SECURITY INFORMATION PUBLICATION 5

Guide to Threat and Risk Assessment For Information Technology

November 1994

This guide has been developed and issued by the IT Security Branch of the RCMP. The responsibilities of the RCMP, as outlined in the Security Policy of the Government of Canada include, "developing, approving and issuing particular technical documents on information technology security;... and advising on their application" and "providing advice on threat and risk assessments, when requested;..." The preparation of this guide is one activity undertaken by the RCMP toward fulfilment of its role as a lead agency.

Table of Contents

Table of Contents

Guide to Threat and Risk Assessment For Information Technology

1. Introduction

This guide is intended to assist practitioners in assessing the threats and risks to Information Technology (IT) assets held within their organizations, and in making recommendations related to IT security. The objective of a threat and risk assessment (TRA) is to involve the various players and gain their support, to enable management to make informed decisions about security and to recommend appropriate and cost-effective safeguards. An assessment of the adequacy of existing safeguards also forms part of the TRA process. Where this assessment indicates that safeguards are inadequate to offset vulnerabilities, additional safeguards are recommended. Also, where the TRA indicates that certain safeguards are no longer needed, the elimination of those safeguards is recommended. A TRA does not result in the selection of mechanisms of prevention, detection and response to reduce risks; instead, it simply indicates the areas where these mechanisms should be applied, and the priorities which should be assigned to the development of such mechanisms. Within the context of risk management, the TRA will recommend how to minimize, avoid, and accept risk.

Planning for the TRA process encompasses establishing the scope of the project, determining the appropriate methodology, setting the time frame, identifying the key players and allocating resources to perform the assessment. Those involved in the TRA process must be cautioned to protect the sensitivity of working papers produced during the process. These working papers often contain information related to the vulnerability of systems and environments, and should be protected at a level commensurate with the most sensitive information available on those systems.

Consideration must be given to specific organizational characteristics that might indicate the need for a strengthened security profile. Such characteristics might include the organization's mandate, the location (i.e. remoteness) and the organization's composition in terms of environment ("hostile", public access) and resources.

2. Process

To conduct a TRA, the following four-step process is typically followed:

Preparation:	determining what to protect;
Threat Assessment:	determining what to protect against, consequences of a threat;
Risk Assessment:	determining whether existing or proposed safeguards are satisfactory; and
Recommend-ations:	identifying what should be done to reduce the risk to a level acceptable to senior management.

Each of these steps is described in detail in subsequent sections.

2.1. Preparation

2.1.1. Defining the Environment

a) Determining the Scope of the Threat and Risk Assessment

Prior to the actual conduct of the TRA, it is necessary to establish its scope which will include the systems under consideration, the interconnectivity with other systems and the profile of the user community. The entire TRA process will often span a number of systems and environments. Thus, in determining the scope, care must be taken to ensure that priorities are set to determine an appropriate order of assessment, i.e. that areas of primary concern or sensitivity are assessed first.

b) Identifying Team Participants

Once the scope of the TRA has been established, the practitioner can establish a representative team of users of the system under consideration. For example, let us suppose that the system contains several applications used by a variety of groups within the institution. To provide a valid cross section of the information

required to conduct the TRA, users, developers, and telecommunications and operations staff must be selected for the team. This team will (at a later step) provide the practitioner with the information required to identify known threats and their potential impact.

c) Determining Intrinsic Concerns

All organizations have certain security concerns that are directly related to the nature of their business. The practitioner should document these special concerns, as they will be instrumental in determining the appropriateness of existing security measures and in making recommendations for improvements.

d) Developing the Baseline

Once the preliminary work is completed, the practitioner can establish the current profile of the organization's security posture. These parameters establish what is known as the security baseline for the TRA process. It is from this baseline that the risks are assessed, and any updates to the TRA are prepared. For example, when a particular safeguard is recommended, that safeguard and its defining recommendation are referred directly to the baseline. A baseline against which recommendations can be made is necessary for two reasons:

1) The baseline provides a starting point for any measurement of progress.

2) The environment is subject to continual change.

The first point provides the practitioner with a means of determining what changes have been made to the environment and how security has been impacted by those changes. The second point allows the practitioner to identify the difference between the current security profile and any future requirements for security, given the changes to the environment which have taken place since the baseline was established.

2.1.2. Assets Identification and Valuation

Identifying IT assets according to their physical and logical groupings can be a difficult task, depending on the size of the organization and the soundness of supporting activities such as materiel management and the availability of comprehensive inventories. The practitioner must identify those assets that form the IT environment, and then assign a value to them. The participants identified in the preparation stage will be instrumental in identifying and assigning value to assets. In the case of IT applications, the "owners" of the information processed by those applications are responsible for preparing the statement of sensitivity[1] which will detail the specific sensitivity requirements for each application in terms of confidentiality, integrity and availability.

