Again, a short paragraph should suffice for each entry.
• Summarize other items in the List of Assessed Residual Risks, which should be attached as an annex.
	Annex E, Calculation of Residual Risk.
	
	Appendix E-2, List of Assessed Residual Risks.

Recommendations. • Summarize each of the recommendations, including their costs. • Present the projected residual risk. • Capture the details in an annex.	 Annex F, Recommendations Phase. Appendix F-5.
Attachments • Some of the following may not be relevant in every case: o Mandate of the TRA Project (where stated explicitly). o TRA Work Plan (including a list of all TRA team members). o Related TRA Reports (where applicable). o Asset Valuation Table/Statement of Sensitivity. o Threat Assessment Table. o Vulnerability Assessment Table. o List of Assessed Residual Risks. o Recommendations Table. o Personnel Interviewed and Sites Visited. o Reference Documents, including – ▪ Relevant Federal Statutes, ▪ Government and Departmental Policies/Directives, ▪ Security Standards and Guidelines, ▪ Design Documentation, ▪ Site Plans, ▪ Vendor Manuals, for both Users and Operators, ▪ Incident Reports/Threat Assessments, ▪ Product Evaluation Reports, ▪ Vulnerability Assessments, ▪ Security Test and Evaluation Reports	 Appendix A-6. Appendix B-5. Appendix C-4. Appendix D-4. Appendix E-2. Appendix F-5

This page intentionally left blank.

Appendix F-7 - Sample TRA Report

1 Background

The Internal Affairs Division (IAD) in the Corporate Services Branch conducts preliminary inquiries into allegations of fraud, industrial espionage and other offences against departmental assets in order to determine whether there are grounds for the local police to initiate a criminal investigation. Given the sensitivity of some cases, certain files are categorized Protected C. Section 16.4.9 of the Management of Information Technology Security (MITS) Operational Security Standard states: "In Canada, departments should use TEMPEST protection for Top Secret and Protected C information when justified by a Threat and Risk Assessment."

2 Aim

The aim of this TRA project is to determine whether the IAD local area network requires TEMPEST protection.

3 Mandate

The TRA Work Plan, attached at Annex A, indicates that the TRA team, with representatives from IAD, the IT Security Coordinator and the Chief Information Officer Branch, is tasked to assess the emanations security risk and recommend one of the four alternatives outlined in section 3.3 of ITSG-12, *Government of Canada Facility Evaluation Procedures*.

4 Scope

IAD is to be provided with a standalone local area network comprising ten workstations and a single server on the 3rd floor of the headquarters building for processing classified and protected information. All physical, personnel and IT security measures recommended in TRA Report 41/05 have been or will be implemented and tested so, apart from the question of TEMPEST protection, the system is ready for final certification and accreditation.

5 Asset Identification and Valuation

IAD conducts approximately 150 inquiries annually. While most of the reports are categorized Protected B, a small number involving industrial espionage are classified Secret. About 20% of the files are categorized Protected C because unauthorized disclosure could reasonably be expected to endanger the lives of confidential sources and jeopardize legal proceedings against organized criminal groups responsible for fraudulent acts often in excess of $10 million. Thus, the information assets within the scope of this assessment are assigned a **High** value.

6 Threat Assessment

During the past year, organized criminal gangs have tried to subvert departmental employees to gain access to IAD files on at least three occasions. Thus, the likelihood of future occurrence is rated **High**. Although the criminal element has extensive financial resources, they have not demonstrated the knowledge and skill required to conduct a TEMPEST attack. Therefore, the gravity of the criminal threat is rated **Medium**. Nevertheless, with a **High** likelihood and a **Medium** gravity, the overall threat rating remains **High**.

7 Vulnerability Assessment

7.1 Existing Safeguards

As indicated in Figure 1, the headquarters building occupies an open field site with observable, controlled space to a distance of almost 200 m. All visitors are identified at the main entrance and escorted throughout the facility. The parking lot is patrolled regularly to detect and report any unauthorized vehicles. The building transformer is located in a locked room in the basement. No wireless equipment is allowed in the facility. The IAD server is housed in a locked room with enhanced access controls. All cabling, including fibre optic links to connect the local area network, is secured in locked telecommunications closets.

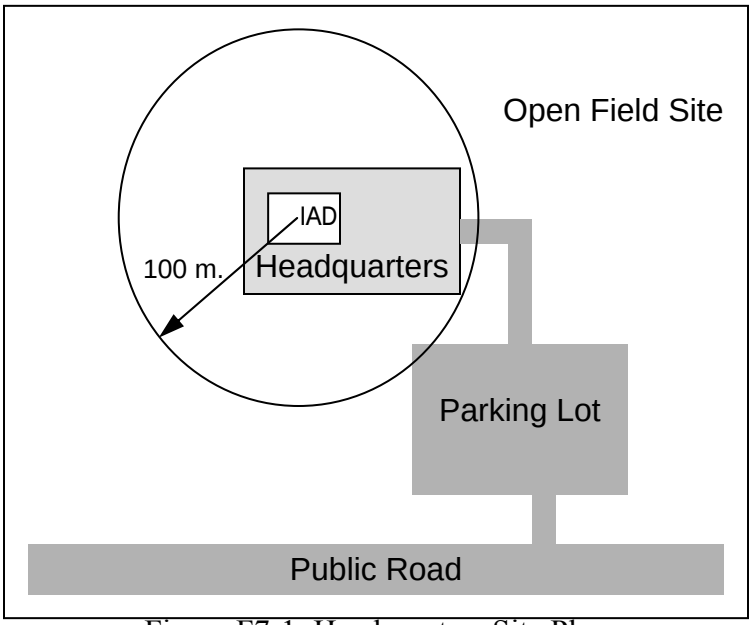

Figure F7-1: Headquarters Site Plan

7.2 Associated Vulnerabilities

The combination of observable space, installation criteria and rigorous access controls provide very effective safeguards to prevent a TEMPEST attack, while roving patrols by security guards afford a moderately effective detection mechanism. Thus, the overall vulnerability of the headquarters is assessed as **Low**, based on a **Low** impact on the probability of compromise and a **Medium** impact on outcome severity.

8 Risk Assessment

With **High** asset values, a **High** threat and a **Low** vulnerability, the assessed residual risk is calculated to be **Medium**, a generally acceptable level, as indicated in Table 1.

