13 September 2011

Harmonized TRA (HTRA) Methodology – Limitations

William Dziadyk, CD, MSc, P.Eng.
BD Pro Inc.
www.bdpro.ca

Acknowledgements

Several senior security risk analysts have reviewed and/or contributed to the development of this discussion paper. In particular, the contributions of Eugen Bacic, Alan Clason, Hugh Ellis, Bob English, Marcel Gingras, Ron Hysert, Steve Irwin, Dev Kohli, Laurie Mack, Gary Maxwell, William Sandberg-Maitland, Steve Schnider, Mike Sues and Roger Tremblay are very much appreciated. With their broad spectrums of analytical and quality review experience using various government and private sector TRA methodologies and their experience in implementing recommended security controls, they have helped identify key areas to be considered in future improvements to the Harmonized Threat and Risk Assessment (HTRA) Methodology[1] and other security risk management guides.

Objectives

The HTRA Methodology is currently being used by many Government of Canada departments. The HTRA Methodology was developed by the Communications Security Establishment Canada (CSEC) and the Royal Canadian Mounted Police (RCMP) to consolidate a variety of prior guidelines with the objective of creating a consistent risk analysis methodology for both information technology security (IT Security) and physical security.

Many Risk Analysts use the HTRA Methodology only as a guide, and tailor the methodology by independently introducing "*workarounds*" to address its various limitations, in order to satisfy the needs of risk owners. Primary objectives of this paper are to analyse the limitations of the HTRA Methodology and propose approaches for improved effectiveness and standardization of the risk analysis and TRA deliverables.

This discussion paper summarizes the main limitations of the HTRA Methodology in order that Risk Analysts can more effectively understand and deal with them while continuing to provide effective and meaningful security risk assessment services to their clients. General issues are summarized in main body of this paper with supporting analytical details recorded in *Annex A – Detailed Analysis of HTRA Issues*.

In addition, the enterprise system architectures, technologies, cyber security tools and the cyber threat environments have changed considerably since the 2007 introduction of the HTRA Methodology. A related objective is to identify some key areas to be considered in future improvements to the HTRA Methodology (and perhaps other risk management standards and guides) to more effectively address these changes. An "HTRA+" or "HTRA v2" is required to improve the quality of risk deliverables to levels that can withstand review scrutiny, support the needs of management accountability frameworks and be used to support business cases for security spending.

The adequacy or limitations of using the Harmonized TRA methodology in performing physical security TRAs has not been specifically addressed in this discussion paper.

Introduction

The HTRA Methodology has been in use since 2007, with stricter adherence to the HTRA report format and content and formats of analysis tables, picking up in 2010. A body of evidence, in the form of completed IT security related TRAs, now exists to support a detailed review of the HTRA Methodology. Many risk management personnel (risk analysts, senior QA reviewers and risk owners) are now able to contribute to such a review. Senior analysts who have contributed to this paper have arrived at a general consensus that a number of issues have been introduced by the new methodology. These issues are resulting in TRA deliverables that are of poorer quality, when compared to some of the better TRAs performed in the pre-HTRA

[1] Harmonized Threat and Risk Assessment (TRA) Methodology, Version TRA-1, Communications Security Establishment and Royal Canadian Mounted Police, 23 Oct 2007. Available at http://www.rcmp-grc.gc.ca/ts-st/pubs/tra-emr/index-eng.htm

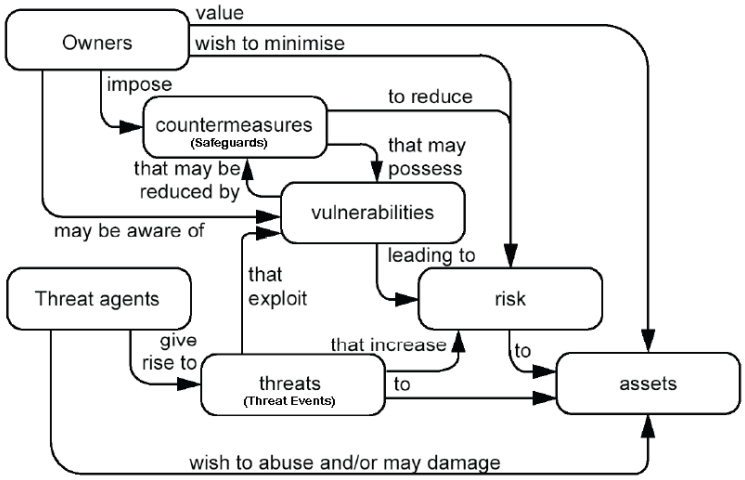
© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.
http://creativecommons.org/licenses/by/2.5/ca/legalcode.en

era. A consensus is building among many senior analysts and QA reviewers that the current methodology, when strictly followed, has the following general problems:

a. Encouraging higher level, generalized analysis and recommendations that are of less use than previous TRAs (in spite of multi-level definition tables that should have increased granularity);
b. Difficult traceability from threats through to recommended safeguards, with multiple analysis tables scattered throughout the report;
c. Missing risk analysis details supporting ratings at all levels: a function of the small-cell, table structures. From a QA reviewer's perspective, the evidence of the analysis is often lacking in the report and necessitates questions of clarification with the Risk Analyst;
d. A risk level formula and rating guide that does not consider safeguard effectiveness, creating excessive residual risk ratings in certain circumstances (cannot be lowered, regardless of safeguards applied); and
e. Poorly detailed safeguard descriptions (existing and recommended) that in many cases cannot be implemented effectively and securely without additional analysis and documentation.

Analysis of HTRA Methodology

The following security context diagram from the Common Criteria[2] summarizes the basic concepts and the general contextual relationships (between Critical Assets, Threat Agents, Threat Events, Vulnerabilities, Safeguards[3] and Risks) which must be adequately addressed in any IT Security risk management analysis methodology.



Specific Threat Events initiated by a Threat Agent to compromise an identified Critical Asset by exploiting both Vulnerabilities and inadequate Safeguards are referred to as "*Threat Scenarios*"[4]. The goal of the TRA analysis of such Threat Scenarios is to reduce (i.e. mitigate) the residual Risk to the identified Critical Assets to an acceptable level by introducing additional recommended Safeguards. One advantage of threat scenario based analysis is that all aspects of a risk can be analysed in single defined abstraction, including effects of multiple vulnerabilities (negative effects) and multiple layered safeguards (positive effects).

The main limitations of using the Harmonized TRA Methodology are in the following areas:

a. Ease-of-Use of Guidance Document – The HTRA Methodology guidance document consists of 290 pages (including 38 separate annexes or appendices). Unlike the predecessor CSEC and RCMP guidance documents, the HTRA guidance document is definitely not a document that one would expect

[2] Common Criteria for Information Technology Security Evaluation, part 1: Introduction and General Model, version 2.3, Aug 2005
[3] In some risk management guidance documents, the terms "countermeasures: or "security controls" are also used to refer to "safeguards".
[4] ITSG-04 defined "Threat Scenario" as "*A postulated set of circumstances in which a specific threat agent can mount a specific type of attack in an attempt to compromise (in one or more ways) one or more system assets*."

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.
http://creativecommons.org/licenses/by/2.5/ca/legalcode.en

clients (i.e. business owners) to read and understand. If needed, it is up the Risk Analyst to explain the HTRA and any of its strengths or limitations to the business owner. Many Risk Analysts also find it to be an overly complex and lengthy guide.

b. Generalization of Analytical Elements - The HTRA high-level generalization approaches, to be used in defining and documenting the details of the analytical elements (assets, threat agents, threat events and safeguards) and in the subsequent analysis, could tend to result in more of a high-level health check rather than the needed detailed recommended lower-level security controls (i.e. detailed safeguards and countermeasures) for specific system implementation work plans. These issues are expanded upon in "Generalization of Analytical Elements" section below;

c. Documentation and Presentation of Analysis – The HTRA Methodology is very process-oriented with many analysis tables to be completed with small cells (12 to 15 characters in most cases) available for recording elements of the analysis. The traceability of the analysis through these various analysis tables is a challenge for the analysts, persons doing QA on the deliverables and clients accepting the deliverables. The formats of the HTRA analysis tables tend to discourage detailed analysis (or the documentation of that detailed analysis) since in general there is only room for titles and ratings in the tables. These issues are expanded upon in "Documentation and Presentation of Analysis" section below;

d. Calculation of Residual Risks – The HTRA Methodology does not explicitly consider existing and recommended Safeguards or the likelihood and motivation of Threat Agents in the calculation of Risk. These issues are expanded upon in "Calculation of Residual Risks" section below; and

e. System Security Certification and Accreditation – TRAs are often conducted in support of security Certification and Accreditation of systems. From a Security Systems Design/Architecture point of view, the outputs of a TRA should clearly identify recommended security controls (i.e. Safeguards) or options required in the system. This will provide the security systems engineer (SSE) with major input which, along with applicable polices and standards (such as NIST SP 800-53) to help derive the systems security requirements. However, the HTRA output provides high-level generalized controls and does not generally provide the level of detail to allow mapping to control standards. These issues are expanded upon in "System Security Certification and Accreditation" section below.

Generalization of Analytical Elements

MITS[5] requires that "*Threat and Risk Assessments can be short and simple or far more detailed and rigorous, depending on the sensitivity, criticality and complexity of the program, system or service being assessed*." For Government of Canada security critical systems where detailed security controls are to be selected from security control catalogues (such as NIST SP 800-53), the TRA will need to use a more detailed and rigorous approach in defining the analytical elements (in particular: assets, threat events and safeguards) than the generalization approach advocated by the HTRA.

The level of detail, level of effort and rigor required for a TRA is very much dependant on the criticality of the target system, the budget of the business owner ... and the processes and documentation required by the chosen TRA methodology.

The HTRA Methodology does have detailed multi phase processes with corresponding required documentation (i.e. completed analysis tables). However the high level generalization or simplification of the analytical elements advocated by the HTRA Methodology tends to require the Risk Analyst to provide more of a high-level health check for an enterprise or system rather than focussed lower-level recommended technical and operational security controls (i.e. safeguards) for implementation within security requirements baselines for individual security critical systems. Most TRAs for security critical systems need a "*more detailed and rigorous*" approach than the high level (i.e. high level generalization of assets, threat agents, threat events and safeguards) approach advocated by the HTRA Methodology. This more focused and detailed approach is required in order to satisfy the business risk owner's risk management requirements (within allocated budget) and identify controls for the following purposes:

[5] Section 13.3.2, Operational Security Standard: Management of Information Technology Security (MITS), Treasury Board of Canada Secretariat , Jun 2004

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.
http://creativecommons.org/licenses/by/2.5/ca/legalcode.en

a. To be included in detailed system security requirements and implementation documents. This is particularly important for defining the security requirements baseline for systems being developed using a Systems Development Lifecycle (SDLC) systems engineering approach;
b. To augment and improve the defense-in-depth security architecture, where most needed;
c. To identify needed interrelated safeguards to counter modern sophisticated multi-phase cyber attacks (i.e. *spear phishing*)*;*
d. To select safeguards from detailed security control catalogues and other system specific security best practices documentation. General purpose (i.e. NIST SP 800-53) and system specific security controls best practices documents are used as a source of security controls to be considered as candidate safeguards to be used in the TRA. Some of these security best practices documents are security control catalogues which use robustness or impact levels such as Low, Medium, and High for defining "*security control baselines*". A goal of most TRAs should be to select and tailor these general purpose (often enterprise level) and system specific security control baselines in order to mitigate the risks and satisfy the system specific security needs; and
e. To be implemented in management action plans or specific system implementation work plans.