The practitioner must consider several aspects contributing to the worth of an asset including, but not limited to, the initial cost of the item. An asset may have an **acquired** value that far outweighs the initial cash outlay. Consider the example of the data collected by geologists during a summer survey of a remote northern area. The project objective may be to collect the data while the area is accessible and interpret and analyse the data over the winter months. The value could be considered to be equal to the cost of the survey in terms of scientists' time, support and travel costs. However, suppose the data is lost in September (therefore not available) and the area is inaccessible until spring. The geologists will have lost an entire year's work plus the cost of the initial survey in that the data must be gathered again the following summer. The asset value must be increased by the costs associated with an additional year's support, time and travel costs as well as any uniqueness in time, conditions and opportunity.

The question of using qualitative versus quantitative methods in the determination

[1] Statements of sensitivity will be discussed in Section 2.1.4.

of asset value must also be addressed. When considering the acquired value of certain assets, it may be more meaningful (than assigning a dollar value) to establish the relative value of an asset within the context of the organizational objectives and mandate. This relative value can be expressed in terms of the confidentiality, integrity and availability requirements for that asset.

2.1.3. Confidentiality, Integrity and Availability (CIA) Requirements

The CIA requirements are identified in the statement of sensitivity discussed in section 2.1.4.

Confidentiality
Confidentiality is used in the context of sensitivity to disclosure. In some instances, the sensitivity involves a degree of time dependency. For example, some research is sensitive as data is being gathered and processed; but once published it becomes a matter of public record and therefore no longer possesses the same degree of confidentiality. In some instances, data may acquire a higher level of confidentiality when put together in an aggregate form, e.g. army movement logistics may be derived from an aggregate of supply data to individual units.

To assess the impact of loss of confidentiality, practitioners must relate the level of sensitivity of the data to the consequences of its untimely release. The data must be appropriately classified or designated according to the following levels:

UNCLASSIFIED OR UNDESIGNATED	basic information
DESIGNATED	varying levels, personal information, sensitive business information
CONFIDENTIAL	compromise could cause injury to the national interest
SECRET	compromise could cause serious injury to the national interest
TOP SECRET	compromise could cause exceptionally grave injury to the national interest

The confidentiality considerations checklist (Table 1) stipulates some questions to be answered in the assessment of the confidentiality requirements of the system or of the information it contains.

CONFIDENTIALITY CONSIDERATIONS CHECKLIST	
	Is the information sensitive in the national interest, i.e. classified?
	Is the information personal?
	What is the consequence of loss of confidentiality of this information?

TABLE 1 – Confidentiality

Integrity
Integrity is used in the context of accuracy and completeness of the information accessible on the system and of the system itself. Where integrity requirements are high, as is the case with financial transactions in banking systems, the potential financial losses will indicate the appropriate levels of investment in safeguards.

The integrity considerations checklist (Table 2) stipulates some aspects to be addressed in the assessment of the integrity requirements of the system or of the information it contains.

INTEGRITY CONSIDERATIONS CHECKLIST	
	Impact of inaccurate data
	Impact of incomplete data

TABLE 2 – Integrity

Availability
The system, to be considered available, must be in place and useable for the intended purpose. While the complete loss of data processing capability is unlikely, it could occur. Unscheduled downtimes of varying degrees of severity are certain. The practitioner must assist the users in establishing how much they rely on the system's being available to provide the expected service. The users must clearly define for the systems staff the maximum acceptable levels of downtime. In this context, the term "availability" relates to continuity of service.

To the practitioner, establishing processing priority based on availability requirements often involves mediating between user groups and reaching agreement on the relative importance of applications to each group. The practitioner must also recognize that availability requirements often change during the lifespan of the application. The user community should document for the systems staff the impact of the loss of availability of the IT systems, support personnel and data.

Those services that are considered to be ***essential or mission-critical services*** must be identified. Such services have a high availability requirement and, as a result, special consideration must be given to the support resources and environmental aspects which affect the provision of service.

The practitioner must determine all critical components involved in the provision of essential service that could be vulnerable to threats. These critical components are also considered to be "assets" for the purposes of the TRA.

The availability considerations checklist (Table 3) stipulates some aspects which should be addressed in the assessment of the availability requirements.