Asset (Group/Subgroup)	Asset Values			Associated Threat (Activity/Agent Category)	T	Related Vulnerabilities	V	Residual Risk ($A_{Val} \times T \times V$)	R
	C	A	I						
IAD Inquiry Files	H	–	–	Organized Criminal Groups	H	See Narrative	L	$4 \times 4 \times 2 = 32$	M

Table F7-1: Calculation of Assessed Residual Risk

9 Recommendations

Under the circumstances, it is unnecessary to incur the 300% cost differential to acquire Level 1 TEMPEST equipment, as defined in ITSG-12, *Government of Canada Facility Evaluation Procedures*. Even with commercial off-the-shelf (COTS) workstations and servers, the assessed residual risk falls within the acceptable range at a **Medium** level. Therefore, it is recommended that Level 3 equipment, essentially COTS workstations and servers be purchased from an ISO 9000 certified vendor, and installed on the IAD local area network. In order to prevent any deterioration in the current security posture, it is also recommended that:

- the facility security officer review building access control procedures and visitor logs monthly for any anomalies indicating potential threat activities;
- the system administrator inspect the IAD local area network semi-annually for signs of tampering or unauthorized modifications; and
- the security awareness cell provide roving guards with additional training and routine reinforcement briefings to recognize and report possible TEMPEST threats.

10 Attachments

- TRA Work Plan,
- TRA Report 41/05, IAD Offices and Local Area Network, and
- List of References.

Notes:

1. This sample TRA report is intended to illustrate a focused assessment to address a very specific issue, the need for TEMPEST protection on a local area network processing Protected C information in Canada.
2. An Executive Summary is not really necessary for a TRA report of this size.
3. In order to avoid the use of classified or protected information in this sample, some of the references to ITSG-12, *Government of Canada Facility Evaluation Procedures*, have been simplified or stated obliquely.
4. This sample TRA Report should not be applied directly to any real assessment without further analysis.

This page intentionally left blank.

Annex G - Conclusion

1 Introduction

1.1 General

The five phases of a TRA project, comprising 21 sequential processes and six successive outputs, are described briefly in the Management Summary and amplified considerably in Annexes A-F with even more details captured in a number of appendices. While this documentation provides a complete TRA methodology, the Conclusion offers some supporting material to supplement the basic toolkit and enhance its utility as follows:

- **Related Processes.** The TRA report is an important input to both security site and design briefs for physical security, and the certification and accreditation of IT systems.
- **TRA Best Practices.** Some practical guidance is offered to expedite the TRA process and achieve more consistent results.
- **TRA Worksheet.** A simple worksheet is presented as a useful aide-mémoire for security practitioners conducting a TRA project.
- **Sensitivity of TRA Reports.** Some factors to consider when categorizing TRA reports as either Classified or Protected are identified explicitly.
- **Glossary and Acronyms.** A complete list of all terms and abbreviations employed throughout the Harmonized TRA Methodology has been compiled to improve communications and promote interoperability amongst interrelated TRA projects.
- **References.** All documents cited in the body of the text are listed alphabetically by category with sources wherever possible for ease of reference.

1.2 Aim

The aim of this annex is to present a variety of supporting material to complement the *Harmonized TRA Methodology* described in the body of the document and promote consistent application across disparate TRA projects.

2 Related Processes

2.1 General

As explained in section 7.2 of the Management Summary and amplified in Appendix A-2, Security Standards versus Threat and Risk Assessments, the TRA is an important element of a continuous risk management program, but it is not the complete solution. In fact, a TRA report must be considered in conjunction with other related processes to achieve comprehensive results. These interrelated activities include physical security briefs for the selection and design of new facilities, certification and accreditation of IT systems, configuration management and change

control to determine whether an assessment requires updating as facilities and IT systems evolve over time, and incident response mechanisms that identify new threats or vulnerabilities.

2.2 Security Site and Design Briefs

Security Site Brief
A document which describes the *physical security* attributes sought in a site when relocating the facility.

Security Design Brief
A document which describes the physical protection philosophy and concepts as well as physical safeguards for a facility.

Security Guide TSB/G1-005
Guide to the Preparation of Physical Security Briefs
January 2000.

A Security Site Brief should be compiled whenever selecting a location to lease, purchase or construct a new facility. In this case, the supporting TRA report should identify site specific security problems, both threats and vulnerabilities, such as neighbourhood vandalism, theft or violent crime, and susceptibilities to flooding and other natural hazards. Once the location has been selected, a Security Design Brief should be prepared to recommend appropriate safeguards for both existing structures and new construction. Again, a supporting TRA report should confirm: (1) asset values of the facility and, more importantly, the employees and services operating from the site; (2) any threats that could affect these assets adversely; and (3) the associated vulnerabilities that could expose the assets to harm. Although the recommended safeguards are determined by an analysis of these factors in the TRA report, they are generally omitted or summarized at a high level in the subsequent Security Design Brief in order to avoid a more highly Classified or Protected document.[1]

2.3 Certification and Accreditation (C&A)

Certification *(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.

Accreditation *(accréditation)* - the official authorisation 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.

Government Security Policy, February 2002

Section 10.12.1(a) of the GSP requires departments to certify and accredit IT systems prior to operation. As indicated in the definition, the certification process involves a rigorous examination of all safeguards associated with an IT system to answer two basic questions, namely: (1) have appropriate security measures been selected to satisfy the system security policy; and (2) have they been implemented correctly? In essence, certification aims to collect enough evidence to provide the accreditor with

[1] For further guidance on both Security Site and Design Briefs, see RCMP Security Guide TSB/G1-005, *Guide to the Preparation of Physical Security Briefs*.

adequate assurance or confidence that the system is sufficiently secure to meet operational requirements and business needs. In this regard, the final TRA report is, perhaps, the most compelling input to the final accreditation decision because it presents an objective assessment of assets, their values, relevant threats, associated vulnerabilities and the impact of recommended safeguards on the projected residual risk.[2]

2.4 Configuration Management and Change Control

Neither facilities nor IT systems remain static over time. Modifications frequently commence and new assets are introduced, often with different asset values, even before the subject of the original TRA report is fully deployed and completely operational. Of course, almost any change to the original design of a facility or IT system could introduce new and possibly unacceptable risks. Therefore, sections 10.11 and 10.12.1(b) of the GSP require departments to review physical security safeguards continuously and conduct assessments of IT configuration changes on a regular basis to determine any impact on residual risks. Since many modifications affect only a small subset of assets identified in the original TRA report, revisions needed to assess the security implications of proposed alterations or additions may be accomplished quite quickly to support informed decision making, provided that the departmental TRA, configuration management and change control processes are closely coupled. As a general rule, no change should be approved until the TRA report has been updated and suitable safeguards have been identified, where necessary, to address any unacceptable risks arising from the amendments. Assigning dates and version numbers to TRA reports can help track these changes.