To manage and mitigate security risks, all of the analytical elements must be adequately considered and documented by the Risk Analyst in any risk management analysis methodology. The limitations in how the HTRA Methodology addresses and documents the identification and categorization of critical assets, safeguard selection, threat agents, and threat events are documented in the *Annex A – Detailed Analysis of HTRA Issues*. The Risk Analyst should understand these limitations and make recommendations such as the following to the client, for tailoring the HTRA Methodology for the effective conduct of the TRA:

a. Assets – see *Annex A – Detailed Analysis of HTRA Issues* entries #1, #2, #3 and #4:
   - Identify critical assets at the component level for the client's security critical systems rather than at the higher levels as often done using the HTRA Methodology;
   - Use a 3 security parameter (confidentiality, integrity and availability) scheme for risk analysis, risk calculation and selection of security controls for security critical systems. The HTRA does use the 3 parameter scheme for earlier phases of the analysis; however a single parameter high water mark ($\mathbf{A}_{\mathbf{val}}$) scheme is used for calculation of Risk;
   - Specifically include consideration of those most valuable information critical assets, associations between such information assets and the associations of people with those information assets;
   - For injury tests for critical assets which have significant estimated monetary or cultural worth, use the categorization injury test criteria provided in the TBS draft standard[6]; and
   - Use alternate formats for Asset Valuation Tables (Statements of Sensitivity) which allow more descriptive critical asset (i.e. business processes or information assets) details to be recorded and allow meaningful categorization rationale to be effectively recorded.
b. Threat Agents – see *Annex A - Detailed Analysis of HTRA Issues* entry #5:
   - Use a more detailed approach for defining threats to individual security critical systems rather than the high level generic "*roll up*" approach used in the HTRA Methodology; and
   - Threat agents should often be consolidated (rather than "*rolled up*") based upon common attributes in order to lead to the selection of safeguards that would counter the threats/vulnerabilities in a unified manner.
c. Threat Events – see *Annex A - Detailed Analysis of HTRA Issues* entries #6 and #11:
   - Use a more detailed approach (than the HTRA consolidation approach) for defining threat events to be used for performing TRAs on security critical systems. Threat Events for security critical systems must clearly include and identify: system related critical asset(s) to protect, vulnerabilities of concern, likely threat agent, likely consequences (i.e. loss of specific confidentiality, integrity or

[6] Operational Security Standard: Identification of Assets, draft, Treasury Board of Canada Secretariat, February 2005

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.
http://creativecommons.org/licenses/by/2.5/ca/legalcode.en

availability) in language understandable by business owners. The formats of the HTRA analysis tables tend to discourage analysis since there is only room for titles and ratings.

d. Safeguards – see *Annex A - Detailed Analysis of HTRA Issues* entries #7 and #8:

- Document the safeguard functionality and effectiveness details in more detail than that allowed by the small cells of HTRA analysis tables;
- Document security requirements (i.e. Safeguards) in enough detail which can be used effectively in an implementation work plan, SOW, or RFP ... etc. in a subsequent body of work to mitigate the found risks; and
- Use and leverage security controls standards in the selection of security controls and determination of residual risks to security critical systems, notwithstanding the negative guidance (See Annex A, analysis entry #7) on use of such standards in the HTRA Methodology. Select needed safeguards from security controls catalogues (such as NIST SP 800-53, Payment Card Industry Data Security Standard (PCI DSS), ISO/IEC 27002 Code of Practice for Information Security Management, SANS 20 Critical Security Controls, and/or other system specific standards), rather than from the HTRA high level Safeguard Listing.

e. Vulnerabilities – see *Annex A – Detailed Analysis of HTRA Issues* entries #9 and #10:

- Document the vulnerabilities in more detail than that allowed by the small cells of HTRA analysis tables;
- Consider more meaningful and relevant vulnerabilities than those implied in the HTRA Sources of Vulnerability Data table D1 (see analysis entry #9) or listed in the HTRA Vulnerability Listing table D2 (see analysis entry #10). The "IT Security" section of the Vulnerability Listing table is inadequate, For example, it does not clearly address vulnerability areas such as the following:
  - Common IT security vulnerabilities – the ones we have been wrestling with for years;
  - Complex hacker attack vectors through sequences of different vulnerabilities in multi-server network architectures;
  - Modern "*temporal risk*" based attacks that occur as a result of concerted attacks of seemingly minor independent probes that are coordinated over a period of months;
  - Interrelated social engineering, technical and other vulnerabilities targeted in newer multi phase cyber crime vectors focussed on specific persons and information;
  - "*zero day vulnerabilities*" exploited by threat agents to target an organization's critical information and fiscal assets;
  - Potential vulnerabilities introduced with introduction of server and desktop virtualization;
  - Vulnerabilities specific to protecting industrial controls systems (aka SCADA -supervisory control and data acquisition systems); and
  - Application software vulnerabilities;
- Include consideration of vulnerability findings from prior or concurrent penetration tests (aka onsite technical vulnerability assessments (OTVAs)) in the analysis.

Documentation and Presentation of Analysis

The Harmonized TRA Methodology is very process oriented with many analysis tables to be completed by the Risk Analyst during each phase. See *Annex A – Detailed Analysis of HTRA Issues* entry #11.

The HTRA process is largely a table filling exercise. There is nothing wrong with this as long as there are supporting documented narratives which can explain the analysis and at a detailed level provide the threads which connect the assets, threats, vulnerabilities, likelihoods, impacts, safeguards/controls, and finally risks. In addition to the generalization of the main analytical elements (assets, threat agents, threat events and safeguards), the HTRA does not require the use of Threat Scenarios to help relate the rows of one table to rows of other tables or require that unique identifiers be used for indentifying these analytical elements when recorded in different tables.

Many modern cyber attacks are complex multi phase endeavours involving social engineering, custom malware and the leveraging of social network information in layered focused attacks (i.e. *spear phishing*)

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.
http://creativecommons.org/licenses/by/2.5/ca/legalcode.en

against a series of vulnerabilities to order to compromise specific targeted critical assets. The concept of Threat Scenarios can assist the Risk Analyst in linking the TRA analysis of such series of independent but interrelated vulnerabilities.

With Threat Scenarios not being used, introduction of unique identifiers and special efforts will be needed by the Risk Analyst to support achieving the following goals related to delivery of a quality product:

a. Identifying needed safeguards to counter modern complex multi-phase cyber attacks;
b. Traceability within the delivered TRA Report of the assets, threat agents, threat events and safeguards which are recorded in the various analysis tables across the phases of the TRA analysis;
c. In order to combine or compare TRAs done by different individuals or to perform semantic or other automated post-analysis of any substantial bodies of TRA analysis results;
d. Effective and efficient quality assurance (peer review or senior QA) and/or potential repeatability of analysis (i.e. sensitivity analysis, threat assessment, safeguard selection analysis, and risk analysis) by Client's Technical Authority or by other third party TRA analysts;
e. The client's potential reuse or leveraging the analysis for other systems or facilities within the client's organization; and
f. Traceability of recommended safeguards to requirements in standard security control standards and to government security standards such as MITS.

The use of unique identifiers for the major analytical elements will also facilitate the Risk Analysts' use of automated tools using relational databases (such as Microsoft Access™ or Corel Paradox™) for effectively and efficiently performing complex interrelated risk analysis. Some experienced Risk Analysts have been using such tools in performing their analysis.

Calculation of Residual Risks

See *Annex A – Detailed Analysis of HTRA Issues* entry #12.

The HTRA Methodology states "*risk (R) may be described as a functional relationship amongst asset values (*A_{Val}*), Threats (T) and Vulnerabilities (V).*"

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

The HTRA risk calculations are based on a scoring method using "ordinal" scales. A recent paper by Hubbard and Evans [7] is very critical of the use of such "ordinal" scales in determination of residual risk.

In the HTRA formula, the effects of the Safeguards (S) parameter on residual risk are buried the considerations of the Vulnerabilities (V) parameter. The HTRA Methodology does not directly consider the effectiveness of existing and recommended Safeguards in the calculation of Risk. The effectiveness of the various Safeguards in mitigating the Risk is buried in the analyst's undocumented considerations of the Vulnerabilities. The risk level formula and rating guide does not consider safeguard effectiveness, creating excessive residual risk ratings in certain circumstances (which cannot be lowered, regardless of safeguards applied).

The lack of an input parameter for safeguards is a serious omission for determining risk (before application of recommended safeguards) and residual risk (after application of recommended safeguards). It may be possible to somehow factor in a basic security safeguard posture when assessing vulnerabilities, but it seems error-prone and difficult for auditors and general readers of the subsequent TRA report to perform traceability on the vulnerability assessment. It is difficult to see the value of this approach unless the HTRA has the premise that the analysis can be performed faster and arrive at the same conclusions by not considering the protective function of existing safeguards. However experience indicates that this is not the case. Some safeguards do work directly on a specific vulnerability. Other safeguards mitigate the composite risk in a more indirect manner by transferring it to other agencies, etc. or by working in combination with other safeguards to mitigate risk.

[7] *Problems with scoring methods and ordinal scales in risk assessment*, D. Hubbard, D. Evans, (published in IBM Journal of Research and Development, May/June 2010), available at www.dylan.org.uk/ordinal.pdf

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.
http://creativecommons.org/licenses/by/2.5/ca/legalcode.en

Detailed consideration of recommended safeguards in the calculation of risk is even more important if the client organization intends to achieve ISO 27001 certification. It would be very difficult to produce a "*Statement of Applicability (SOA)*", without using an explicit residual risk based on mitigating safeguards, or "controls". The SOA is the blueprint for acquisition of new safeguards for the organization and justifies their procurement to upper management by directly linking these acquisitions to risk reduction.

The relationship between safeguards and vulnerabilities, threat agent motivation, and even the valuation of assets is sometimes complex and often needs to be fully documented.

The most difficult part of any TRA is often determining the vulnerabilities and the impact of safeguards on these vulnerabilities in the application/system. The documentation of these vulnerability related risk considerations are not clearly addressed in the table filling processes of the HTRA. The HTRA guidance also encourages the vulnerabilities to be identified and generalized at a higher level in order to be documented in small cells of HTRA tables.