AVAILABILITY CONSIDERATIONS CHECKLIST	
	Changes in availability requirements within the system's life cycle
	Documented impact of loss of availability
	Documented maximum acceptable periods of downtime

TABLE 3 – Availability

2.1.4. Statements of Sensitivity

The CIA requirements are documented in the statements of sensitivity (SOSs). The preparation of a statement of sensitivity[2] should be a prerequisite to the implementation of a new application or changes to existing ones. Applications developed and implemented without statements of sensitivity often do not allow for the necessary security requirements to adequately protect the information available on the system. The statement of sensitivity should be prepared by the responsibility centre which provides data to, and uses or has ownership of, the application. The analysis that leads to the preparation of the statement of sensitivity is sometimes conducted by a number of different people each of whom has some interest in the system or data under consideration.

The user representation for completing the statement of sensitivity could be one

[2] A sample of statement of sensitivity is included in Appendix B.

person or several, depending on the size and complexity of the application being assessed.

A separate statement of sensitivity is required for each major application used on the computer system or anticipated for installation. For example, payroll and inventory would each require a statement of sensitivity, even if they are to be run on the same system. The sensitivity-related valuation of assets is not necessarily linked to numerical values associated with initial or replacement costs; but rather is linked to a relative value associated with the application's requirements for confidentiality, integrity and availability.

2.2. Threat Assessment

The second step of the TRA process is the **Threat Assessment**. The threat concepts of class, likelihood, consequence, impact and exposure are highlighted. Specific threat events such as earthquakes, hacker attempts, virus attacks etc. fall into a particular threat class, depending on the nature of the compromise. Examples of threats within each class can be found in Figure 1.

2.2.1. Description of Threat

The threats that may target the assets under consideration must be described by the practitioner. These threats may originate from either deliberate or accidental events.

2.2.2. Classes of Threats

The practitioner will classify the threats into one of the five main **classes** of threats: disclosure, interruption, modification, destruction and removal or loss.

Disclosure
Assets that have a high **confidentiality** requirement are sensitive to **disclosure.** This class of threats compromises sensitive assets through unauthorized disclosure of the sensitive information.

Interruption
Interruption relates primarily to service assets. Interruption impacts the **availability** of the asset or service. A power outage is an example of a threat which falls into the interruption class.

THREAT CLASS	SAMPLE THREATS
DISCLOSURE	Compromising Emanations Interception Improper Maintenance Procedures Hackers
INTERRUPTION	Earthquake Fire Flood Malicious Code Power Failure
MODIFICATION	Data Entry Errors Hackers Malicious Code
DESTRUCTION	Earthquake Fire Flood Power Spikes
REMOVAL	Theft of Data Theft of Systems

FIGURE 1 – Sample Threats

Modification
The primary impact of this class of threats is on the **integrity** requirement. Recall that integrity, as defined in the GSP, includes both accuracy and completeness of the information. A hacker attempt would fall into this class of threat if changes were made.

Destruction
A threat which destroys the asset falls into the destruction class. Assets that have a high **availability** requirement are particularly sensitive to **destruction.** Threats such as earthquake, flood, fire and vandalism are within the destruction class.

Removal or Loss
When an asset is subject to theft or has been misplaced or lost, the impact is primarily on the **confidentiality and availability** of the asset. Portable computers or laptops are particularly vulnerable to the threat of removal or loss.

2.2.3. Threat Likelihood

The practitioner must consider, on a per-asset basis, both the type of threat that the asset may be subjected to and the likelihood of the threat. The likelihood of threat can be estimated from past experience, from threat information provided by lead agencies and from sources such as other organizations or services.

Likelihood levels of low, medium and high are used according to the following definitions (Source: Government of Canada Security Policy):

> **Not Applicable** may be used to indicate that a threat is considered not to be relevant to the situation under review.
>
> **Low** means there is no history and the threat is considered unlikely to occur.
>
> **Medium** means there is some history and an assessment that the threat may occur.
>
> **High** means there is a significant history and an assessment that the threat is quite likely to occur.

2.2.4. Consequences, Impact and Exposure

Once the assets are listed and the threats are categorized according to the five major classes, the practitioner must assess the **impact** of a threat occurring in the absence of any safeguards. In order to assess the impact, the practitioner must be able to understand and describe the business of the organization. The practitioner must consider what the effect would be on the work being done, on the organization itself, and on those elements of the business that rely on the information or service provided by the specific asset under threat.

During this process, the practitioner seeks to answer the question "What is the consequence of each particular threat?" This consequence is related to the losses or other consequences (both real and perceived) which could result from a specific threat being successful.

