Guideline

GNWT
ELECTRONIC INFORMATION SECURITY
Threat-Risk Analysis

Introduction

This guide is intended to assist in assessing the threats and risks to Electronic Information Assets (EI) assets held within the Government of the Northwest Territories, and in making recommendations related to EI security. The objectives of a threat and risk assessment (TRA) are to:

- Involve the various stakeholders and gain their support
- Enable management to make informed decisions about security
- Recommend appropriate and cost-effective safeguards
- Assess the adequacy of existing safeguards
- Recommend additional safeguards
- Eliminate redundant safeguards
- Ensure consistency across government

A TRA does not result in the selection of mechanisms of prevention, detection and response to reduce risks; instead, it indicates the areas where these mechanisms should be applied and in what priority. 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.

“Electronic information” refers to the data and information held by the Government of the NWT and its boards and agencies, used in the management planning and deliverey of its programs and services on behave of the citizens of the Northwest Territories.

Process

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

1. **Preparation:** determining what to protect;

2. **Threat Assessment:** determining what to protect against, consequences of a threat;

3. **Risk Assessment:** determining whether existing or proposed safeguards are satisfactory; and

4. **Recommendations:** identifying what should be done to reduce the risk to a level acceptable to senior management

The four steps are examined below.

Step One- Preparation

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 the interconnectivity with other systems and the profile of the user community. The entire TRA process could span a number of systems and environments. 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

Users, developers, and telecommunications and operations staff should be selected for the team. The purpose of the team is to, among other things, identify and assign value to IT assets as well as documenting known threats and their potential impact.

c) Developing the Baseline

The foundation of the TRA is a security baseline that documents the current security that an organization has in place. It is from this baseline that the risks are assessed, and any updates to the TRA are prepared. The baseline provides a starting point for any measurement of progress. It should be updated as the security environment changes.

Assets Identification and Valuation

Identifying EI assets can be a difficult task, depending on the size of the department or division and the soundness of supporting activities such as materiel management and the availability of comprehensive inventories. Examples of asset include People Soft, Student Financial Assistance program of Education, Culture and Employment and the time recording system for the Legal Division in the Department of Justice. Once assets are identified the owners of the information must assign a value to them. The owners should 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. For example in evaluating a database application the cost of acquiring and entering the data managed by the database should be considered as well.

The question of using qualitative versus quantitative methods in the determination 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.

For an application to be considered an asset it must meet one of the following criteria;

- Loss would have a critical impact on the public
- The application is worth over $50,000
- Unique contribution to a program
- Is a module of a larger application that can be separated out and needs more security than the rest of the program

Statements of Sensitivity

The **Confidentiality, Integrity and Availability (CIA)** requirements are documented in the statements of sensitivity (SoSs). The preparation of a statement of sensitivity 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 owners of the application should prepare the statement of sensitivity.

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, 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.

Confidentiality

Confidentiality is used in the context of sensitivity to disclosure. In some instances, the sensitivity involves a degree of time dependency. Some research is sensitive as data is being gathered and processed; but once published it becomes a matter of public record. In some instances, data may acquire a higher level of confidentiality when put together in an aggregate form.

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

Security Classification Guideline - Table 1

Category	Definition
High	Could reasonably be expected to **cause extremely serious personal or enterprise injury**, significant financial loss in the hundreds of thousands to many millions of dollars, loss of life or public safety, social hardship and major political or economic impact
Medium	Could reasonably be expected to **cause serious personal or enterprise injury**, loss of competitive advantage, loss of confidence in the government program, financial loss in the tens of thousands of dollars, legal action and damage to partnerships, relationships and reputation
Low	Could reasonably be expected to **cause significant injury to individuals or enterprises** that would result in financial losses in the hundreds to thousands, a limited impact in service level or performance, embarrassment and inconvenience
Basic	Will **not result in injury** to individuals, governments or to private sector institutions

Integrity

Integrity is used in the context of accuracy and completeness of the information accessible on the system and of the system itself. Information created by the system must be complete, authentic and reliable. For example security must be in place that will prevent unauthorized changes to a record.

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. Users should be consulted in establishing on how much they rely on the system's being available to provide the expected service.

Step Two- Threat Assessment

The threat concepts of class, likelihood, consequence, impact and exposure are used to carry out the assignment. Specific threat events such as hacker attempts, virus attacks etc. fall into a particular threat class. The threats that may target the assets under consideration must be described.

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	Blizzards Fire Flood Power Spikes Extend power outage
REMOVAL	Theft of Data Theft of Systems

Threat Likelihood

Not only is it necessary to identify the type of threat that the asset may be subjected to but also 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:

> **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.

Consequences, Impact and Exposure

Once the assets are listed and the threats are categorized according to the five major classes, the **impact** of a threat occurring in the absence of any safeguards must be assessed. The critical question is "What is the consequence of each particular threat?" In order to assess the impact, the effect 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 must all be determined.