In addition, the motivation and likelihood of Threat Agents is not directly considered in the HTRA calculation of Risk.

Prior to the introduction of the HTRA, a blend of the RCMP (SIP-5[8] and R1-001[9]) and the CSEC (ITSG-04[10], MG-2[11], MG-3[12], and MG-4[13]) methodologies was used. In this blended methodology, the Risk was determined in a subjective manner, however the Risk was clearly considered to be a function of considerations directly related to the Critical Assets, Threat Events, Safeguards and Vulnerabilities. (The motivation and likelihood of Threat Agents was also indirectly considered in the calculation of Risk.)

$$\mathbf{R = } f \mathbf{(A, T, S, V)}$$

There is a need for effectively including the effectiveness of existing and recommended Safeguards (S) in the calculation of Risk.

System Security Certification and Accreditation

See *Annex A – Detailed Analysis of HTRA Issues* entry #13.

From a Security Systems Design/Architecture point of view, the outputs of a TRA should clearly identify the recommended security controls (i.e. Safeguards) and/or options required in the system. This will provide the security systems engineer (SSE) with major input which, along with applicable polices and standards (such as NIST SP 800-53) to help derive the systems security requirements. However, the HTRA output provides high-level generalized controls and does not generally provide the level of detail to allow mapping to control standards.

Threat scenario based views of the TRA analysis should be provided to the business owner. An advantage of threat scenario based analysis is that all aspects of a risk can be analysed in single defined abstraction, including effects of multiple vulnerabilities (negative effects) and multiple layered safeguards (positive effects). Such abstractions are much easier to be understood by business owners, making the TRA potentially more valuable in the C&A process where the business owners are responsible for accrediting the system and accepting the residual risk.

The HTRA Methodology does not provide any guidance related to Certification and Accreditation of systems. The HTRA does state that such guidance is to be found in the *Guide to Certification and Accreditation for Information Technology Systems* (MG-4). However, MG-4 is no longer available and is "*under review*".

[8] RCMP Security Information Guide 5, Guide to Threat and Risk Assessment for Information Technology, Nov 1994
[9] RCMP Guide to Threat and Risk Assessment Involving On-Site Physical Security Examination: R1-001, 2004
[10] Threat and Risk Assessment Working Guide (ITSG-04), Communications Security Establishment, Oct 1999
[11] A Guide to Security Risk Management for Information Technology Systems, Communications Security Establishment, Jan 1996
[12] A Guide to Risk Assessment and Safeguard Selection, Communications Security Establishment, Jan 1996
[13] A Guide to Certification and Accreditation for Information Technology Systems (MG-4), Communications Security Establishment, Jan 1996

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.
http://creativecommons.org/licenses/by/2.5/ca/legalcode.en

Conclusions

In many cases where a more focused detailed and rigorous approach is needed to satisfy the risk management needs of the Business Owner, experienced Risk Analysts have independently introduced "*workarounds*" or enhancements (such as those discussed in this paper) to the HTRA Methodology. Others have continued to use a proven methodology, which is a blend of the RCMP (SIP-5 and R1-001) and the CSEC (ITSG-04, MG-2, MG-3, and MG-4) methodologies. All of these guidance documents are no longer available. In addition with the withdrawal of MG-4, there is no longer a standard guidance document available to Risk Analysts that addresses security Certification and Accreditation for systems.

The HTRA process is largely a table filling exercise. Improvements are needed which would clearly support and encourage the use of automated tools using relational database approaches for performing the complex interrelated risk analysis.

It is acknowledged that other TRA methodologies used by other levels of government and in the private sector also typically suffer from some of the limitations discussed in this HTRA paper. Some of these other methodologies do include an initial security controls compliance review phase. There is real value in considering the incorporation of some of the "lessons learned" and potential efficiencies from these other TRA methodologies for improving HTRA deliverables.

Like many of its predecessors, the HTRA Methodology should only be used as a guideline not a mandated contracted process. Junior people entering the TRA profession for the first time may find it informative, however many treat it as a prescriptive table filling exercise. Many experienced Risk Analysts find it cumbersome/time consuming and overall not very useful in focusing in on the real problems.

If use of the Harmonized TRA Methodology is a contractual requirement, the lead Risk Analyst, at the project kick-off meeting, should consider ensuring that the client is made aware of relevant limitations discussed herein and propose customization to the contract deliverable. At such kick-off meetings, the client is often represented by a "technical authority" who reports to the actual business risk owner. At these project kick-off meeting, the lead Risk Analyst is encouraged to propose tailoring to the methodology to improve the needed level of detail for defining and documenting assets, threat agents, threat events, vulnerabilities and selecting safeguards; in order to satisfy the business risk owner's risk management requirements and the intent of MITS. The business risk owner is ultimately accountable to understand, monitor and accept the identified residual risks.

Comments and feedback on the Harmonized TRA Methodology were not solicited from experienced security risk management practitioners prior to it being issued in 2007. Government of Canada users and Risk Analysts now have about 4 years of experience using the HTRA guide. It should now be possible for the two lead agencies to validate how well that guidance:

a. Supports satisfying the MITS goals for TRAs that are "*more detailed and rigorous, depending on the sensitivity, criticality and complexity of the program, system or service being assessed*".
b. Improves the quality of TRAs and facilitates effective QA of the deliverables by third parties and acceptance and use of the risk management deliverables by clients (i.e. business owners). (Are the Business Owners getting what they thought they were paying for?);
c. Allows effective selection of security safeguards for mitigating risks to Government of Canada security critical systems;
d. Meets the needs of Certification and Accreditation authorities in user departments; and
e. Satisfies the underlying requirements of the former guidance documents (SIP-5, R1-001, MG-2 MG-3 MG-4 and ITSG-04) which the HTRA was intended to replace.

Risk Analysts are encouraged to provide feedback to their government clients, CSEC and/or the RCMP based on their use of the HTRA Methodology. Such feedback should also recommend that the effectiveness of the HTRA Methodology be validated before the former guides are officially superseded by the HTRA.

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.
http://creativecommons.org/licenses/by/2.5/ca/legalcode.en

Annex A – Detailed Analysis of HTRA Issues

1. **Asset Identification – Level of Detail**

The HTRA Appendix B-2 Asset Listing (pages B2-1 – B2-8) uses a standard list of assets for security Risk Analysts to select assets from and provides guidance such as "*When developing a Statement of Sensitivity ... all assets within the scope of the assessment may be transferred at appropriate level of detail from the Asset Listing* ..." to the subsequent sensitivity analysis. As shown in extract from the HTRA Appendix B-2 Asset Listing, there are 5 levels of asset detail (**Class, Category, Group, Subgroup** and **Component/Individual**) for the Risk Analyst to choose from when identifying critical assets.

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		
		C...		
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

The asset listing and its breakdown is not relevant for most TRAs performed for security critical systems. It is also difficult to consistently carry forward the breakdown into subsequent steps of the methodology.

In many TRAs for modern distributed systems, the most valuable assets are the information and associations between information. Yet that focus on the information and its attributes often escapes adequate attention. Furthermore, the association of people with information is also valuable, and often overlooked.

In the HTRA Appendix B-2 examples, at the ***component*** level, the critical assets are only described using a short title. In the subsequent HTRA analysis tables for recording additional critical asset details, the cells for identifying and describing critical assets are limited to about 12 to 15 characters. More detail is required. (See related analysis entry #11.)

HTRA Annex B – Asset Identification and Valuation Phase, Section 2.9.3 Caveat (page B-6) states: "... *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 aidemémoire and guide to help organize and structure the collection and collation of relevant asset data, rather than a checklist to be followed without question."*

Many of the TRAs which have been conducted using the HTRA Methodology use the higher level ***Groups*** or ***Subgroups*** rather than lower level application specific or system specific ***Components*** in the identification of critical assets for subsequent sensitivity analysis.

To support the goals of risk management at the system level, it is necessary that many architecture, system and application related critical assets be defined at the ***Component*** level. Given the specificity of Security Controls Catalogues (such as NIST SP 800-53) and the related security control baselines, the assets to be protected may need to be at the ***component*** level in order that relevant lower-level security controls for mitigating risk can be considered as TRA Safeguards.

If use of the Harmonized TRA Methodology is a contractual requirement, the lead Risk Analyst should ensure that the client is made aware of the limitations discussed herein and should recommend that critical assets:

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.

	• be identified at the ***component*** level for client's security critical systems, if this level of analytical rigour for specific architectures, systems and applications is required by the client, rather than at the higher levels as often done using the HTRA; • specifically include consideration of those most valuable information critical assets, associations between such information assets and the associations of people with those information assets; • be documented to include detailed description of the Critical Assets; and • be assigned ***unique identifiers*** to facilitate: - Traceability of targeted critical assets within the Statement of Sensitivity and subsequent sections of the TRA report; - Repeatability of sensitivity analysis and quality assurance by TRA Analyst and/or Technical Authority; - Potential reuse or leveraging of the asset identification analysis for other systems or facilities within the Client Organization; and - Use of relational databases (such as MS Access, Corel Paradox, etc ...) or spreadsheet based automated tools for performing complex interrelated risk analysis.

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.

2.

Asset Categorization (Valuation) Scheme

Effective risk management approaches rely heavily on there being an effective and standard means of valuating the critical assets in terms of 3 security parameters *confidentiality, integrity and availability*.

See related analysis entry #1.

The HTRA does not provide detailed asset identification and categorization guidance. As indicated in HTRA Section 1 Introduction (page MS-1), Figure MS-1 of the HTRA, the HTRA Methodology relies on the draft TBS Identification of Assets[14] standard for injury test guidance for the Statements of Sensitivities analysis (or HTRA Asset Identification and Valuation Phase).

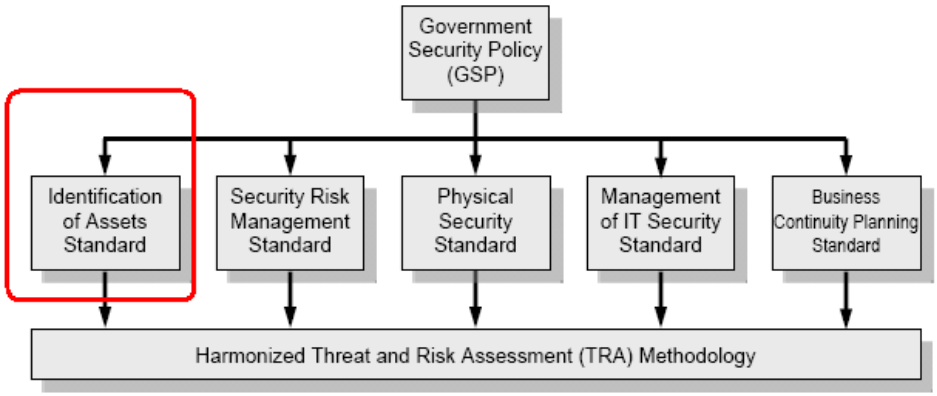


Figure MS-1: Contextual Framework for the Harmonized TRA Methodology

However, the HTRA uses a "*high water mark*" scheme where the "*asset value*" is taken to be the highest of the 3 security parameters (confidentiality, integrity and availability) for subsequent risk analysis calculations, selection of security controls and determination of residual risks. This means that this single parameter high water mark "*asset value*" used in the HTRA is not directly compatible with the 3 security parameter asset categorization scheme required by the draft TBS standard. (The TBS standard also provides categorization guidance for a 4th parameter "value". See analysis entry #3.)