The Government of Canada Security policy identifies an impact- reporting mechanism based on an **injury** assessment. In the case of classified or designated assets or information, group impact into levels of **less serious injury**, **serious injury** and **exceptionally grave injury**. Consequences could be expressed in such terms as "**loss of trust**", "**loss of privacy**", "**loss of asset**" or "**loss of service**". The practitioner could add other similarly phrased consequences as needed.

The mapping of the consequence onto one of the three impact ratings (exceptionally grave, serious, less serious) would vary according to departmental priorities. For example, in one department a **loss of trust** might be regarded as **serious injury** in terms of impact, while in another department, the same **loss of trust** might be considered to be **exceptionally grave injury.** The **impact assessment** allows the practitioner to determine the impact to the organization in terms of the real and perceived costs associated with the loss of confidentiality, integrity, and availability.

The identification of **exposure** allows the organization to rank the risk scenario according to the likelihood and impact, and thus assign a priority.

This general exposure rating for data and assets is outlined in Table 4 where impact takes precedence over likelihood. This table provides a means of prioritizing the impact through a rating that considers only the likelihood of a particular threat and the associated impact on the organization should the threat materialize. Table 4 does not consider the safeguards

employed to counterbalance a particular threat.

		IMPACT (INJURY)		
		Exceptionally Grave	Serious	Less Serious
LIKELIHOOD	HIGH	9	8	5
	MEDIUM	7	6	3
	LOW	4	2	1

TABLE 4
Exposure Ratings for Data and Assets[3]

2.2.5. Summarizing Threat Assessment

Threat Assessment as described in this section encompasses:

a) Describing **threats** in terms of who, how and when.

b) Establishing into which **threat class** a threat falls.

c) Determining the **threat likelihood**.

d) Determining the **consequences** on the business operations should a threat be successful.

e) Assessing the **impact** of the consequences as less serious, serious or exceptionally grave injury.

f) Assigning an **exposure rating** to each threat, in terms of the relative severity to the organization.

g) **Priorizing** the impacts/likelihood pairs, according to the ratings determined in (f).

Table 5 provides a sample summary sheet on which the threat assessment information may be entered on a per-asset basis.

[3] Note that for this table *Impact* takes precedence over *Likelihood*.

ASSET	THREAT ASSESSMENT					
	AGENT/ EVENT	CLASS OF THREAT	LIKELIHOOD OF OCCURRENCE	CONSEQUENCE OF OCCURRENCE	IMPACT (INJURY)	EXPOSURE RATING
Describe the Asset.	Describe the threat event.	Disclosure Interruption Modification Destruction Removal.	Low Medium High.	List the consequences to the organization of the threat occurring.	Exceptionally grave, serious, less serious.	Numerical Value 1 to 9.

TABLE 5 – Generic Threat Assessment

2.3. Risk Assessment

Risk assessment is necessary to determine risk assumed by the organization where existing or proposed safeguards[4] are deemed inadequate to protect the asset against an identified threat. Where existing safeguards are not adequate, a vulnerability is noted and analyzed.

Risk assessment is ***"an evaluation of the chance of vulnerabilities being exploited, based on the effectiveness of existing or proposed security safeguards".***

This definition leads the risk assessment process into an evaluation of the vulnerabilities and the likelihood that a vulnerability would be exploited by a threat in the presence of either existing or proposed security measures.

2.3.1. Evaluating Existing Safeguards

Determining what existing safeguards could counter the identified threats is the next logical step in the process of TRA. Once the existing safeguards are grouped on a per-threat basis, the practitioner can assess the security posture of the business or facility relative to each threat, and determine whether any residual vulnerability or weakness exists.

2.3.2. Vulnerabilities

Attention should be paid to times during which the asset is most vulnerable, for example, during periods of public access and unrestricted access or while in transit. In some instances, an asset has an associated time sensitivity. For example, the information may be sensitive while under review or development (e.g. budget) and then may lose its sensitivity upon release to the public.

[4] An assessment of risk is made in two places; first, in the presence of existing safeguards and second, when looking at specific recommendations for proposed safeguards.

There are three possible security posture scenarios in the threat and safeguards environment. The first is identified in Figure 2 as an equilibrium state. This state of equilibrium is the most desirable security posture. In this environment, threats are identified and appropriate safeguards are in place to reduce the associated risks to a level which is acceptable to the organization's senior management.