2.5 Incident Response Mechanisms

In a similar vein, new threats and vulnerabilities appear on a regular basis. Some can be identified proactively with an ongoing review of professional journals, news media and intelligence reports, while others will be detected after the fact, when responding to security incidents. In either case, existing TRA reports should be updated to incorporate new threat and vulnerability assessments and the residual risks recomputed. Where the revised risks surpass the acceptable threshold, remedial action should be recommended to maintain a satisfactory security posture. Again, reuse of the original TRA report can expedite the response to any new factors.

3 TRA Best Practices

As indicated in the Introduction,[3] the objectives of the *Harmonized TRA Methodology* include intuitive simplicity, improved modularity, and greater flexibility to enhance both consistency and interoperability. Some basic guidelines or best practices to achieve optimum results with the new methodology have been extracted from each annex and summarized below:

- Limit the scope of each TRA project as much as possible.

2 For further guidance on certification and accreditation, see the CSE publication MG-4, *A Guide to Certification and Accreditation for Information Technology Systems*.

3 See the Introduction, page 2.

- Decompose facilities, systems or business operations into modules to permit several smaller TRA reports rather than a single assessment of overwhelming proportion.
- Identify all linkages amongst related TRA reports.
- Note all relevant risk variables within the scope of the assessment at a higher level of detail, but concentrate on the more valuable assets, the greatest threats and the most serious vulnerabilities, those that are more likely to cause unacceptable residual risks.
- Do not over-analyze any of the risk variables. The first intuitive assessment of asset values, and threat or vulnerability levels is generally more accurate and always more efficient than convoluted arguments over obscure possibilities.
- Similarly, avoid complex threat scenarios to focus primarily on direct threats.
- When TRA team members cannot agree on a single asset value or threat and vulnerability level, note the differences, and compute residual risk using both values.
- To save time and effort, re-use data from earlier TRA reports whenever feasible.
- An informal TRA is particularly useful to determine whether elements of previous assessments may be re-applied to comparable assets in similar circumstances.
- Always apply mandatory security standards. When available and practical, other security standards should be employed in preference to a formal TRA.
- Again, as explained in Appendix A-2, an informal TRA is generally necessary to determine whether these standards are fully applicable in any given situation.
- Keep the final TRA report as short as possible.
- Identify only the most valuable assets, the greatest threats, the most serious vulnerabilities and any unacceptable residual risks in the body of the document, relegating most of the details to supporting annexes and tables.
- Use footnotes to explain the rationale behind any asset value or threat and vulnerability level that is not readily apparent.

4 TRA Worksheet

Appendix G-1 provides a simple TRA Worksheet as a useful aide-mémoire for security practitioners. This four-page document lists all processes and subordinate activities in each successive phase of a TRA project with complete cross references to the applicable annexes and appendices in the body of the text. The worksheet also contains abbreviated versions of the injury table as well as threat and vulnerability metrics. Therefore, with practice, an experienced TRA analyst could compile a complete TRA report following this checklist and entering relevant data in the applicable tables, namely the Statement of Sensitivity (Appendix B-5), Threat Assessment Table (Appendix C-4) and Vulnerability Assessment Table (Appendix D-4).

5 Sensitivity of TRA Reports

5.1 General

In general, most TRA reports are sensitive to unauthorized disclosure because they identify vulnerabilities that might be exploited to compromise assets of value. Availability concerns are usually less significant, despite the obvious costs associated with replacing a lost assessment.

Conversely, unauthorized modification of the findings could cause serious injuries if the analysis were subsequently misinterpreted to recommend inappropriate or inadequate safeguards. Thus, a TRA report invariably warrants categorization to identify confidentiality, availability and integrity values in accordance with the *Identification of Assets Operational Security Standard* and the injury tests explained in section 3 of Annex B and amplified in Appendix B-4.

5.2 Confidentiality Value

In principle, confidentiality values must be assigned according to the level of injury that could reasonably be expected in the event of unauthorized disclosure. In practical terms, however, there are usually two important considerations:

- **Information Sources.** Frequently, the data collected during a TRA project will include either Classified or Protected information, especially during the Threat Assessment Phase. Unless the material can be sanitized or downgraded, the final TRA report must be categorized and marked accordingly.
- **Potential for Abuse.** Even those reports that do not contain Classified or Protected inputs may require categorization and protection for confidentiality purposes, because vulnerabilities identified during the fourth phase of the TRA project might facilitate threats to availability or integrity, leading to unauthorized destruction, removal, modification, interruption or use of assets. If that were the case, the likely level of injury should be determined in accordance with the Expanded Injury Table in Appendix B-4. Then, the final TRA report should be categorized as Classified or Protected to the same level depending upon whether the injury would affect the national or other interests, and marked accordingly.

5.3 Availability Value

Presumably a TRA report would have to be replaced if it were lost or destroyed. Therefore, the simplest measure of availability value would be the estimated cost to reconstruct the document based upon the salaries expended and other associated expenses. This sum should be compared with the Financial Impact column in the Expanded Injury Table to determine the appropriate availability value, usually in the Low or Medium ranges. In a few cases, however, the TRA report may be vitally necessary for immediate operational purposes, such as an impending troop deployment to an active theatre overseas. In situations like this, the delay to recreate the original assessment may have much more severe consequences, even potential loss of life, so the document would warrant a higher availability value commensurate with the prospective injuries.

5.4 Integrity Value

Unauthorized modification of a TRA report could undermine the entire analytical process, leading to inadequate or incomplete recommendations, thereby jeopardizing employees, assets and service delivery. Given the potential consequences, the integrity value of most TRA reports should be as high as the most serious injury arising from any possible compromise to the confidentiality, availability or integrity of assets within the scope of the assessment, whatever the

cause. For example, with a TRA project involving Top Secret information and, therefore, Very High confidentiality value, the integrity value of the final report should also be Very High because deliberate and even accidental alteration of its content could expose the sensitive data to unauthorized disclosure.