(NIST SP-800 53 also uses a "*high water mark*" scheme. However the NIST high water mark scheme is only used for "*the express purpose of selecting an initial set of security controls from one of the three security control baselines*" in the SP 800-53 catalogue of safeguards).

The HTRA uses a 5 level asset categorization (referred to as "valuation" in HTRA) (VL=1, L=2, M=3, H=4 and VH=5) scheme for the 3 security parameters (confidentiality, integrity and availability). The reader is referred to the draft TBS standard for injury test related guidance.

However, the draft TBS standard uses a 3 level asset categorization (L, M, and H) scheme for the 4 security parameters (confidentiality, integrity, availability and value). Below is a summary of the TBS confidentiality related injury test guidance:

[14] Operational Security Standard: Identification of Assets, draft, Treasury Board of Canada Secretariat, February 2005

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.

Annex A – Detailed Analysis of HTRA Issues

Sensitivities	Sensitivity Rating Scale		
	High	**Medium**	**Low**
Confidentiality **(Impacts to the 125national interest)**	**Injury level:** High **Injury test:** Confidentiality compromise could reasonably be expected to cause exceptionally grave injury to the national interest. **Examples include**: • Widespread loss of life; • Loss of the continuity of government; • Exceptionally grave damage to the effectiveness or security of Canadian and allied forces; • Exceptionally grave damage to the effectiveness of extremely valuable intelligence operations; • Exceptionally grave damage to relations with other governments; • Severe long-term damage to the Canadian economy. **Info Rating: TOP SECRET**	**Injury level:** Medium **Injury test:** Confidentiality compromise could reasonably be expected to cause serious injury to the national interest. **Examples include**: • Increased international tension; • Serious damage to international or federal-provincial relations; • Serious damage to the operational effectiveness of the Canadian Forces; • Serious damage to valuable intelligence operations; • Significant threats to the national critical infrastructure; • Serious damage to civil order. **Info Rating: SECRET**	**Injury level:** Low **Injury test:** Confidentiality compromise could reasonably be expected to cause limited injury to the national interest. **Examples include**: • Damage to diplomatic relations; • Damage to the operational effectiveness of the Canadian forces; • Damage to the effectiveness of intelligence operations; **Info Rating: CONFIDENTIAL**
Confidentiality **(Impacts to private & non-national interests)**	**Injury level:** High **Injury test:** Confidentiality compromise could reasonably be expected to cause extremely serious injury to private or non-national interests. **Examples include**: • Loss of life; • Extremely significant financial losses. **Info Rating: PROTECTED C**	**Injury level:** Medium **Injury test:** Confidentiality compromise **could** reasonably be expected to cause serious injury to private or non-national interests. **Examples include**: • Substantial distress to individuals due to the loss of privacy; • Significant loss of competitive advantage to a Canadian company; • Impeding the investigation of a serious crime; • Impeding the development of major government policies. **Info Rating: PROTECTED B**	**Injury level:** Low **Injury test:** Confidentiality compromise could reasonably be expected to cause limited injury to private or non-national interests. **Examples include**: • Personal information such as tombstone data, e.g., names, addresses and dates of birth; • Personal identifiers, e.g., PRI, military service numbers, SIN; An individual's linguistic profile; • Third party business information provided in confidence. **Info Rating: PROTECTED A**

Below is comparison between TBS and HTRA schemes for the Confidentiality categorizations used in labelling sensitive information.

Domain	Confidentiality Categorization	TBS	HTRA
Classified	Top Secret	High	Very High
	Secret	Medium	High
	Confidentiality	Low	Medium
Protected	Protected C	High	High
	Protected B	Medium	Medium
	Protected A	Low	Low

Notwithstanding that HTRA refers to the draft TBS standard for guidance, the HTRA categorization scheme is not consistent with the TBS scheme for categorizing Classified information. The HTRA does provide some rationale for this inconsistency; however confusion is introduced regarding how to consistently use the injury test criteria in the draft TBS standard.

If use of the Harmonized TRA Methodology is a contractual requirement, the lead Risk Analyst should ensure that the client is made aware of the limitations discussed herein and should recommend that:

- 3 security parameter (confidentiality, integrity and availability) scheme be used for risk analysis and selection of security controls for security critical systems rather than using a single parameter high water mark scheme as used in the HTRA Methodology; and
- The categorization rating scheme used be consistent with guidance provided in the draft TBS standard or other standards by TBS.

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.

3.

Conflicting Definitions of "Asset Value"

The HTRA Methodology uses the term "***Asset Value***" for purposes which conflict with the accepted meaning of this term as defined in related risk management guidance.

MITS 12.2 "Identification and Categorization of Information and IT Assets" states "*In accordance with the Operational Security Standard for the Identification and Categorization of Assets, departments must determine the criticality and sensitivity of their information and IT **assets** with regard to confidentiality, integrity, availability and **value**.*"

The HTRA Methodology relies on the draft TBS Identification of Assets[15] standard for injury test guidance for the Statements of Sensitivities analysis. (See analysis entry #2 for details.) The draft TBS standard includes injury test guidance pertaining to heritage or monetary worth. Below is a summary of this TBS guidance for "**Asset Value"**:

Sensitivities	Sensitivity Rating Scale		
	High	**Medium**	**Low**
Value	**Injury level:** High **Injury test:** High degree of injury to value **Examples include:** • a single asset whose monetary value or replacement cost would be extremely high (very expensive equipment, paintings); • a concentration of assets in a specific building area ,the overall monetary value or replacement cost of which would be extremely high (e.g. a receiving area for computer and other equipment; a large cash unit); • irreplaceable important cultural artefacts; and • large holdings of firearms or drugs.	**Injury level:** Medium **Injury test**: Medium degree of injury to value **Examples include:** • a single asset whose monetary value or replacement cost would be significant; • a concentration of assets in a specific building area ,the overall monetary value or replacement cost of which would be significant (e.g. a receiving area for computer and other equipment; a cash unit); and • small holdings of firearms or drugs.	**Injury level:** Low **Injury test:** Low degree of injury to value **Examples include:** • taxi chits; and • small amounts of cash.

Ref: Operational Security Standard: Identification of Assets, draft, Treasury Board of Canada Secretariat, February 2005

The HTRA Methodology uses a "high water mark" scheme where the "***Asset Value***" is defined to be the highest of the 3 security parameters (Confidentiality, Integrity and Availability). Based on this high water mark, a numerical parameter between 1 and 5 is assigned to **"*Asset Value*" (A_{Val})** which is used in the Risk calculations. (See analysis entry #12 for details).

The HTRA Methodology also sometimes uses the plural term "***Asset Values***" to refer the set of injury test C, A, I and $ categorization results for a particular critical asset.

TRA-1 Harmonized Threat and Risk Assessment Methodology

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								

HTRA Appendix B, Section 4.2.5 Value (pp B-12 – P-13) states:

- GSP definition of "Value" as being "*estimated worth, monetary, cultural or other*"; and
- "*The fourth measure of **asset value**, the least useful in the context of the Harmonized TRA*

[15] Operational Security Standard: Identification of Assets, draft, Treasury Board of Canada Secretariat, February 2005

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.

Methodology for several reasons. ...."

The HTRA then uses the term "*replacement cost*" or "*replacement value*" for injury tests pertaining to heritage or monetary worth rather than "Asset Value" as defined in MITS and the TBS draft standard.

Notwithstanding that HTRA states that "asset value" (as defined in MITS) is least useful, it is relabelled as "Replacement Cost" and is included in the HTRA Statement of Sensitivity analysis tables, but it is not used in determination of "Asset Value" (as used in HTRA formula for calculating Risk). It is all potentially very confusing to some readers.

TRA-1 Harmonized Threat and Risk Assessment Methodology

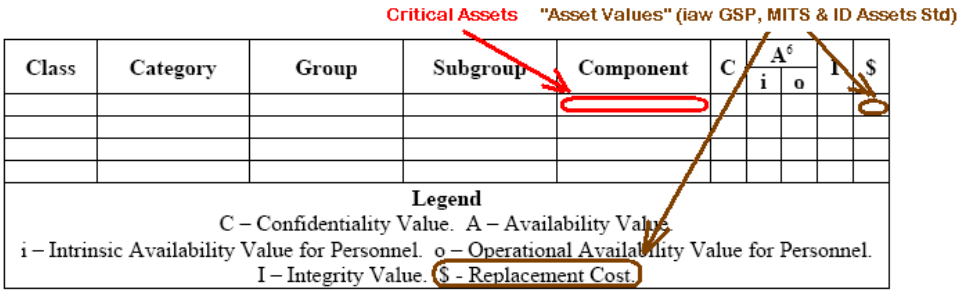


Table B-4: Sample Asset Valuation Table/Statement of Sensitivity

---

If use of the Harmonized TRA Methodology is a contractual requirement, the lead Risk Analyst should ensure that the client is made aware of the limitations discussed herein and should recommend that:

- Injury tests for critical assets which have significant estimated monetary or cultural worth use the "asset value" injury test criteria provided in the TBS draft standard. This is particularly important for large value financial business applications and the results should be appropriately considered in the determination of Risk; and
- Different terminology should be used for the high water mark of the values of Confidentiality, Integrity and Availability, if this high water mark is to be used in the HTRA formula for calculation of Risk.

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.

4.

Assets – Statement of Sensitivity (SoS) Analysis

The HTRA Methodology uses a tabular format for documenting Asset Categorization (or Valuation) for the Statement of Sensitivity has:

- A column with individual small cells for documenting the identification and description of the critical asset. There is only enough space to record the title of the critical assets.
- Small column on right side with individual small cells for documenting categorization results of the injury tests for Confidentiality (C), Availability (A), Integrity (I) and monetary Value ($).

TRA-1 Harmonized Threat and Risk Assessment Methodology

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

Critical Assets

results of injury tests

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

The HTRA Methodology tabular form does not include any injury test related rationale for Confidentiality, Integrity, Availability and Value categorization decisions.

Using such an abbreviated tabular approach in the performance of the SoS, the critical assets will be very high level and the categorization rationale will not be documented. The security Risk Analysts are almost encouraged to minimize such important risk management data because of the need to enter such information into a small cell of a table prescribed in a methodology.