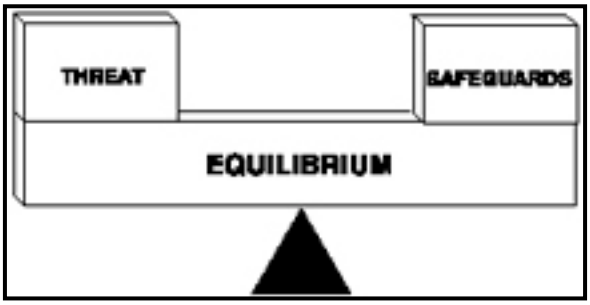

FIGURE 2 – Equilibrium State

The second security posture which an organization might experience is referred to as a ***vulnerable*** state (Figure 3), since the threats outweigh the safeguards. The insecurity produced can result in a variety of IT - related losses which compromise the confidentiality, integrity and availability of the information.

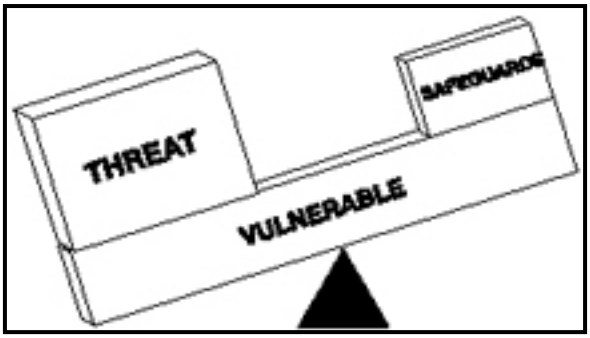

FIGURE 3 – Vulnerable State

The third security posture is referred to as an ***excessive*** state (Figure 4) since the safeguards employed exceed the threats. The result is an overspending in the area of security measures which is not commensurate with the threat; and thus is not justifiable.

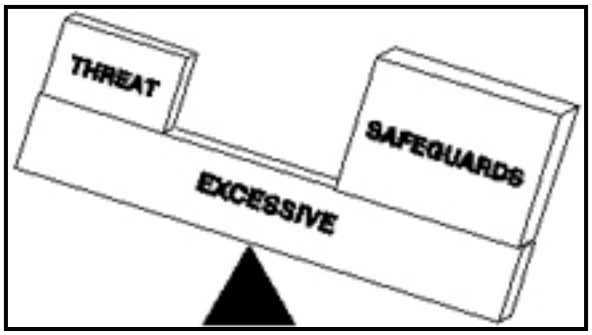

FIGURE 4 – Excessive State

When it is determined that the security posture matches Figure 3 - Vulnerable, the practitioner must consider the possibility that a vulnerability would be exploited. This depends on a number of factors, some of which were explored in the Threat Assessment:

- likelihood of threat;
- possible motive for exploiting the vulnerability;
- value of the asset to the organization and to the threat agent; and
- effort required to exploit the vulnerability.

For example, a vulnerability could exist but, in the absence of one or more of the above factors, it may never be exploited.

2.3.3. Risk

Risk is defined as, "the chance of vulnerabilities being exploited".

The level of risk existing in the organization can be categorized as:

high — requiring immediate attention and safeguard implementation;

medium — requiring attention and safeguard implementation in the near future; or

low — requiring some attention and consideration for safeguard implementation as good business practice.

The practitioner will be able to decide the priority for each component of the risk management program based on items such as the nature of identified threats

and the impact on the organization. Having reviewed the existing safeguards and vulnerabilities, the practitioner establishes the adequacy of safeguards and recommends change. For an example of establishing risk for deliberate threat scenarios, refer to Annex E.

2.3.4. Summarizing Risk Assessment

Risk Assessment as described in this section encompasses:

a) examining existing safeguards;

b) establishing vulnerabilities; and

c) determining the level of risk based on a number of factors.

Table 6 provides a sample summary sheet for entering the risk assessment information on a per-asset basis.

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

2.4. Recommendations

The closing phase of the TRA process includes the proposal of recommendations. These recommendations are intended to improve the security posture of the organization through risk reduction, provide considerations for business recovery activities should a threat cause damage, and identify implementation constraints. Once safeguards that would augment the existing safeguards and improve the security profile are proposed, the risk posture can be re-evaluated as low, medium or high.

2.4.1. Proposed Safeguards

At this point in the process, the practitioner has analyzed the nature of the threats, the impact of successful threats, and the organization's vulnerability to these threats and has subsequently judged the risk to be low, medium, or high. Where the practitioner perceives that the risk can be reduced, appropriate recommendations are made. The practitioner may recommend a number of scenarios, each with an associated effect and cost, from which senior management will make an appropriate selection.

Where the assessment of threats and associated risks leads to specific recommendations, the practitioner must also consider the **feasibility** of such recommendations.