6 Glossary and Acronyms

A common and consistent vocabulary for risk management is essential to improve communications amongst security practitioners and interoperability amongst interrelated TRA projects, especially those involving shared information and assets. To that end, all technical terms and acronyms employed throughout the body of the *Harmonized TRA Methodology* are listed in Appendix G-2, along with the source where applicable.

7 References

Many different policies and other related documents are cited throughout the *Harmonized TRA Methodology*. To facilitate cross-referencing and further research, all of this material is listed in Appendix G-3 under the following broad categories:

- Treasury Board Policies and Related Publications;
- GSP: Operational Security Standards;
- GSP: Technical Documentation –
  - CSE Publications,
  - DFAIT Travel Warnings,
  - PSEPC Publications,
  - PWGSC Publications, and
  - RCMP Publications.

Wherever possible the Uniform Resource Identifier (URI) is provided to locate the documents on either the Internet or Publiservice, the government of Canada Intranet.

Appendix G-1 - TRA Worksheet

TRA Phase – Process – Activity	Reference	Page No.
Preparation Phase		
• Establish TRA Project Mandate	• Annex A, Section 3	A-3
• Determine the Scope of Assessment	• Annex A, Section 4	A-4
o Planning Factors	o Section 4.2	A-4
▪ Purpose of the Assessment	▪ Section 4.2.2	A-4
▪ Stage of Development	▪ Section 4.2.3	A-6
▪ Risk Environment	▪ Section 4.2.4	A-7
▪ Some Practical Considerations	▪ Section 4.2.5	A-7
• Select TRA Team	• Annex A, Section 5	A-8
o Team Size	o Section 5.2	A-8
o Team Qualifications	o Section 5.3	A-9
o Core Team Members	o Section 5.4	A-9
o Other Resources	o Section 5.5	A-11
• Draft TRA Work Plan	• Annex A, Section 6 (Appendix A-6)	A-13
Asset Identification and Valuation Phase		
• Identify Assets within the Scope of Assessment	• Annex B, Section 2 (Appendix B-1)	B-2
o Tangible Assets	o Section 2.2	B-2
o Intangible Assets	o Section 2.3	B-2
o Personnel	o Section 2.4	B-3
o Services	o Section 2.5	B-3
o Asset Listing	o Section 2.9 (Appendix B-2)	B-5
• Assess Injuries	• Annex B, Section 3	B-6
o Injury Table (Table 1 below)	o Section 3.3 (Appendix B-4)	B-8
• Assign Asset Values	• Annex B, Section 4	B-10
o Practical Application	o Section 4.2	B-11
▪ Confidentiality	▪ Section 4.2.2	B-11
▪ Availability	▪ Section 4.2.3	B-11
▪ Integrity	▪ Section 4.2.4	B-12
▪ Multiple Values	▪ Section 4.2.6	B-13
o Other Issues	o Section 4.3	B-13
▪ Variable Asset Values	▪ Section 4.3.2	B-13
▪ Aggregation and Inference	▪ Section 4.3.3	B-14
▪ Asset Valuation Conventions	▪ Section 4.3.4	B-15
• Compile Asset Valuation Table/Statement of Sensitivity	• Annex B, Section 5 (Appendix B-5)	B-15
Threat Assessment Phase		
• Identify Threats	• Annex C, Section 2	C-1
o Threat Classes	o Section 2.2	C-2
▪ Deliberate Threats	▪ Section 2.2.2	C-2
▪ Accidental Threats	▪ Section 2.2.3	C-2
▪ Natural Hazards	▪ Section 2.2.4	C-2
o Sources of Threat Data	o Section 2.3 (Appendix C-1)	C-3
o Data Collection Techniques	o Section 2.4	C-3
o Threat Listing	o Section 2.5 (Appendix C-2)	C-4
• Assess the Likelihood of Occurrence (Table 2 below)	• Annex C, Section 3 (Appendix C-3)	C-11
• Assess the Gravity (Table 3 below)	• Annex C, Section 4 (Appendix C-3)	C-13
• Assign Threat Levels (Table 4 below)	• Annex C, Section 5 (Appendix C-3)	C-14
• Compile and Prioritize Threat Assessment Table	• Annex C, Section 6 (Appendix C-4)	C-17

Risk Assessment Phase – Vulnerability Assessment • Identify Existing and Proposed Safeguards • Assess Their Effectiveness • Determine Remaining Vulnerabilities o Sources of Vulnerability Data o Data Collection Techniques o Vulnerability Listing • Assess Their Impact o Probability of Compromise (Table 5 below) o Severity of Outcome (Table 6 below) • Assign Vulnerability Levels (Table 7 below) • Compile and Prioritize Vulnerability Assessment Table	• Annex D, Section 2 • Annex D, Section 3 • Annex D, Section 4 o Section 4.3 (Appendix D-1) o Section 4.4 o Section 4.5 (Appendix D-2) • Annex D, Section 5 (Appendix D-3) o Section 5.2 o Section 5.3 • Annex D, Section 6 • Annex D, Section 7 (Appendix D-4)	D-1 D-2 D-5 D-10 D-11 D-11 D-13 D-13 D-15 D-17 D-20
Risk Assessment Phase – Calculation of Residual Risk • Compute Residual Risks o Basic Risk Calculation (Table 8 below) o Risk Levels (Table 9 below) • Compile Prioritized List of Assessed Residual Risks	• Annex E, Section 2 o Section 2.2 o Section 2.3 (Appendix E-1) • Annex E, Section 3 (Appendix E-2)	E-1 E-1 E-2 E-4
Recommendation Phase • Identify Unacceptable Residual Risks o Risk Ranges (Table 9 below) • Select Potential Safeguards o Safeguard Effectiveness • Identify Costs o Direct Costs o Indirect Costs/Benefits o Cost Effectiveness • Assess Projected Residual Risks • Prepare Final TRA Report	• Annex F, Section 2 o Section 2.3 • Annex F, Section 3 (Appendix F-2) o Section 3.3 (Appendix F-3) • Annex F, Section 4 o Section 4.2 o Section 4.3 o Section 4.4 (Appendix F-4) • Annex F, Section 5 (Appendix F-5) • Annex F, Section 6 (Appendix F-6)	F-1 F-2 F-4 F-6 F-9 F-9 F-10 F-11 F-13 F-13