If use of the Harmonized TRA Methodology is a contractual requirement, the lead Risk Analyst should ensure that the client is made aware of the limitations discussed herein and should recommend use of alternate tabular formats which allow more descriptive critical asset (i.e. business processes or information assets) details to be recorded and allow meaningful categorization rationale to be effectively recorded. The injury test rationale statements should always follow the table entries in text format, so as to not lose the rationale of the ratings as agreed by the business owners. An alternate example tabular format for recording the analysis is presented below.

Critical Assets - Statements of Sensitivity

Page 1

Crtical Assets	Confidentiality	Availability	Integrity	Value
CA001 - Operational Management Systems The main management system is the ____. This is a plant level enabler system that collects machine events data, transfers and distributes files/data from systems to equipment (and visa versa), and processes performance data. While the ____ can function without this device, after 8 hrs of downtime the manual work-a-rounds and inability to manage the MPE in real time lead to a rise in operating costs. There is financial information in this system. This asset category also includes Controllers which manage _____ suites and communicates with	Protected A While there is some system management and reporting data on the system, it has minimal sensitivity. There are some uniqu ____ codes which could provide volume information	Medium Loss of this equipment would lower the ability to effectively manage the environment. The performance would slowly degrade.	Medium The management data in the Operational Management Systems if modified could lead to ____making inappropriate management decisions resulting in higher operations costs. Significant corruption of this information would be evident; however, smaller errors could go un-noticed.	High This is the primary performance management system for the ____.
CA002 - National level _____ This critical asset comprises equipments directly associated with the national level_____. This includes everything in the standard ____ _____ processing streams, _____ and additionally includes the coded tray system and all associated equipment (e.g. PDP-11). Note that while the coded tray system supports the letter sortation process, it is a local system.	Protected A While some transient information is captured in ____ such as in the ____. this information is considered to have some sensitivity. There are some unique _____which could provide volume information associated ____	High The availability of this equipment is crucial for ____usiness operations. Interruption of this asset would have severe operational and financial impact.	Medium While integrity is important any major corruption of information would be corrected by manual system processes downstream _____	High ____ processing is key to ____ profitability. ____ has close to ____ in assets over_____ and related systems
CA003 _____ systems This critical asset includes all components of the _____ _____ equipment. In-line cubing weight and volume reporting is considered separately as it interfaces with the ____ system and the local sorters can function without this reporting function.	Protected A While some transient information is captured in ____ystems none of it is considered to be sensitivity. There are some uniqu _____ odes which could provide volume	High The availability of this equipment is critical for _____usiness operation. Interruption of these assets would have severe operational and financial impact.	Medium While integrity is important any corruption of information would be corrected by manual system processes downstream from sorting.	High Automated ____ is also key to ____ profitability, however, the relative volumes of _____ compared to

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons “Attribution 2.5 Canada” License.

5.

Threat Agent Definition

The HTRA sometimes uses the terms "Threat" and "Threat agent" interchangeably. The HTRA Annex C Threat Assessment Phase, Appendix C-1 Threat Listing (pages C2-1 – C2-6) provides a high level list of standard generic threats to consider. Below are the first 3 columns of the five column "Threat Listing" table:

Class	Activity	Category
Deliberate	War	Nation States
Deliberate	War	Revolutionaries
Deliberate	War	Rebels
Deliberate	Espionage	Hostile Intelligence Service
Deliberate	Espionage	Other State Sponsored Organizations
Deliberate	Espionage	News Media
Deliberate	Espionage	Industrial Espionage
Deliberate	Sabotage	State Sponsored
Deliberate	Sabotage	Competitor
Deliberate	Sabotage	Disgruntled Employees
Deliberate	Sabotage	Outside Activists
Deliberate	Sabotage	Hackers
Deliberate	Subversion	State Sponsored
Deliberate	Subversion	Political Activists
Deliberate	Subversion	Lobbyists
Deliberate	Subversion	Competitors
Deliberate	Subversion	Labour Unrest
Deliberate	Subversion	Hackers
Deliberate	Terrorism	International Terrorists
Deliberate	Terrorism	Domestic Terrorists
Deliberate	Criminal Acts	Insiders
Deliberate	Criminal Acts	Outsiders
Deliberate	Criminal Acts	Organized Crime
Deliberate	Criminal Acts	Others
Accidents	Office Accidents	Employees
Accidents	Lost Assets	Employees
Accidents	Lost Assets	Contractors
Accidents	Data Corruption	Employees
Accidents	Data Corruption	Clients
Accidents	Software Errors	Software vendors
Accidents	Software Errors	System integrators
Accidents	Software Errors	Internal Programmers
Accidents	Software Errors	System Administrators
Accidents	Hardware Failure	Hardware Vendors
Accidents	Hardware Failure	System Integrators
Accidents	Hardware Failure	System Administrators
Accidents	Mechanical Failures	Equipment vendors
Accidents	Mechanical Failures	Public Utilities
Accidents	Mechanical Failures	Building Custodians
Accidents	Mechanical Failures	Equipment Operators
Accidents	Structural Failures	Architects
Accidents	Structural Failures	Construction Industry
Accidents	Structural Failures	Building Occupants
Accidents	Fires	Employees
Accidents	Industrial Accidents	Transportation Workers
Accidents	Industrial Accidents	Manufacturing Teams
Accidents	Traffic Accidents	Employees
Accidents	Nuclear Accidents	Nuclear Power Plant
Accidents	Nuclear Accidents	Medical Facilities
Natural Hazards	Disease	Bacteria
Natural Hazards	Disease	Spirochete
Natural Hazards	Disease	Virus

HTRA Annex C Threat Assessment Phase, Sect 5.2.6 Level of Granularity (page C-16) provides the following threat definition guidance *"... 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 ..."*

There is a growing consensus among senior Risk Analysts that consideration of threat agents should often be *consolidated* (rather than "*rolled up*") based upon common attributes in order to lead to the selection of safeguards that would counter the threats/vulnerabilities in a unified manner. For example, in many cases the Risk Analyst should not be overly concerned about:

- whether it is employees, spies, hackers, or companies who want to attempt password exhaustion attacks. The Risk Analysts should recommend implementation of strong authentication and other safeguards to reduce the risk for all attackers.
- who is trying to sniff the network. The Risk Analyst should focus on those who have the best access/motivation/resources, and design encryption and other safeguards to defeat these threat agents.

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.

The HTRA threat profile definition guidance and required Threat Listing table shown below results in a generic and very high level approach in defining the threat profile to be addressed in a TRA.

TRA-1 Harmonized Threat and Risk Assessment Methodology

Appendix C-2 - Threat Listing

Threat Agents

Threat Events

	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

In the HTRA Threat Listing Table, the cells for identifying and describing Threat Agents and Threat Events are limited to about 12 and 25 characters respectively. As a result, the TRA analysis delivered to clients is also likely at a very high level. For risk management required to protect specific government operations, Government of Canada security critical systems and information, the threat profiles must be more granular in order that specific security controls can be selected to mitigate the risks.

By attempting to be comprehensive, the threat listing table is actually broad and shallow. It's hard to say there are omissions since the categories are so all-inclusive, but the rolled up categories are at such a high level as to be nearly useless to direct the analyst. So we have the threat of war and military invasion, and at the other end of the spectrum, algae poisoning in the water supply, yet we do not have the threat of password exhaustion attacks, identity spoofing, replay attacks, buffer overflows/other malformed input, etc.

Also, by repeating various threat events for various threat agents, the analyst potentially gets an N x M expansion of the table, and this can result in a loss of analytical focus due to the large table. The more relevant threat scenarios can get hidden by the "included, just to be complete" table entries. For example: organized crime, foreign governments, disgruntled employees or hackers could cause denial of service attacks, intercept data, or exploit networks. This approach can cause an explosion of table entries (4 agents x 3 events in this small example). (Add this to later permutations of vulnerabilities, and the analyst literally gets an exponential expansion of items to analyze.)

In many cases, the use of the HTRA high-level threat profiles approach should actually be discouraged in order that the Security Controls Profiles (high granular security control baselines) can effectively and efficiently be used and tailored for protecting individual security critical systems.

If use of the Harmonized TRA Methodology is a contractual requirement, the lead Risk Analyst should ensure that the client is made aware of the limitations discussed herein and should recommend to the client that:

- a more granular approach be used for defining threats to individual security critical systems rather than the high level generic approach used in the HTRA Methodology; and
- threats agents should be assigned **unique identifiers** to facilitate:
  - Traceability of considered threat agents within subsequent sections of the TRA report;
  - repeatability of threat assessment and quality assurance by TRA Analyst and/or Technical Authority;
  - Potential reuse or leveraging of the threat profile for other facilities or systems within the Client's organization; and
  - Use of relational databases (such as MS Access, Corel Paradox, etc ...) or spreadsheet based automated tools for performing complex interrelated risk analysis.

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.

6.	**Threat Events – Simplification & Consolidation** HTRA Annex C Threat Assessment Phase, Sect 2.5.1 (page C-4) defines a Threat Event as "*An actual incident in which a threat agent exploits a vulnerability with potentially adverse effects on an asset of value."* In the HTRA the term "Threat Scenario" is sometimes used interchangeably with "Threat Event" HTRA Annex C Sect 5.2.6 (page C-16) provides the following threat event level of detail guidance "*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*." The HTRA Methodology does not provide an organized approach for addressing modern "*temporal risk*" based attacks. Such temporal risks are associated with threats that occur as a result of a concerted attack of seemingly independent and minor probes that are coordinated over a period of time -- months, typically. Patient attacks and threats are very worrisome in that it's the result of an accumulation of patient, trivial attacks that may be totally ignored as individually they aren't that big a deal but collectively they are very dangerous. The HTRA guidance for consolidating and documenting threat events in limited cells of analysis tables often results in identification of higher level security controls (or safeguards) and a lack of lower level system specific controls needed to effectively and efficiently mitigate system or application specific risks. In addition, the use of this simplified HTRA approach for consolidated threat events is not consistent with effective and efficient use of detailed lower level of detail system or product security specific standards. best practices documents or government security controls baseline documents (i.e. NIST SP 800-53, NSA SNAC family of guides, DoD DISA STIG family of guides, various CSEC lower level IT Security Guides (ITSGs) ...) --- If use of the Harmonized TRA Methodology is a contractual requirement, the lead Risk Analyst should ensure that the client is made aware of the limitations discussed herein and should recommend that: • A more detailed approach (than the HTRA consolidation approach of using limited cells in analysis tables) be used for defining and documenting threat events be used for performing TRAs on security critical systems; • Threat Scenarios for security critical systems must clearly include and identify: system related critical asset(s) to protect, vulnerabilities of concern, likely threat agent, likely consequences (i.e. loss of specific confidentiality, integrity or availability) in language understandable by business owners; and • Threat Scenarios should be assigned unique identifiers, title and description. The addressed critical assets and threat agents would be identified using their respective unique identifiers. Where the assessed residual risks exceed the target residual risk level, a list of recommendations proposing additional safeguards (with their unique identifiers) to achieve the target residual risk level is to be provided with an assessment of their effectiveness and cost. The use of unique identifiers for existing and recommended safeguards will also facilitate identification of higher priority recommendations due to their impact on multiple Threat Scenarios.