2.4.2. Projected Risk

In some instances, proposed safeguards will reduce or eliminate some, but not all, risks. For such instances, the resulting projected risk should be documented and signed off by senior management. For example, the initial risk assessment

indicated a high risk situation, and several safeguards were recommended by the TRA team. In the presence of these additional safeguards, the risk is re-evaluated as being moderate to low. Thus the priority level of this scenario is reduced but not eliminated, and senior management should acknowledge and accept or reject the projected risk levels. Rejecting the risk implies that other safeguards must be sought to further reduce or eliminate the risk.

Ranking of the implemented safeguards can be accomplished in a number of ways, for example:

– Refer to the impact-rating column of the threat assessment phase (see Table 5 and Appendix C).
– Compare the change in risk level before a proposed safeguard is implemented, in the risk assessment phase risk column (Table 6 and Appendix C) to after, in the recommendations phase risk column (Appendix C).

Impact ratings of 9 should be looked at first because they represent events that have high likelihood and very serious impact. In some instances the change in risk level from high to low is desirable, in particular where the exposure rating is high.

2.4.3. Overall Assessment of Safeguards

Safeguards and associated risk should be evaluated based on the following categories:

– completely satisfactory;
– satisfactory in most aspects;
– needs improvement.

The risks of deliberate threats to the organization have been established by way of the Risk Assessment Grid described in Appendix E. For **accidental** threats, the risk will be assessed according to their history within the organization or similar institutions and the observed effectiveness of associated safeguards in each comparable environment. The highest priority must be assigned to those threats posing a high risk to the organization. For each of these threats, the practitioner will propose safeguards to eliminate the risk or reduce it to a level acceptable to senior management. The adequacy of each of these proposed safeguards must be evaluated as **completely satisfactory, satisfactory in most aspects, or needs improvement**.

The practitioner establishes the appropriateness and interdependencies of safeguards, and answers such questions as: Are safeguards in conflict? Does one safeguard offset the usefulness of another? Does the safeguard overcompensate the threat? What threats have not been fully compensated for? What is the risk that vulnerabilities which are not fully compensated for are likely to be exploited and by whom?

3. Updates

The TRA is considered to be a vital, living document which is essential to meeting the security objectives of the organization. The TRA must be updated at least annually, or whenever an occurrence reveals a deficiency in the existing assessment. The TRA should also be updated whenever changes are planned to the systems or environments in which the IT processing occurs, which could create new risks or redundant safeguards.

3.1. Regular Review

Regular reviews allow the practitioner to revisit the TRA document and assess whether the IT security requirements within the organization have changed. These regular reviews are necessary in light of both the dynamics of the technologies in place to support IT and the dynamics of technologies available to threat agents to help them attack the IT systems of the organization.

3.2. Systems Changes

Changes to systems can greatly impact the security profile; therefore, every change must be assessed. The TRA document provides the practitioner with a baseline against which the effects of these changes can be measured. Examples of changes include the

move of an organization from stand-alone PCs to a Local Area Network environment, the introduction of new applications to existing systems, the introduction of Wide Area Network capability to existing IT environments, a change in communications links or protocols used to move information between departmental units, or a change in the level of the most sensitive information on the system.

3.3. Threat Profile Changes

Changes in the threat profile will also have a potential impact on the TRA. For example, when threat agent motivation diminishes or the effort expended by the threat agent increases, the threat from that source may be reduced. Since changes in the threat profile do not always follow a cyclical pattern, the practitioner must stay in touch with the current threat levels and update the TRA accordingly.

4. Advice and Guidance

4.1. Threats

Sources of historical threat information vary, depending on the type of information sought. For threat information based on events that have already occurred within the organization, the practitioner should consult the Departmental Security Officer. For threat information related to investigations under the Criminal Code of Canada involving IT assets, the practitioner should consult the OIC, Information Technology (IT) Security Branch of the RCMP. Where threat information relates to COMSEC, the practitioner should consult the Communications Security Establishment. The Canadian Security Intelligence Service (CSIS) provides threat information and advice on threat assessment when requested.

4.2. TRA Process

Advice and guidance on the TRA process as described in this document are available through the OIC,IT Security Branch of the RCMP.

GLOSSARY OF TERMS

Analyse: to study or determine the nature and relationship of the parts.

Assess: to evaluate the extent to which certain factors (Threats, Vulnerabilities and Risks) affect the IT environment.

Asset: any item that has value.

Availability: the condition of being usable on demand to support business functions.

Compromise: unauthorized disclosure, destruction, removal, modification or interruption.

Confidentiality: the sensitivity of information or assets to unauthorized disclosure, recorded as classification or designation, each of which implies a degree of injury should unauthorized disclosure occur.