Asset Identification and Valuation Phase

Table 1: Graduated Injury Table

Level of Injury	Injury to People		Financial Impact
	Physical	Psychological	
Very High	Widespread Loss of Life	Widespread Trauma	> $1 billion
High	Potential Loss of Life	Serious Stress/Trauma	> $10 million
Medium	Injury/Illness	Public Suspicion/Doubts	> $100 thousand
Low	Discomfort	Minor Embarrassment	> $1 thousand
Very Low	Negligible	Negligible	< $1 thousand

Threat Assessment Phase

Table 2: Threat Likelihood Table

Past Frequency	Same Location Similar Assets	Remote Location but Similar Assets or Same Location but Different Assets	Remote Location Other Assets
Daily	High	High	High
1-10 Days	High	High	Medium
10-100 Days	High	Medium	Low
100-1,000 Days	Medium	Low	Very Low
1,000-10,000 Days	Low	Very Low	Very Low
Over 10,000 Days	Very Low	Very Low	Very Low

Threat Assessment Phase (continued)

Table 3: Threat Gravity Table		
Deliberate Threat Agent Capabilities	**Magnitude of Accidents or Natural Hazards**	**Threat Impact or Gravity**
Extensive Knowledge/Skill Extensive Resources	Highly Destructive Extremely Grave Error Widespread Misuse	High
Limited Knowledge/Skill Extensive Resources **or** Extensive Knowledge/Skill Limited Resources **or** Moderate Knowledge/Skill Moderate Resources	Moderately Destructive Serious Error Significant Misuse	Medium
Limited Knowledge/Skill Limited Resources	Modestly Destructive Minor Error Limited Misuse	Low

Table 4: Threat Levels Table				
Threat Impact	**Threat Likelihood**			
	Very Low	**Low**	**Medium**	**High**
High	Low	Medium	High	Very High
Medium	Very Low	Low	Medium	High
Low	Very Low	Very Low	Low	Medium

Risk Assessment Phase – Vulnerability Assessment

Table 5: Vulnerability Impact on Probability of Compromise (Prevention)		
Safeguard Effectiveness	**Associated Vulnerabilities**	**Probability of Compromise**
No Safeguard Safeguard Largely Ineffective Probability of Compromise > 75%	Easily Exploited Needs Little Knowledge/Skill/Resources Assets Highly Accessible Assets Very Complex/Fragile/Portable Employees Ill-Informed/Poorly Trained	High
Safeguard Moderately Effective Probability of Compromise 25-75%	Not Easily Exploited Needs Some Knowledge/Skill/Resources Assets Moderately Accessible Assets Fairly Complex/Fragile/Portable Moderate Employee Awareness/Training	Medium
Safeguard Very Effective Probability of Compromise < 25% (Safeguard Performs Only Detection, Response or Recovery Functions)	Difficult to Exploit Needs Extensive Knowledge/Skill/Resources Assets Highly Accessible Assets Very Simple/Robust/Static Employees Well-Informed/Trained	Low (Not Applicable)

Risk Assessment Phase – Vulnerability Assessment (continued)

Table 6: Vulnerability Impact on Severity of the Outcome (Detection, Response or Recovery)		
Safeguard Effectiveness	**Associated Vulnerabilities**	**Severity of Outcome**
No Safeguard Safeguards Largely Ineffective Assets Exposed to Extensive Injury	Unlikely to Detect Compromise Damage Difficult to Contain Prolonged Recovery Times/Poor Service Levels Assets Very Complex/Fragile Employees Ill-Informed/Poorly Trained	High
Safeguard Moderately Effective Assets Exposed to Moderate Injury	Compromise Probably Detected Over Time Damage Partially Contained Moderate Recovery Times/Service Levels Assets Fairly Complex/Fragile Moderate Employee Awareness/Training	Medium
Safeguard Very Effective Assets Exposed to Limited Injury (Safeguard Performs Only a Prevention Function)	Compromise Almost Certainly Detected Quickly Damage Tightly Contained Quick and Complete Recovery Assets Very Simple/Robust Employees Well-Informed/Trained	Low (Not Applicable)

Table 7: Vulnerability Assessment			
Vulnerability Impact on Severity of the Outcome(Detection, Response & Recovery)	**Vulnerability Impact on Probability of Compromise (Prevention)**		
	Low (N/A)	**Medium**	**High**
High	Medium	High	Very High
Medium	Low	Medium	High
Low (N/A)	Very Low	Low	Medium

Risk Assessment Phase – Calculation of Residual Risk

Table 8: Numeric Scores for Asset Value, Threat and Vulnerability Levels					
Asset Value, Threat and Vulnerability Levels	Very Low	Low	Medium	High	Very High
Scores for Risk Computation	1	2	3	4	5

Table 9: Risk Levels and Ranges					
Basic Risk Score	1-4	5-12	15-32	36-75	80-125
Risk Level	Very Low	Low	Medium	High	Very High
Number of Outcomes in Range	13	34	43	28	7
Risk Acceptability	Definitely Acceptable	Probably Acceptable	Possibly Acceptable	Probably Unacceptable	Definitely Unacceptable

Notes:

1. The TRA Worksheet lists all successive processes and activities within each phase of a TRA project.
2. Copies of all tables required to assess asset values, threat and vulnerability levels, and residual risks are included in the same logical sequence for ease of use.
3. This worksheet with copies of the Asset Valuation Table/Statement of Sensitivity (Appendix B-5), Threat Assessment Table (Appendix C-4), Vulnerability Assessment Table (Appendix D-4), List of Assessed Residual Risks (Appendix E-2) and Recommendations Table (Appendix (F-5) form the basic toolkit to complete a TRA.

Appendix G-2 - Glossary and Acronyms

1 Preface

Terms and abbreviations defined in Appendix G-2, Glossary and Acronyms, are used throughout the Harmonized Threat and Risk Assessment Methodology. Most are derived from the GSP and relevant supporting documentation. In some cases, however, earlier definitions have been expanded to achieve greater clarity, consistency or completeness. Where this occurs, both the old and new definitions are included for purposes of comparison. Finally, a number of new expressions have been coined to describe specific concepts or processes within the methodology.