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.

7.	**Use of Security Standards – Safeguard Selection** The simplified HTRA approaches for consolidating Threat Events (see related analysis entry #5) and rolling-up Threat Agents to a higher level "category" or "activity" level (see related analysis entry #6) are not consistent with effective and efficient safeguard selection from standards. The HTRA Methodology does not select safeguards from detailed lower level of detail system specific or product specific security standards, best practices documents or government security controls baseline documents (i.e. NIST SP 800-53, NSA SNAC family of guides, SANS 20 Critical Controls for Effective Cyber Defence, DoD DISA STIG family of guides, various CSEC ITSGs ...) The HTRA does not clearly advocate use of such security controls standards in TRAs and provides following negative (or ambiguous) guidance related to their utility in TRAs for selection of Safeguards: • HTRA Sect 3.3.12, (page F-8): *(... conformity with approved standards offers little indication of relative safeguard effectiveness for the purposes of comparative analysis amongst different options. ...*) • HTRA Sect 4.4, (page A2-9): (*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 ...*) As worded, this HTRA guidance implies that such standards are useful to apply as a quick solution and are not useful as source of safeguards to consider within a TRA. • HTRA Sect 3.4.1, (page A2-7): (... *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*.) As worded, this HTRA guidance implies to the reader that such standards are useful to counter worst-case scenarios and are not useful as source of safeguards to consider within a TRA. • HTRA Sect 3.4.2, (page A2-7): *(...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. ... 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.)* The relationship between the risk assessment and standards should be clarified and supported in guides such as the HTRA. Standards fundamentally provide the mechanism to reuse expensive TRA findings and apply them in a manner which is also supportive of security architectural standardization. It is acknowledged that such standards do become stale in a fast moving IT world, so they must be refreshed often. The use of such standards should also be used to encourage development of Departmental standards to facilitate less costly certification and accreditation of highly similar systems within common security architectures. --- If use of the Harmonized TRA Methodology is a contractual requirement, the lead Risk Analyst should ensure that the client is made aware of the limitations discussed herein and should recommend that: • Security standards and profiles be used in the selection of security controls and determination of residual risks to security critical systems, notwithstanding the negative guidance on use of such standards in the HTRA Methodology.

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.

8.

Security Controls (Safeguards) Selection

The HTRA does not provide any guidance on using standard security requirements baselines such as those documented in various standard security controls catalogues. (See related analysis entry #7)

> In other (i.e. not using HTRA Methodology) TRAs, this initial baseline set of safeguards is often selected from a standard security controls catalogue relevant to the business, operational and compliance assessment focus of the client. Example best practice security controls catalogues considered are NIST SP 800-53, Payment Card Industry Data Security Standard (PCI DSS), SANS 20 Critical Security Controls and ISO/IEC 27002 Code of Practice for Information Security Management. The initial relevant security controls baseline is then tailored and enhanced with additional or compensating controls during the TRA to arrive at the required set of security controls to reduce residual risks to acceptable levels.

Rather using standard catalogues of security controls, the HTRA provides a high level hierarchical (Class, Group and Safeguard) **Safeguard Listing**. See extract below. The HTRA (Appendix F-2 Safeguard Listing (pages F2-1 – F-2-9) is very high level compared to level of detail found in standard security control catalogues. The HTRA listing only provides the title of each security control and does not provide functional or implementation details. The user would need to consult the cited references (GSP, MITS, MG-series, ITSGs, etc ...) for any needed security, functional or implementation details.

TRA-1 Harmonized Threat and Risk Assessment Methodology

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									
[illegible]				I, T, S	√	√			[illegible]
[illegible]			√					E, C	
[illegible]ergency 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	√		√		MITS 16.4.4, ITSD-01 Annex C, ITSB-013, [illegible]9, ITSG-13

HTRA provides some general guidance on use of the Safeguard Listing:

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons “Attribution 2.5 Canada” License.

- Annex D Vulnerability Assessment, Sect 2.2, (page D-2) Safeguard Listing*: (...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 aidemémoire to facilitate the Safeguard Identification Process within the Vulnerability Assessment.);*
- Appendix D-3 Vulnerability Metrics, Sect 1, (page D3-1), Instructions: *(For each vulnerability exposing assets to threats ..., 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. ...);*
- Appendix F-2 Safeguard Listing, Footnote 1, (page F2-7): (*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 ...:*
  - *Columns 2-4 indicate which of the three risk variables might be lowered by the safeguard, asset values (AVal), 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. ...* "
- Appendix F-2 Safeguard Listing, Footnote 2, (page F2-9): (*The Safeguard Listing should be employed with caution for it cannot be complete and there are exceptions to many entries. ... 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.*)

Many TRAs which have been conducted using the HTRA Methodology, only use the Safeguard Listing titles in the analysis and thus do not provide low level functional, security or implementation details which might be extracted from the referenced documents. Poorly detailed safeguard descriptions (existing and recommended) cannot be implemented securely without additional analysis and documentation.

The HTRA model does not provide clear guidance for a Risk Analyst or a client to easily call up a TRA's results (i.e. recommended safeguards) in order to move forward in an organized ongoing risk management manner. The current model is more fashioned towards measuring status of risk at a point in time whereby the report (including recommended safeguards) is created and then perhaps just filed. It would be more effective if a set of detailed security requirements were clearly the required output of the TRA which would then drive an implementation work plan, Statements of Work (SOW), or Request for Proposals (RFP) ... etc. in a subsequent body of work to address the found risks.

Since the HTRA was issued in 2007, no new material has been added to the Safeguard Listing to address changes to threat environments, standard security architectures, new technologies (i.e. virtualization) or suggestions from user departments. In addition, the list of references which are intended to "*describe the safeguard and its intended use*" is now very much out-of-date.

If use of the Harmonized TRA Methodology is a contractual requirement, the lead Risk Analyst should ensure that the client is made aware of the limitations discussed herein and should recommend that:

- Needed safeguards should be selected from standard security controls catalogues (such as NIST SP 800-53, Payment Card Industry Data Security Standard (PCI DSS), SANS 20 Critical Security Controls and/or ISO/IEC 27002 Code of Practice for Information Security Management), rather than from the HTRA high level Safeguard Listing;
- Safeguards effectiveness details are documented in more than small cells of HTRA analysis tables;
- Detailed security requirements are the required output of the TRA which would then drive an implementation work plan, SOW, or RFP ... etc. in a subsequent body of work to address the found risks; and
- All safeguards should be assigned **unique identifiers** to facilitate:
  - Traceability of existing and recommended safeguards in subsequent sections of the TRA;
  - Repeatability of safeguard selection analysis and quality assurance by TRA Analyst and/or Client's Technical Authority;
  - Standard approach for identifying controls which may be common across many threat

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.

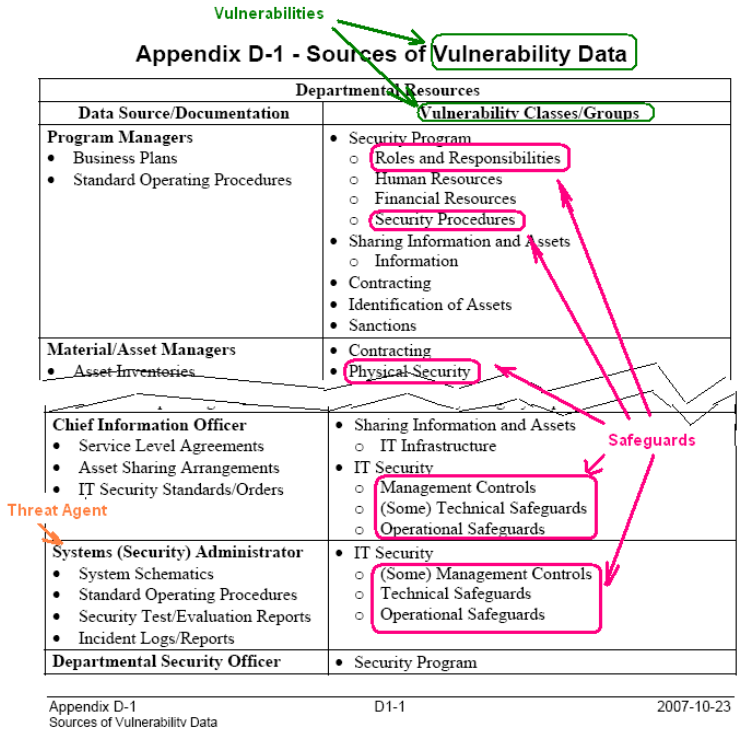
	events in this TRA. This approach will allow quicker determination of business or operational impact of implementing specific controls by identifying those higher priority recommended safeguards which potentially mitigate risks for multiple threats events; - Potential reuse or leveraging of the safeguard selection analysis for other systems or facilities within the Client's organization; - Traceability to requirements in standard security control catalogues and in government security standards such as TBS Management of Information Technology Security (MITS); and - Use of relational databases (such as MS Access, Corel Paradox, etc ...) or spreadsheet based automated tools for performing complex interrelated risk analysis.

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.

9.

Relationship between Vulnerabilities, Safeguards and Threat Agents

The HTRA Methodology Section 4.3 “Sources of Vulnerability Data” provides the following Appendix D-1 table as a guide to be used by Risk Analysts when identifying vulnerabilities to be addressed in the TRA..



Appendix D-1 - Sources of Vulnerability Data

Departmental Resources	
Data Source/Documentation	**Vulnerability Classes/Groups**
Program Managers • Business Plans • Standard Operating Procedures	• Security Program ○ Roles and Responsibilities ○ Human Resources ○ Financial Resources ○ Security Procedures • Sharing Information and Assets ○ Information • Contracting • Identification of Assets • Sanctions
Material/Asset Managers • Asset Inventories	• Contracting • Physical Security
Chief Information Officer • Service Level Agreements • Asset Sharing Arrangements • IT Security Standards/Orders	• Sharing Information and Assets ○ IT Infrastructure • IT Security ○ Management Controls ○ (Some) Technical Safeguards ○ Operational Safeguards
Systems (Security) Administrator • System Schematics • Standard Operating Procedures • Security Test/Evaluation Reports • Incident Logs/Reports	• IT Security ○ (Some) Management Controls ○ Technical Safeguards ○ Operational Safeguards
Departmental Security Officer	• Security Program

Appendix D-1 D1-1 2007-10-23
Sources of Vulnerability Data

The Appendix D-1 table includes a combination of:

- sources of vulnerability information;
- types or categories of security safeguards; and
- some potential threat agents such as privileged users (Systems Administrators)

This table introduces some confusion as to what is vulnerability and what is a safeguard. To the more experienced Risk Analysts, this may not be a significant issue; however for new, junior or inexperienced analysts this table introduces confusion regarding relationships between Threats, Vulnerabilities and Safeguards.