Consequence: outcome, effect.

Critical: crucial, decisive.

Equilibrium: a state of balance existing between two or more opposing forces.

Evaluate: to determine the amount or worth of, or to appraise.

Exposure: the state of being vulnerable to criticism or attack.

Impact: effect of one thing on another.

Information technology: The scientific, technological and engineering disciplines and the management technologies used in information handling, communication and processing; the fields of electronic data processing, telecommunications, networks, and their convergence in systems; applications and associated software and equipment together with their interaction with humans and machines.

Intangible: incapable of being perceived by touch.

Integrity: the accuracy and completeness of information and assets and the authenticity of transactions.

Likelihood: the state or quality of being probable, probability.

Practitioner: one who practises within an area of expertise.

Process: a series of continuous actions to bring about a result.

Qualitative: of or pertaining to quality, describable.

Quantitative: of or pertaining to quantity, measurable.

Risk assessment: an evaluation of the chance of vulnerabilities being exploited, based on the effectiveness of existing or proposed safeguards.

Safeguards: actions or measures taken to offset a particular security concern or threat.

Security baseline: an established security profile or posture which has been determined at an established point in time.

Tangible: perceptible by touch.

Threat assessment: an evaluation of the nature, likelihood and consequence of acts or events that could place sensitive information and assets as risk.

Threat: any potential event or act that could cause one or more of the following to occur: unauthorized disclosure, destruction, removal, modification or interruption of sensitive information, assets or services, or injury to people. A threat may be deliberate or accidental.

STATEMENT OF SENSITIVITY

GENERAL INFORMATION

Branch: _____ Division: _____
Contact Name: _____ Phone: _____

ENVIRONMENT:

(System)

System Name: _____
Application: _____
Other: _____

(Hardware)

Mainframe/Mini: _____
Micro Computer: _____
LAN/WAN/MAN: _____
Secure Phone/FAX: _____
Other: _____

CONFIDENTIALITY

Is the information processed considered:

CLASSIFIED ( ) No ( ) Yes Level (if Yes): _____
or
DESIGNATED ( ) No ( ) Yes Level (if Yes): _____
or
Releasable under the Access to Information statute:
( ) No ( ) Yes
Details: _____

What would be the consequences if data is disclosed to unauthorized people?

	No	Yes
Loss of service	( )	( )
Financial costs	( )	( )
Loss of employment	( )	( )
Legal implications	( )	( )
Loss of trust	( )	( )
	( )	( )

Other: _____

AVAILABILITY

How critical is the information on the system?

Public:	( ) Low	( ) Medium	( ) High	( ) Very critical
Department:	( ) Low	( ) Medium	( ) High	( ) Very critical
Branch:	( ) Low	( ) Medium	( ) High	( ) Very critical

What is the greatest length of time (in days) that the information on the system can be unavailable?

( ) 1 or less ( ) 1-2 ( ) 3-10 ( ) 11-30 ( ) 30+

Do contingencies exist to ensure recovery of the service?

Backups:	( ) Unknown	( ) No	( ) Yes
Offsite storage:	( ) Unknown	( ) No	( ) Yes

Other method of recovery: _____

Give an estimated daily cost if the allowable period of unavailability is exceeded?

Cost ($): _____

Would the destruction of this system cause:

	No	Yes
Loss of service	( )	( )
Financial costs	( )	( )
Loss of employment	( )	( )
Legal implications	( )	( )
Loss of trust	( )	( )

Other: _____

INTEGRITY

How critical is the accuracy of the information required to be?

( ) somewhat critical ( ) very critical

Are there any procedures in place to verify the accuracy of the information? ( ) No ( ) Yes

Would the corruption of this information cause:

	No	Yes
Loss of service	( )	( )
Financial costs	( )	( )
Loss of employment	( )	( )
Legal implications	( )	( )
Loss of trust	( )	( )

Other: _____

Are anti-virus software programs used on a regulated basis?