2 Sources

The sources for all previously defined terms are indicated for each entry, while new definitions are clearly identified as such, according to the following key:

[GSP]..... Government Security Policy
[IA]..... Identification of Assets Operational Security Standard
[PSS]..... Operational Standard on Physical Security
[New]..... Harmonized TRA Methodology Working Group

3 Navigation

Hyperlinks are used within the glossary to navigate. Press [CTRL] and [CLICK] on the letter of the alphabet listed below to scroll to that area of the glossary. The letter Icons in the body of the glossary are followed by a "Home" link which will return the cursor to this navigation line.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Accidental Threats ( ) **– [New]** – unplanned threats caused by human beings.

Accepted Residual Risk ( ) **– [New]** – the level of risk approved by the risk acceptance authority, usually based upon the final recommendations in a TRA report.

Accreditation *(accréditation)* **– [GSP]** – the official authorisation 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.

Aggregation (regroupement) **– [IA]** – the situation where a collection of assets may be categorized at a higher level of sensitivity than its component parts due to the increased injury that could result if it is compromised. Generally aggregation applies to confidentiality, but it can also apply in certain circumstances to availability and integrity.

Assessed Residual Risk ( ) **– [New]** – the residual risk calculated during the Risk Assessment Phase of a TRA project.

Assets (biens) **– [GSP]** – 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.

ASIS – American Society for Industrial Security.

ATIP (AIPRP) –Access to Information Act and Privacy Act.

Availability (disponibilité) **– [GSP]** - the condition of being usable on demand to support operations, programs and services.

B Home

BCP (PCO) – Business Continuity Planning.

BCPC ( ) – Business Continuity Plan Coordinator.

Baseline security requirements (exigences sécuritaires de base) – [GSP] - mandatory provisions of the Government Security Policy and its associated operational standards and technical documentation.

BIA ( ) – Business Impact Analysis.

Business Continuity Planning (planification de la continuité opérationnelle) **– [GSP]** - an all-encompassing term which includes the development and timely execution of plans, measures, procedures and arrangements to ensure minimal or no interruption to the availability of critical services and assets.

C Home

CERT/CC ( ) – Computer Emergency Response Team/Coordination Center, Carnegie Mellon University.

Certification (certification) **– [GSP]** - 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.

CIO (DPI) – Chief Information Officer.

Classified assets (biens classifiés) – **[GSP]** - assets whose unauthorized disclosure would reasonably be expected to cause injury to the national interest.

Classified Information (renseignements classifiés) – **[GSP]** - 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.

Compromise (compromission) – **[GSP] -** Unauthorized disclosure, destruction, removal, modification, interruption or use of assets.

Confidentiality (confidentialité) – [GSP] - 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*.

Critical assets (biens essentiels) – [GSP] - assets supporting a critical service.

Critical Service (service essentiel) – **[GSP]** - service whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, security or economic well-being of Canadians, or to the efficient functioning of the Government of Canada.

CSE (CST) – Communications Security Establishment.

CSIS (SCRS) – Canadian Security Intelligence Service.

Csis, Inc. ( ) -- Canadian Society for Industrial Security, Inc.

D Home

Deliberate Threats ( ) – **[New]** – Planned or premeditated threats caused by human beings.

Destruction ( ) – **[New]** – the physical alteration of assets or injury to employees that can render them unavailable to perform their primary functions.

Detection (détection) – **[PSS]** – The use of appropriate devices, systems and procedures to signal that an attempted or actual unauthorized access has occurred.

DFAIT ( ) – Department of Foreign Affairs and International Trade.

Dollar Value ( ) – **[New]** – appreciated or depreciated worth of tangible assets; replacement cost.

DSO (ASM) – Departmental Security Officer.

E Home

EAA (AAE) – **Electronic Authorization and Authentication**.

F Home

Facility (installation) – **[GSP]** – A physical setting used to serve a specific purpose. A facility may be within a building, or a whole building, or a building plus its site; or it may be a construction that is not a building. The term encompasses both the physical object and its use.

G Home

GSP (PGS) – Government Security Policy.

H Home

HRSDC ( ) – Human Resources and Social Development Canada.

I Home

IM/IT ( ) – Information Management/Information Technology

Inference (inférence) – **[IA]** – the situation where assets categorized at one level of sensitivity may be analyzed to draw conclusions that could result in greater injury.

Information (renseignements) – **[PSS] -** any pattern of symbols or sounds to which meaning may be assigned.

Information Technology Security (sécurité des technologies de l'information) – **[GSP]** – safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information.

Injury (préjudice) – **[IA]** – the damage that results from the compromise of assets.

Integrity *(intégrité)* - **[GSP]** - the accuracy and completeness of assets, and the authenticity of transactions.

Interruption ( ) **–** **[New]** – a temporary disruption to the availability of employees, assets or services.

ITSC ( ) **–** Information Technology Security Coordinator.

Lead Security Department ( ) **– [New, based on GSP]** – departments or agencies with government-wide security responsibilities defined in the GSP.

Modification ( ) **– [New]** – the alteration of data or sensors and systems that process information, thereby affecting the accuracy or completeness of assets or the authenticity of transactions.

National interest (intérêt national) **– [PSS]** – concerns the defence and maintenance of the social, political and economic stability of Canada.

Natural Hazards ( ) **– [New]** – threats attributable to forces of nature.

Need-to-know (besoin de connaître) **– [GSP]** – The need for someone to access and know information in order to perform his or her duties.

OSH – Occupational Safety and Health.

PDRR ( ) **–** Protection, Detection, Response and Recovery; the Active Defence Strategy.

(TRA) Phase ( ) **– [New]** – the five major segments of a TRA project, namely the Preparation, Asset Identification and Valuation, Threat Assessment, Risk Assessment and Recommendations Phases.

Physical Security (sécurité matérielle) **– [GSP]** – the use of physical safeguards to prevent and delay unauthorized access to assets, detect attempted and actual unauthorized access and activate appropriate response.

PIA ( ) **–** Privacy Impact Assessment.

(TRA) Process ( ) **– [New]** – the principal activities within each phase of a TRA project.

(TRA) Project ( ) **– [New]** – application of the TRA processes to a specific subject, to produce a complete TRA report based on the full TRA record.

Projected Residual Risk ( ) **– [New]** – the residual risk achieved with implementation of all recommendations in the final TRA report.