See related analysis entry #10.

If use of the Harmonized TRA Methodology is a contractual requirement, the lead Risk Analyst should ensure that the client is made aware of the limitations discussed herein and should recommend that Appendix D1 table “Sources of Vulnerability Data” only be used as a rough guide and that meaningful and relevant vulnerabilities will be identified and analysed for the scope of the TRA, as discussed in analysis entry #10.

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons “Attribution 2.5 Canada” License.

10.

Vulnerability Analysis

The HTRA guidance in the Vulnerability Listing table generalizes vulnerabilities at a high level and the lower level details are largely left to the interpretation of the Risk Analyst.

Appendix D-2 - Vulnerability Listing

Vulnerabilities

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		√	√	√	√	√
		[illegible]		√	√			
		Emergency Destruction		√		√		
IT Security	Management Controls	System Development Life Cycle		√	√	√	√	√
		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		√		√	√	√

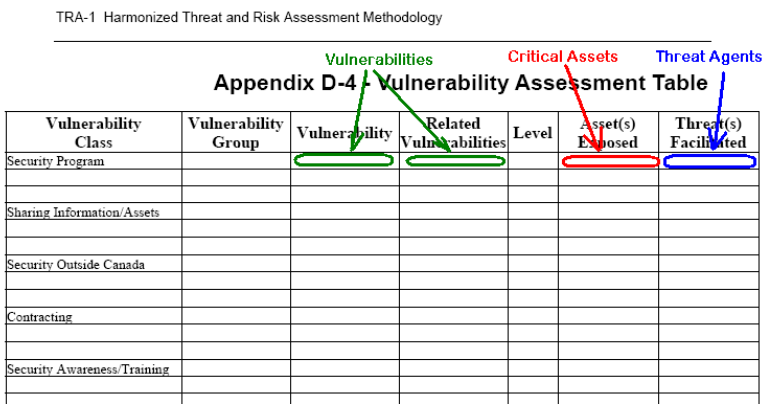
The "IT Security" section of the Vulnerabilities Listing table is inadequate and does not clearly address the common IT security vulnerabilities – the ones we have been wrestling with for years. For example: lack of input validation, use of fixed passwords, the entire family of user password vulnerabilities (too short, too easy to guess, excessive lifetime, shared passwords, not protected in transit, etc.), presence of back doors, lack of encryption for data at rest or in transit, excessive privilege for persons and processes, integrity vulnerabilities (replay, deletion, weak hashing, etc.), lack of separation of security critical code from other code, lack of protection of audit trails, cryptographic vulnerabilities (bad random number/initialization vector generation, bad key management through the life cycle, short keys, weak algorithms/improper implementations), network attacks (attacks against DNS, trust attacks, attacks against time services, denial of service/flooding,) etc.

In addition the Vulnerabilities Listing table does not clearly address vulnerability areas such as the following:

- Complex hacker attack vectors through sequences of different vulnerabilities in multi-server network architectures;
- Modern "temporal risk" based attacks that occur as a result of a concerted attack of seemingly independent and minor probes that are coordinated over a period of time -- months, typically;
- Interrelated social engineering, technical and other vulnerabilities targeted in newer multi phase cyber crime vectors focussed on specific persons and information;
- "*zero day vulnerabilities*" exploited by threat agents to target an organization's critical information and fiscal assets;
- Potential vulnerabilities introduced with introduction of server and desktop virtualization;
- Vulnerabilities specific to protecting industrial controls systems (aka SCADA -supervisory control and data acquisition systems); and
- Application software vulnerabilities.

The HTRA does not provide any guidance on including vulnerability findings of prior or concurrent server penetration testing (aka onsite technical vulnerability assessments (OTVAs)) in the TRA analysis

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.



In the HTRA Vulnerability Assessment Table, the cells for identifying and describing Vulnerabilities are limited to about 12 characters. As a result, the vulnerability analysis delivered to clients is at high level.

If use of the Harmonized TRA Methodology is a contractual requirement, the lead Risk Analyst should ensure that the client is made aware of the limitations discussed herein and should recommend that:

- vulnerabilities be documented in more detail than that allowed by the small cells of HTRA analysis tables;
- more meaningful vulnerabilities than those provided in the HTRA Vulnerability Listing table be considered; and
- vulnerability findings from prior or concurrent penetration tests be considered in the TRA analysis.

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons “Attribution 2.5 Canada” License.

11.

Analysis Tables to be Completed – Traceability and Repeatability

The Harmonized TRA Methodology is very process oriented with many different analysis tables to be completed by the Risk Analyst during each phase. Below are some of the major analysis tables which are required by the HTRA Methodology. (See analysis entries #3, #4 and #10 for additional HTRA analysis tables.)

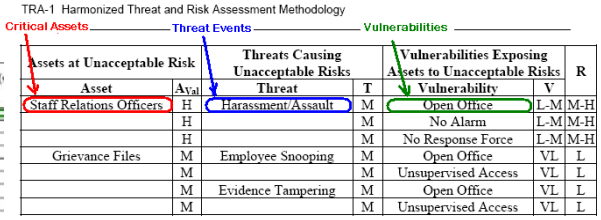
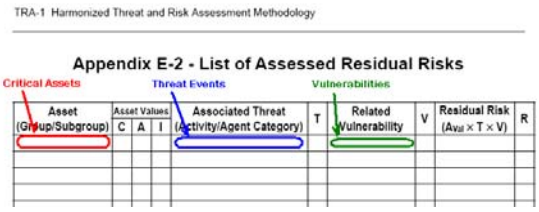
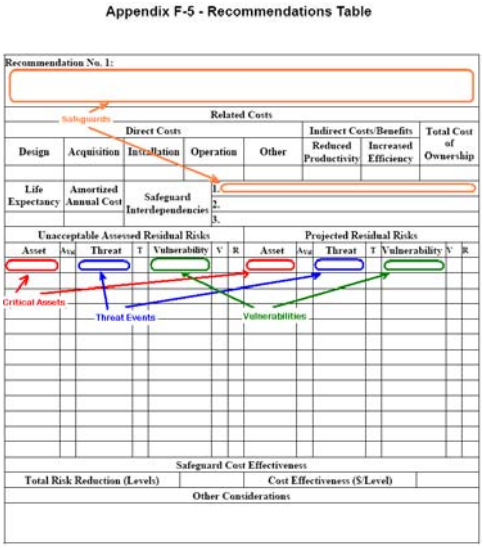


Table F3-4: Projected Residual Risks with a Locked Entrance and Escorted Access





The HTRA analysis recorded in the rows in each table, are not clearly associated with the analysis recorded in the rows of other analysis tables completed in other phases. (Other methodologies use the concept of uniquely numbered Threat Scenarios to provide this logical linkage between related analyses recorded in different analysis tables. Specific Threat Events initiated by a Threat Agent to compromise an identified Critical Asset by exploiting both Vulnerabilities and inadequate Safeguards is referred to as a Threat Scenario.)

With shorthand notations being used in multiple tables, it is very difficult to combine or compare TRAs done by different individuals as they typically have differing views on what is important and should be recorded in the small cells of the HTRA tables.

With numbered Threat Scenarios <u>not</u> being used and the lack of unique identifiers for Threat Events, Threat Agents, Critical Assets and Safeguards it is difficult to show traceability of the TRA analysis from some of the tables to the next table. In addition, the cells for identifying and describing Critical Assets, Threat Events, Threat Agents and Vulnerabilities are limited to about 12 to 15 characters in most cases.

Risk analysis details supporting ratings is not recorded due to the small-cell, table structures. From a QA reviewer's perspective, the evidence of the analysis in the deliverable report is often lacking and necessitates questions of clarification with the Risk Analyst.

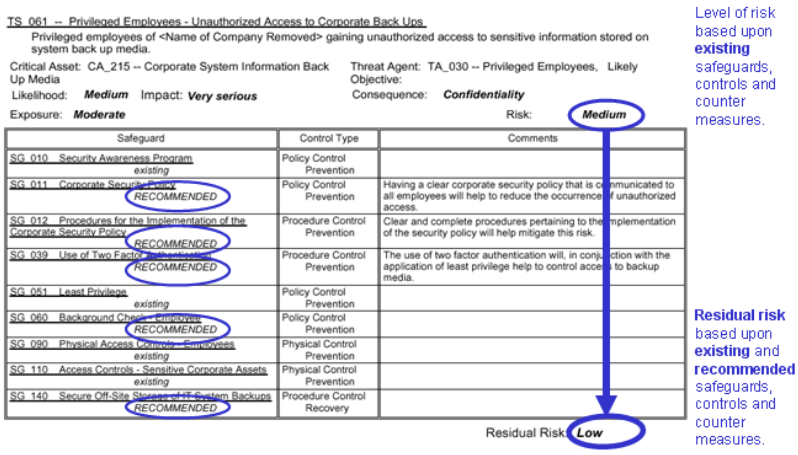
If use of the Harmonized TRA Methodology is a contractual requirement, the lead Risk Analyst should ensure that the client is made aware of the limitations discussed herein and should recommend that alternate tabular formats based on the used of the unique Threat Scenarios analysed be used for documenting the TRA analysis rather than those used in the HTRA Methodology. Such alternate tabular formats should include the use of unique identifiers and detailed descriptions of analytical elements (Critical Assets, Threat Agents, Threat Events, and Safeguards) being addressed in the Threat Scenario being analysed.

An alternate tabular format for recording the analysis is presented below. This example page is for an individual Threat Scenario where the relevant Critical Assets, Threat Event, Threat Agent, Vulnerabilities, Safeguards and Risk details are recorded. This Threat Scenario based tabular format

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.

could be tailored to address unique needs of the client and the methodology.

Recommended" Safeguards in context of Risk Mitigation Decisions



TS_061 -- Privileged Employees - Unauthorized Access to Corporate Back Ups

Privileged employees of <Name of Company Removed> gaining unauthorized access to sensitive information stored on system back up media.

Critical Asset: CA_215 -- Corporate System Information Back Up Media

Threat Agent: TA_030 -- Privileged Employees, Likely

Objective:

Likelihood: ***Medium*** Impact: ***Very serious***

Consequence: ***Confidentiality***

Exposure: ***Moderate***

Risk: ***Medium***

Safeguard	Control Type	Comments
SG_010 Security Awareness Program *existing*	Policy Control Prevention	
SG_011 Corporate Security Policy *RECOMMENDED*	Policy Control Prevention	Having a clear corporate security policy that is communicated to all employees will help to reduce the occurrence of unauthorized access.
SG_012 Procedures for the Implementation of the Corporate Security Policy *RECOMMENDED*	Procedure Control Prevention	Clear and complete procedures pertaining to the implementation of the security policy will help mitigate this risk.
SG_039 Use of Two Factor Authentication *RECOMMENDED*	Procedure Control Prevention	The use of two factor authentication will, in conjunction with the application of least privilege help to control access to backup media.
SG_051 Least Privilege *existing*	Policy Control Prevention	
SG_060 Background Checks - Employees *RECOMMENDED*	Policy Control Prevention	
SG_090 Physical Access Controls - Employees *existing*	Physical Control Prevention	
SG_110 Access Controls - Sensitive Corporate Assets *existing*	Physical Control Prevention	
SG_140 Secure Off-Site Storage of IT System Backups *RECOMMENDED*	Procedure Control Recovery	

Residual Risk: ***Low***

Level of risk based upon **existing** safeguards, controls and counter measures.