( ) Yes ( ) No Frequency: _____

Signature: _____ Date: _____

GENERIC THREAT AND RISK ASSESSMENT SUMMARY SHEET

ASSET	THREAT ASESSMENT						RISK ASESSMENT			RECOMMENDATIONS		
	Agent/ Event	Class of Threat	Likelihood	Consequences of Occurrence	Impact	Exposure Rating	Existing Safeguards	Vulnerabil-ities	Risk	Proposed Safeguards	Projected Risk	Assessment of Safeguards
Describe the asset.	DESCRIBE the threat event or agent on a per asset basis.	IDENTIFY the class of threat as: ✓ Disclosure ✓ Interruption ✓Modification ✓ Destruction ✓ Removal	ASSESS the likely-hood as: ✓ Low ✓ Medium ✓ High	DESCRIBE the cones-quence in terms of: ✓ Loss of Privacy ✓ Loss of Trust ✓ Loss of Asset ✓ Loss of Service ✓ etc.	ASSESS the injury as: ✓Exceptionally Grave ✓ Serious ✓ Less Serious	PRIORITI-ZE from 1 to 9 using Exposure Rating table.	DESCRIBE safeguards in place to counter the threat.	DESCRIBE the vulnera-bilities rela-ted to the threat.	ASSESS the risk as: ✓ Low ✓ Medium ✓ High	RECOMMEND implementation of new safe-guards or removal of unnecessary safeguards.	ASSESS the projected risk as: ✓ Low ✓ Medium ✓ High	ASSESS the safeguards as: ✓ Completely Satisfactory ✓ Satisfactory in most Aspects ✓ Needs Improvement

TRA Implementation Plan Checklists

This Appendix contains four checklists to enable the practitioner to ensure that all of the steps of the TRA process are planned for and subsequently followed. The four planning phases are Preparation, Threat Assessment, Risk Assessment and Recommendations.

PHASE I - PREPARATION

ACTIVITY	START DATE	END DATE	PARTICIPANTS R – responsible C – contributors		COMMENTS
			R/C	Estimated Days	
2.1.1 Define the environment					
2.1.2 Identify and valuate assets					
2.1.3 CIA requirements					
2.1.4 Statements of sensitivity					
Additional steps as required					

PHASE II – THREAT ASSESSMENT

ACTIVITY	START DATE	END DATE	PARTICIPANTS R – responsible C – contributors		COMMENTS
			R/C	Estimated Days	
2.2.1 Determine classes of threats					
2.2.2 Determine threat likelihood					
2.2.3 Prepare impact assessment					
2.2.4 Summarize threat assessment					
Additional steps as required					

PHASE III – RISK ASSESSMENT

ACTIVITY	START DATE	END DATE	PARTICIPANTS R – responsible C – contributors		COMMENTS
			R/C	Estimated Days	
2.3.1 Determine existing safeguards					
2.3.2 Identify vulnerabilities					
2.3.3 Establish risk assessment levels					
2.3.4 Assess the adequacy of existing safeguards					
2.3.5 Summarize the risk assessment					

PHASE IV - RECOMMENDATIONS

ACTIVITY	START DATE	END DATE	PARTICIPANTS R – responsible C – contributors		COMMENTS
			R/C	Estimated Days	
2.4.1 Define recommendations for risk reduction Establish priority list for implementation of proposed safeguards					
2.4.2 Define recommendations for business continuity					
2.4.3 Define recommendations for security implementation					
Prepare sign-off sheets for senior managers					
Additional steps as required					

THE RISK ASSESSMENT GRID FOR DELIBERATE THREATS

Determining the levels of risk within an organization requires that the practitioner document those factors which are contributing to that risk. One way of documenting this information for **deliberate** threat scenarios is by using a Risk Assessment Grid (Table E – 1). The BENEFIT column indicates the potential benefit to the threat agent of exploiting a particular vulnerability i.e. carrying out the threat. The IMPACT column indicates the impact on the organization if the threat actually takes place.

The next column EFFORT EXPENDED represents the effort expended by the threat agent to compromise security. This effort is assessed by giving consideration to the effectiveness of any *existing* safeguards.[5] As the effort expended by the threat agent increases, the likelihood that the event will occur decreases.

In the context of **deliberate** threats to systems and data, the risk assessment grid may be applied directly. Where the threats are **accidental**, the concepts of benefit to, and effort expended by, the threat agent to carry out the act are not relevant. An alternate means of assessing the risk associated with accidental or non-deliberate events should be established. Since accidental events are often unpredictable, the practitioner should consider trends from within the organization and the government, and assess the risk according to past observations in each of these areas.

[5] Recall that in section 2.2.3 *Impact Assessment* we considered the environment in the absence of safeguards. Now we are looking at the risk given the existing safeguards.

TABLE E–1 – RISK ASSESSMENT GRID

BENEFIT (to Threat Agent)	IMPACT (on Department)	EFFORT EXPENDED (by Threat Agent)	RISK (to Department)
High	Exceptionally Grave	Low	High
		Medium	Medium – High
		High	Low – Medium
Medium	Serious	Low	Medium – High
		Medium	Medium
		High	Medium – Low
Low	Less Serious	Low	Low
		Medium	Low
		High	Low