

## Chapter 6 – DEFINITION OF A COMMON METHODOLOGY

It is always a good practice to go back to the basics and examine what are the components of risk management and where commonality may exist between different risk identification exercises. In this section, the analysts attempt to present some of the standard ways in which risk analysis is conducted. The result is a proposed common TRA framework.

### 6.1 THE DIFFERENT COMPONENTS OF RISK ANALYSIS

The traditional risk analysis framework is well established, although some methodologies provide emphasis on different risk factors. The Canadian ITSG-04 is more a threat and asset centric methodology. The NIST 800-30 is more vulnerability centric with little insight to confidentiality, integrity and availability. One must agree that even though the outcome, the risk value, is common to all methods, considerable variation exists in terms of interpretation of the basic terms and the general process model. Common language between methodologies is lacking, resulting in limitation in the development of a common framework. If a common approach is the ultimate goal, all stakeholders should agree on the basic components of a TRA. Following the functional description of the risk,  $R=f(A_{Val}, T, V)$ , the components of a TRA are (definition from ITSG-04):

- 1) **Assets Identification or the Statement of Sensitivity (SoS):** A description of the confidentiality, integrity and availability requirements associated with the information or assets stored or processed in or transmitted by an IT system;
- 2) **Threat Assessment:** An evaluation of threat agent characteristics including resources, motivation, intent, capability, opportunity, likelihood and consequence of acts that could place sensitive information and assets at risk;
- 3) **Vulnerability Assessment:** An evaluation of the vulnerabilities of an IT component, program or system to determine if the controls in place are sufficient to address security issues that could impact the confidentiality, integrity, or availability of the system assets; and other types of impact are possible such as costs; and
- 4) **Risk Assessment:** An evaluation of risk based on threat assessment information, the effectiveness of existing and proposed security safeguards, the likelihood of system vulnerabilities being exploited and the consequences of the associated compromise to system assets.

[One of the recommendations from the previous risk management study<sup>1</sup> was to ensure a common language or common terminology is used in the common risk management framework]. The NATO working group agreed on a NATO vocabulary. However, for this study, the NATO glossary was not made available to the analysts. For that reason, it is assumed that the selection of terminology was agreed upon, which on its own, is a significant step towards a common framework. Another fundamental assumption is that regardless of the risk management methodology, the four basic steps described above are an integral part of the common framework.

### 6.2 GENERIC RISK ASSESSMENT FRAMEWORK

The four basic TRA components can be expanded upon to develop a generic functional framework. The previous study suggested a general functional framework for either manual or automated risk assessment. The rationale behind this approach is to provide a basis for commonality, clearly define the inputs and outputs to each TRA phases to minimize potential factual error and to allow insight into where

---

<sup>1</sup> Common Methods For Security Risk Analysis, prepared for DRDC by Cinnabar Networks Inc., 22 December 2004.

## DEFINITION OF A COMMON METHODOLOGY

automation (or partial automation) could take place (blue). The outputs or deliverables are often combined in a single report. The generic functional framework would comprise the following elements.

**Table 6-1: Generic Risk Assessment Framework**

Function	Description	Inputs	Outputs
Business Model	The organization business model is defined and understood.	Legislation Interviews Observations Success Factors	Mission Statement Business Requirements User Requirements Target Risk Level TRA Scope
System Architecture Analysis	System Architecture is analyzed and assessed as a basis for asset location analysis and vulnerability analysis.	Interviews Documentation Observations System Development Life Cycle Phase TRA Scope	System Architecture System Description Concept of Operation Information Flow Description User Community Refined TRA Scope
Asset Classification, Impact Analysis and Injury Test	Information assets are identified, described, classified by sensitivity.	System Description Interviews – Directed questions Documentation Observations Qualitative Rating Description	Asset Profiles Statement of Sensitivity Sensitivity Impact Statement Requirements for other Security Services
Threat Assessment	Threat agents are identified by class characteristics and behavioural analysis; Threat Scenarios are constructed using simple tabular or more complex, e.g., attack tree-based, Bayesian, or causal net-based representations.	Interviews Documentation Observations Architecture Asset Profiles Expert Knowledge Qualitative Rating Description	Threat Agents Table Threat Scenarios Table

<b>Function</b>	<b>Description</b>	<b>Inputs</b>	<b>Outputs</b>
Vulnerability Assessment	System vulnerabilities are identified and assessed; relationship to threat scenarios identified using simple tabular or tree-based representations.	Interviews Documentation Observations Architecture Threat Scenarios Expert Knowledge	Vulnerability Categories Vulnerability Table
Safeguard Analysis	Existing safeguards are identified and assessed for strength; relationship to vulnerabilities identified.	Interviews Documentation Observations Architecture Vulnerability Table Expert Knowledge	Safeguard Categories Initial Safeguard Tables
Risk Assessment	Existing risk is assessed by threat scenario: associated vulnerabilities, safeguards and threat agent characteristics functionally determine an effective threat level that reflects current mitigation; Statement of Sensitivity and threat levels provide inputs of risk level determination.	Statement of Sensitivity Threat Agents Table Threat Scenarios Table Vulnerability Table Safeguard Tables Qualitative Rating Description	Risk Mitigation Strategy Initial Risk Assessment
Additional Safeguard Recommendations	New Safeguards are identified and assessed for strength; relationship to vulnerabilities and threat scenarios identified, indicating effective risk mitigation rationale; strategic deployment of new safeguards indicated.	Safeguard Categories Initial Safeguard Tables Architecture Vulnerability Table Expert Knowledge	Enhanced Safeguard Tables
Residual Risk Assessment	As in Risk Analysis above, but with the Enhanced Safeguard Tables, to show the effect of the mitigation strategy of adding new safeguards.	Statement of Sensitivity Threat agents Table Threat Scenarios Table Vulnerability Table Enhanced Safeguard tables	Recommendations Residual Risk Assessment

## DEFINITION OF A COMMON METHODOLOGY

Function	Description	Inputs	Outputs
Remediation Plan	A follow up plan to ensure recommendations are addressed in due time and the risk is monitored upon implementation of mitigating strategy.	Recommendations Enhanced Safeguard Tables Timeline Team Responsibility	Prioritization of Recommendations Remediation Plan
Final Report	A comprehensive and useful TRA report to document findings of the analysis and to provide inputs to other risk management activities.	SoS Threat Assessment Vulnerability Assessment Risk Assessment Prioritization of Recommendations Remediation Plan	TRA Report Executive Summary Certification Process

This generic framework is uniquely developed from the melding of different TRA methodologies to address weaknesses that were observed in the TRA process. It covers all phases and elements of a TRA leaving no undue facets for potential inaccuracy or omission. This method is more streamlined resulting in a more accurate analysis and precise risk ratings.

Further discussions are provided in the next sections on automation, standardization and commonality. The Canadian contribution would give precedence to risk management work using these innovative concepts.