Protected Assets (biens protégés) **– [PSS]** – assets whose unauthorized disclosure would reasonably be expected to cause injury to a non-national interest.

Protected Information (renseignements protégés) **– [GSP] –** information related to other than 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 a non-national interest.

Protection (protection) **– [PSS] –** for physical security, protection means the use of physical, procedural and psychological barriers to delay or deter unauthorized access, including visual and acoustic barriers.

PSEPC ( ) – Public Safety and Emergency Protection Canada.

PWGSC ( ) – Public Works and Government Services Canada.

R&D ( ) **–** Research and Development.

RCMP (GRC) **–** Royal Canadian Mounted Police.

(TRA) Record *( )* **– [New]** – a TRA Report plus all relevant documentation collected during the TRA project to support the final conclusions and recommendations.

Recovery ( ) **– [PSS]** – to the restoration of full levels of service delivery.

Residual Risk *( )* **– [New]** – the risk that remains after safeguards have been selected and implemented.

(TRA) Report (rapport) **– [New]** – the final output of a TRA project, presented to the risk acceptance authority for management review and approval.

Response (intervention) **– [PSS]** – the implementation of measures to ensure that security incidents are reported to appropriate security officials and immediate and long-term corrective action taken.

Risk (risqué) **– [GSP]** – the chance of a vulnerability being exploited.

Risk Acceptance Authority *( )* **– [New]** – a senior manager with the authority, responsibility and accountability for reviewing and approving recommendations in a TRA report.

S Home

Safeguards (Mesures de protection) **– [New]** – assets or external controls that reduce overall risk to employees, other assets or service delivery by decreasing the likelihood of a threat event, reducing the probability of compromise, or mitigating the severity of the outcome through direct or indirect interaction with asset values, threats or vulnerabilities.

SOS ( ) **–** Statement of Sensitivity; used synonymously with Asset Valuation Table.

SOW ( ) **–** Statement of Work.

Surreptitious Attack (attaque subreptice) **– [PSS]** – a secret unauthorized attack to breach or circumvent a defensive system or some of its components in such a manner that the custodians and/or security force cannot readily detect the attack.

T Home

Threat (menace) **– 1 [GSP]** – any potential event or act, deliberate or accidental, that could cause injury to employees or assets**; 2 [New]** – any potential event or act, deliberate, accidental or natural hazard, that could cause injury to employees or assets, and thereby affect service delivery adversely.

TRA (EMR) **–** Threat and Risk Assessment.

Unauthorized access ***(accès non autorisé)*** **– [PSS]** – Access to assets by an individual who is not properly security screened and/or does not have a need-to-know.

Unauthorized disclosure ***(divulgation non autorisée)*** **– [PSS]** – Disclosure that is forbidden by law or by governmental or departmental policies.

Value **(*valeur*) – [GSP]** – estimated worth, monetary, cultural or other.

Vulnerability ***(vulnérabilité)*** **– 1 [GSP]** – an inadequacy related to security that could permit a threat to cause injury; **2 [New] --** an attribute of an asset or the environment in which it is located that increases the likelihood of a threat event, the probability of compromise or the severity of the outcome. Vulnerabilities are inversely proportional to safeguard effectiveness.

Zones ***(zones)*** **– [PSS]** – a series of clearly discernible spaces to progressively control access.

Appendix G-3 - References[1]

Treasury Board Policies and Related Publications

Government Security Policy, February 2002.
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg_e.asp

Integrated Risk Management Framework, April 2001.
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/rmf-cgr_e.asp

Management Accountability Framework, 2003.
http://www.tbs-sct.gc.ca/maf-crg/maf-crg_e.asp

Occupational Safety and Health Policy, 1999.
http://www.tbs-sct.gc.ca/pubs_pol/hrpubs/TBM_119/osh_e.asp

Privacy and Data Protection Policy, December 1993.
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/CHAP1_1_e.asp

Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks, August 2002.
http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld_e.asp

Privacy Impact Assessment Policy, May 2002.
http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr_e.asp

Report of the Independent Review Panel on Modernization of Comptrollership in the Government of Canada, October 1997.
http://www.tbs-sct.gc.ca/cmo_mfc/resources2/review_panel/rirp06_e.asp

Results for Canadians: A Framework for the Government of Canada, March 2001.
http://www.tbs-sct.gc.ca/res_can/rc_e.asp

Risk Management Policy, April 1994.
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/riskmanagpol_e.asp

GSP: Operational Security Standards

Identification of Assets, Draft, February 9, 2005.
http://publiservice.tbs-sct.gc.ca/gos-sog/gs-sg/spins/2005/2005-03_e.asp

1 Please note, some publications are only available on the federal government Intranet, known as Publiservice or Genet, and cannot be accessed from external sources.

Business Continuity Planning (BCP) Program, March 2004.
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/ossbcp-nsopca_e.asp

Management of Information Technology Security, April 2004.
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/23RECON_e.asp

Readiness Levels for Federal Government Facilities, November 1, 2002.
http://publiservice.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/oss-nos_e.asp

Security in Contracting Management, Draft, March 24, 2005.
http://publiservice.tbs-sct.gc.ca/gos-sog/gs-sg/spins/2005/2005-06_e.asp

Security Investigations and Sanctions, Draft, May 28, 2005.

Security Risk Management, Draft, May 1, 2005.

Security Screening, Draft, April 30, 2004.

Security Training and Awareness, Draft, March 15, 2005.
http://publiservice.tbs-sct.gc.ca/gos-sog/gs-sg/spins/2005/2005-05_e.asp

GSP: Technical Documentation

CSE Publications

ITSA-09 – *COMSEC Equipment Disposal*, January 15, 1998.
http://www.cse-cst.gc.ca/documents/publications/gov-pubs/itsa/itsa09-e.pdf

ITSA-10 – *COMSEC Incident Reporting*, December 1, 2004.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsa/itsa10-e.html

ITSB-02 – *Government of Canada Wireless Vulnerability Assessment*, August 2002.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsb/itsb02-e.html

ITSB-03 – *Trends in Wireless Technology and Security*, October 30, 2002.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsb/itsb03-e.html

ITSB-06 – *CSE Approves Secure BlackBerry*, May 6, 2003.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsb/itsb06-e.html

ITSB-09 – *STU-III Operation during a Power Outage*, October 10, 2003.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsb/itsb09-e.html