A 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**" etc.

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** assists in determining 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 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. It 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

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

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

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

Step Three- Risk Assessment

Risk assessment is ***"an evaluation of the chance of vulnerabilities being exploited, based on the effectiveness of existing or proposed security safeguards".*** Risk assessment is necessary to determine risk assumed by the organization where existing or proposed safeguards are deemed inadequate to protect the asset against an identified threat. Where existing safeguards are not adequate, a vulnerability is noted and analyzed.

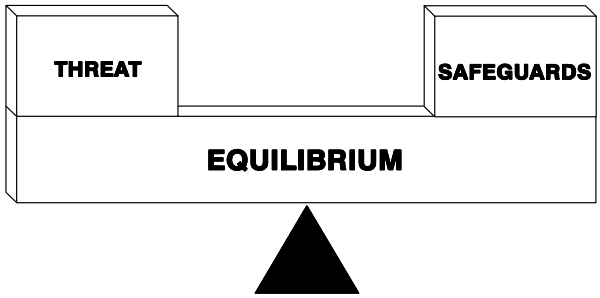
Evaluating Existing Safeguards

Determining what existing safeguards could counter the identified threats is the next step in the process of TRA. Once the existing safeguards are grouped on a per-threat basis, the relative to each threat can be assessed to determine whether any residual vulnerability or weakness exists.

Vulnerabilities

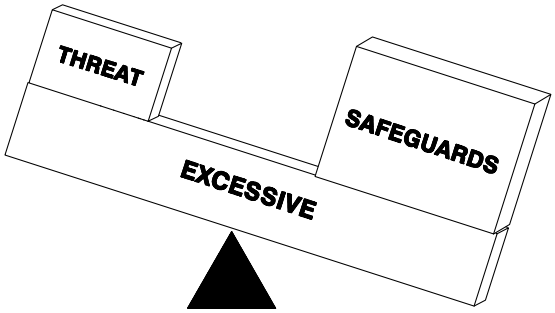
Attention should be paid to times during which the asset is most vulnerable, for example, during periods of public access and unrestricted access or while in transit.

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



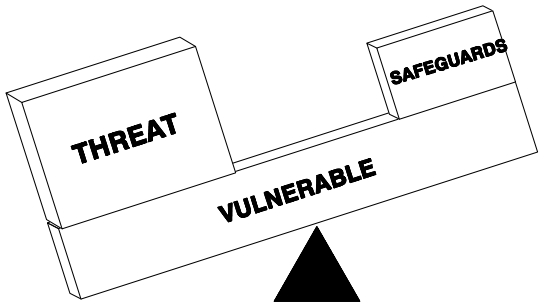
Equilibrium State

The second security posture is referred to as an ***excessive*** state since the safeguards employed exceed the threats. The result is an overspending in the area of security measures that is not commensurate with the threat.



Excessive State

The third 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 EI - related losses, which compromise the confidentiality, integrity, and availability of the information.



Vulnerable State

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

When it is determined that the security posture is Vulnerable, the possibility that a vulnerability could be exploited must be considered. . 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,
- effort required to exploit the vulnerability.

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.

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.

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 risk level

Sample summary sheet for entering the risk assessment information on a per-asset basis.

.

Step Four- Recommendations

The closing phase of the TRA process includes recommendations. Recommendations should 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.

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 the TRA team recommended several safeguards. 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.

Overall Assessment of Safeguards

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

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

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. For each threat, safeguards to eliminate the risk or reduce it to a level acceptable to senior managements should be proposed.
It is necessary to establish the appropriateness and interdependencies of safeguards, and the following questions should be asked

- 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?

Updates

The TRA is considered to be a vital, living document that 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 or when the threat profile changes. The TRA should also be updated whenever changes are planned to the systems or environments, in which the EI processing occurs, which could create new risks or redundant safeguards.

Threat and Risk Assessment Summary Sheet

Department: _____

Division: _____

Asset Description

_____

_____

_____

_____

_____

_____

_____

Exposure: _____

Threat Assessment

Threat Description

_____
_____
_____
_____
_____
_____

Class of Threat:

Disclosure___ Interruption___ Modification____ Destruction___ Removal ____

Likelihood of Threat:

Low___ Medium____ High____

Consequence of Threat Occurring

_____
_____
_____
_____
_____

Impact

Extremely Serious____ Serious_____ Less Serious_____

Exposure Rating_____

Risk Assessment

Existing Safeguards

_____
_____
_____
_____
_____
_____

Vulnerability Description

_____
_____
_____
_____
_____
_____

Risk

Low___ Medium____ High____

Proposed Safeguards

_____
_____
_____
_____
_____
_____

Projected Risk

Low___ Medium____ High____

Safeguards Assessment

Satisfactory____ Satisfactory in most aspects____ Needs Improvement____