Residual risk based upon **existing** and **recommended** safeguards, controls and counter measures.

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons “Attribution 2.5 Canada” License.

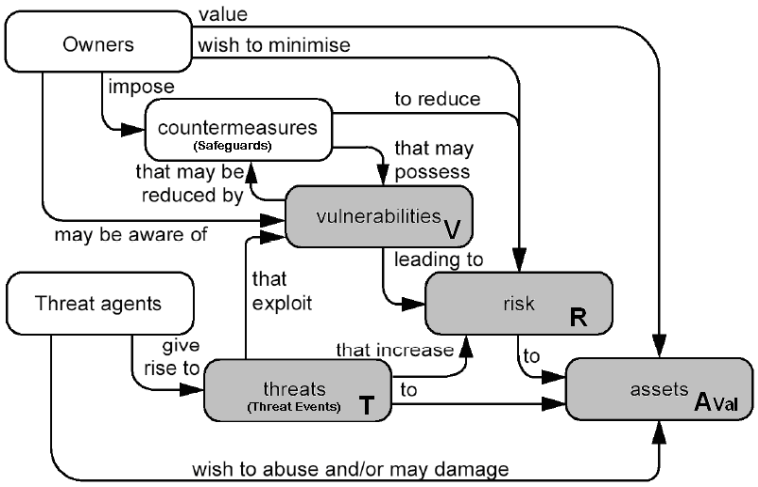
12.

Residual Risk Analysis

The HTRA Appendix A-2 page A201 states "*risk (R) may be described as a functional relationship amongst asset values (A_{Val}),, Threats (T) and Vulnerabilities (V).*"

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

The HTRA Methodology does not directly consider existing and recommended Safeguards or the Threat Agents in the calculation of Risk.



The HTRA Methodology Risk calculation uses a "high water mark" scheme where the Asset Value is taken to be the highest of the 3 security parameters (Confidentiality, Integrity and Availability). Based on this high water mark, a numerical parameter between 1 and 5 is assigned to **A_{Val}**.

The HTRA Methodology Risk calculation uses a five level scheme (VL, L, M, H and VH) for both Threats and Vulnerabilities. Using this scheme, a numerical parameter between 1 and 5 is assigned to both **T** and **V**.

The 3 parameters are then simply multiplied to calculate the "risk score".

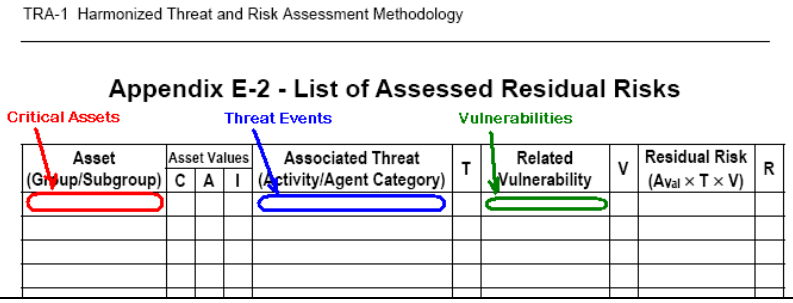
$$\textbf{Risk Score} = (A_{Val} \times T \times V)$$

This "risk score" is used to look-up the "Risk Level" (R) using HTRA page E1-2, Table E1-2. (It should be noted that table E1-2 and related HTRA guidance is ambiguous for risk scores of 13, 14, 33, 34, 35, 76, 77, 78, and 79)

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

The HTRA Methodology requires that the calculations and "Risk Scores" be recorded in tabular form.


TRA-1 Harmonized Threat and Risk Assessment Methodology

Appendix E-2 - List of Assessed Residual Risks

Critical Assets — Threat Events — Vulnerabilities

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

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.

The HTRA provides one example of such a completed calculation where the Availability (A) sensitivity parameter is taken to be the *High Water Mark* **Aval**:

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

The HTRA risk calculations are based on a scoring method using "ordinal" scales. A recent paper by Hubbard and Evans [16] has some very relevant findings on how the type of scale and definition of what the values in the scale mean and how they can affect the accuracy of the risk assessment. They are critical of "ordinal" scales in particular. "Probabilistic" scales are recommended if they represent, or are derived from quantitative probability estimates.

The risk level formula and rating guide does not consider safeguard effectiveness, creating excessive residual risk ratings in certain circumstances for "very high" "5" value assets. For such "very high" asset values in the HTRA formula, the risk cannot be effectively lowered, regardless of safeguards applied.

The lack of an input parameter for safeguards is a serious omission for both risk and residual risk. It may be possible to somehow factor in a basic security safeguard posture when assessing vulnerabilities, but it seems error-prone and difficult for auditors and general readers of the TRA to perform traceability on the vulnerability assessment. It is difficult to see the value of this approach unless the HTRA has the premise that the analysis can be performed faster and arrive at the same conclusions by not considering the protective function of existing safeguards. However experience indicates that this is not the case. Some safeguards do work directly on a specific vulnerability. Other safeguards mitigate the composite risk in a more indirect manner by transferring it to other agencies, etc. or by working in combination with other safeguards.

The relationship between safeguards and vulnerabilities, threat agent motivation, and even the valuation of assets is sometimes complex and often needs to be fully documented.

When calculating residual risk, the consideration of recommended safeguards is even more important. For example, there would be no way to apply the methodology of ISO 27001 and produce a document called the Statement of Applicability (SOA)[17], without using an explicit residual risk based on mitigating safeguards, or "controls". The SOA is the blueprint for acquisition of new safeguards for the organization and justifies their procurement to upper management by directly linking these acquisitions to risk reduction.

Prior to the introduction of the HTRA, a blend of the RCMP SIP-5[18] and the CSEC (ITSG-04[19], MG-2[20], MG-3[21], and MG-4[22]) methodologies was used. In this methodology, the Risk was determined in a subjective manner, however the Risk was clearly considered to be a function of

[16] *Problems with scoring methods and ordinal scales in risk assessment*, D. Hubbard, D. Evans, (published in IBM Journal of Research and Development, May/June 2010), available at www.dylan.org.uk/ordinal.pdf

[17] The statement of applicability identifies the controls chosen for environment, and explains how and why they are appropriate. The SOA is derived from the output of the risk assessment/ risk treatment plan and, if ISO27001 compliance is to be achieved, must directly relate the selected controls back to the original risks they are intended to mitigate. Normally the controls are selected from ISO27002, but it is possible to also include own controls. A number of sector specific schemes are being introduced which stipulate additional mandatory controls. Reference: http://iso-17799.safemode.org/index.php?page=Statement_of_Applicability

[18] RCMP Security Information Guide 5, Guide to Threat and Risk Assessment for Information Technology, Nov 1994

[19] Threat and Risk Assessment Working Guide (ITSG-04), Communications Security Establishment (CSEC), Oct 1999

[20] A Guide to Security Risk Management for Information Technology Systems, Communications Security Establishment (CSEC), Jan 1996

[21] A Guide to Risk Assessment and Safeguard Selection, Communications Security Establishment (CSEC), January 1996

[22] A Guide to Certification and Accreditation for Information Technology Systems (MG-4), Communications Security Establishment (CSEC), Jan 1996

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.

considerations related to the Critical Assets, Threat Events, Safeguards and Vulnerabilities.

$$\mathbf{R = \mathit{f}\ (A, T, S, V)}$$

Below is a table from SIP-5 which illustrates this functional relationship between calculated Risk based upon the Critical Assets, Threat Events, Safeguards and Vulnerabilities. In this methodology, the motivation and likelihood of Threat Agents was also indirectly considered.

RCMP SIP 5, Guide to TRA for Information Systems, Nov 1994

Critical Assets Threat Events Safeguards Vulnerabilities

ASSET	THREAT	Risk Assessment		
		EXISTING SAFEGUARDS	VULNERABILITIES	RISK
Describe the asset	Describe the specific threat against it	Describe existing safeguards to protect the asset against the threat	Describe any vulnerabilities that may be observed	Establish the risk level

TABLE 6 – Generic Risk Assessment

If use of the Harmonized TRA Methodology is a contractual requirement, the lead Risk Analyst should ensure that the client (including the business risk owner) is made aware of the limitations discussed herein and should recommend that alternate formulas be used for calculating risk which include the direct consideration existing and recommended Safeguards and motivation and likelihood of Threat Agents in the calculation of Risk

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons “Attribution 2.5 Canada” License.

13. **Certification and Accreditation - Guidance**

The HTRA Methodology does not provide any guidance related to Certification and Accreditation of systems. In Section 2.3 *Certification and Accreditation (C&A)* of *Annex G – Conclusions,* it is stated in footnote 2 that such guidance is to be found in CSEC *Guide to Certification and Accreditation for Information Technology Systems* (MG-4).

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.

Annex G Conclusion G-3 2007-10-23

MG-4 is "*Under Review*" and is no longer available on the CSEC web site.

MG-2 A Guide to Security Risk Management for Information Technology Systems

* *Under review. For any question, please email Client Services at: itsclientservices@cse-cst.gc.ca*

MG-3 A Guide to Risk Assessment and Safeguard Selection for Information Technology Systems

* *Under review. For any question, please email Client Services at: itsclientservices@cse-cst.gc.ca*

MG-4 A Guide to Certification and Accreditation for Information Technology Systems

* *Under review. For any question, please email Client Services at: itsclientservices@cse-cst.gc.ca*

To read these files download the free Adobe® Acrobat® Reader which allows you to view, navigate, and print PDF files across all major computer platforms.

Last Modified: 2010-11-03 Important Notices

Currently there are no publicly available C&A guidance documents available to Risk Analysts to use for ensuring that TRAs performed using the HTRA Methodology and the deliverables are consistent with the needs of the system Certification and Accreditation and system development life cycle (SDLC).

If use of the Harmonized TRA Methodology is a contractual requirement, the lead Risk Analyst should ensure that the client is made aware of the limitations discussed herein and should recommend that CSEC be requested to provide archive copies of MG-4 (or other C&A specific guidance) to be used for any C&A related guidance.

© 2011 BD Pro Inc. -- Copies and extracts are allowed with attribution.
This work is licensed under the Creative Commons "Attribution 2.5 Canada" License.