ITSB-12 – *Procurement of the Blackberry Security Module*, October 29, 2003.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsb/itsb12-e.html

ITSB-13 – *Key Ordering for STE*, October 28, 2003.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsb/itsb13-e.html

ITSB-15 – *Security Vulnerability - Wireless Local Area Network (WLAN) Capable Laptops*, February 11, 2004.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsb/itsb15-e.html

ITSB-18 – *NATO Recommended Products List (NRPL) - TEMPEST Approved Products*, May 5, 2004.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsb/itsb18-e.html

ITSB-19 – *Security Measures - Wireless Electronic Devices*, May 19, 2004.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsb/itsb19-e.html

ITSB-29 – *SECTERA Global System for Mobile Communication Security Module (SGSM) Wireless Standing Offer*, May 1, 2006.
http://www.cse-cst.gc.ca/documents/publications/gov-pubs/itsb/itsb29-e.pdf

ITSD-01 – *Directives for the Application of Communications Security in the Government of Canada*, January 2005.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsd/itsd01-e.html

ITSD-02 – *IT Security Zones Baseline Security Requirements*, May 2003.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsd/itsd02-e.html

ITSG-06 – *Clearing and Declassifying Electronic Data Storage Devices*, August 2000.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/itsg06-e.html

ITSG-10 – *COMSEC Material Control Manual*, January 2003.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/itsg10-e.html

ITSG-13 – *Cryptographic Key Ordering Manual*, May 2006.
http://www.cse-cst.gc.ca/documents/publications/gov-pubs/itsg/itsg13-e.pdf

ITSG-20 – *Windows Server 2003 Recommended Baseline Security*, March 2004.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/itsg20-e.html

ITSPSR-14 – Telework Project, March 2002.
http://www.cse-cst.gc.ca/publications/gov-pubs/itspsr/itspsr14-e.html

ITSPSR-16 – *Personal Communications Services (PCS) and Cellular System Vulnerability Assessment*, October 2002.
http://www.cse-cst.gc.ca/publications/gov-pubs/itspsr/itspsr16-e.html

ITSPSR-17 – *Bluetooth Vulnerability Assessment*, October 2002.
http://www.cse-cst.gc.ca/publications/gov-pubs/itspsr/itspsr17-e.html

ITSPSR-18 – *Personal Digital Assistant Vulnerability Assessment*, October 2002.
http://www.cse-cst.gc.ca/publications/gov-pubs/itspsr/itspsr18-e.html

ITSPSR-19 – *Windows 2000 Pro and Windows XP Pro Recommended Baseline Security*, May 2003.
http://www.cse-cst.gc.ca/publications/gov-pubs/itspsr/itspsr19-e.html
ITSPSR-21 – 802.11 Wireless LAN Vulnerability Assessment, May 2003.
http://www.cse-cst.gc.ca/publications/gov-pubs/itspsr/itspsr21-e.html

MG-1 – *Network Security, Analysis and Implementation*, January 1996.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/mg1-e.html

MG-2 – *A Guide to Security Risk Management for Information Technology Systems*, January 1996.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/mg2-e.html

MG-4 – *A Guide to Certification and Accreditation for Information Technology Systems*, January 1996.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/mg4-e.html

MG-9 – *Canadian Handbook on Information Technology Security*, March 1998.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/mg9-e.html

DFAIT Travel Warnings

Consular Affairs Travel Warnings
http://www.voyage.gc.ca/dest/sos/warnings-en.asp

PSEPC Publications

Business Continuity Planning Program Technical Documentation, March 4, 2004.
http://rcmp-grc.gc.ca/tsb-genet/awareness/2004-PSEPC-BCP-en.doc

PWGSC Publications

Industrial Security Manual, May 2006.
http://www.ciisd.gc.ca/text/ism/toc-e.asp

RCMP Publications

G1-001 – *Security Equipment Guide*.
http://www.rcmp-grc.gc.ca/tsb-genet/seg/html/home_e.htm

G1-002 – *Security Lighting*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_e.htm

G1-003 – *Glazing*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_e.htm

G1-004 – *Construction of Special Discussion Areas*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_e.htm

G1-005 – *Preparation of Physical Security Briefs*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_e.htm

G1-006 – *Identification Cards/Access Badges*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_e.htm

G1-007 – *Security Sealing of Building Emergency/Master Keys or Cypher Lock Codes*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_e.htm

G1-008 – *Guidelines for Guard Services*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_e.htm

G1-009 – *Standard for the Transport and Transmittal of Sensitive Information and Assets*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_e.htm

G1-010 – *Security Connotations of the 1995 National Building Code*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_e.htm

G1-011 – *Overhead Door Specifications*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_e.htm

G1-013 – *Security Control Room Space Requirements*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_e.htm

G1-014 – *Exterior Fixed Ladder Barrier Specification*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_e.htm

G1-015 – *Entry Controls for Overhead Doors*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_e.htm

G1-016 – *Master Key Systems*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_e.htm

G1-017 – *Hardware*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_e.htm

G1-018 – *Doors and Frames*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_e.htm

G1-019 – *Vaults*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_e.htm

G1-024 – *Control of Access*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_e.htm

G1-025 – *Protection, Detection and Response*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_e.htm

G1-026 – *Application of Physical Security Zones*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_e.htm

G1-027 – *Tenant and Custodian Departments Physical Security Responsibilities*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_e.htm

G1-029 – *Secure Rooms*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_e.htm

G1-030 – *Security Awareness Guide*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/g1-030_e.htm

G1-031 – *Server Rooms*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_e.htm

G2-002 – *Guide to Minimizing Computer Theft*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/it_sec/index_e.htm

G2-003 – *Hard Drive Secure Information Removal and Destruction Guidelines*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/it_sec/index_e.htm

G2-004 – *Windows 2000 Professional Advanced Security Configuration Guide*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/it_sec/index_e.htm

G2-005 – *Windows 2000 Active Directory Security Configuration Guide*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/it_sec/index_e.htm

B2-001 – *Suggested DSX Replacement Products*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/it_sec/index_e.htm

R2-001 – *Biometric Technologies: An Assessment of Practical Applications*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/it_sec/index_e.htm

R2-002 – *Future Trends in Malicious Code*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/it_sec/index_e.htm

DSX-G – *RCMP Hard Disk Overwrite Software (DSX) User Manual*.
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/it_sec/index_e.htm

This page intentionally left blank.