Threat and Risk Assessment Guide
GCPSG-022 (2025)

Prepared By:
Royal Canadian Mounted Police
Lead Security Agency for Physical Security
Departmental Security
NHQ 73 Leikin Drive Ottawa Ontario, K1A 0R2

Publication Issued: 2025-01-15
Updated: YYYY-MM-DD

Foreword

The GCPSG-022 - Threat and Risk Assessment Guide is an UNCLASSIFIED publication, issued under the authority of the Royal Canadian Mounted Police Lead Security Agency for Physical Security (RCMP LSA).

This is a Government of Canada publication and serves as a companion guide for the RCMP LSAs Threat and Risk Assessment (TRA) professional development course however may also be used in addressing the initiation and completion of a TRA for departments, agencies and employees of the Government of Canada.

Suggestions for amendments and other information can be sent to the RCMP Lead Security Agency RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

Reproduction

Effective Date

The effective date of GCPSG-022 – Threat and Risk Assessment Guide is 2025-01-15

Record of Amendments

Amendment No.	Date	Entered By	Summary of Amendment

Note: Authority for modifications or variances is Royal Canadian Mounted Police Lead Security Agency for Physical Security (RCMP LSA).

Contents

1. Introduction

The RCMP, as the Lead Security Agency (LSA) for physical security for the Government of Canada, (GC) is responsible for providing advice and guidance on all matters relating to physical security.

1.1. Purpose

The purpose of this document is to serve as a companion guide for the RCMP LSAs Threat and Risk Assessment (TRA) Course and also to provide GC employees with guidance on conducting a physical security TRA. This is intended to be used by employees leading or assigned to a TRA team, and will explain the seven core phases of the TRA process. This guide will provide foundational knowledge of the TRA process, empower employees to conduct thorough and complete assessments, and provide comprehensive reports to decision makers.

1.2. Applicability

This guide applies to GC employees and is applicable to members tasked with leading or participation in a TRA. The guide covers the core concepts of the seven phases of a TRA. Examples are given in the document from specific TRA methodologies, but may be substituted by the TRA team at their discretion. This guide is designed to be a supporting document to the RCMP LSA TRA professional development course, but can be used to support a functional understanding of the TRA process.

1.3. Equity, Diversity, and Inclusion in Physical Security Systems

All employees of the GC have a responsibility to safeguard persons, information and assets of the GC. It is important that security policies and practices do not serve as barriers to inclusivity, but instead support and respect all GC personnel while ensuring appropriate security measures are maintained for the protection of GC personnel, assets, and information.

Initiatives to promote equality and inclusion among the diverse communities and heritages within the GC, should be respected in the development and maintenance of physical security systems. Departments and agencies should follow all GC legislation, policy and directives on Equity, Diversity, and Inclusion (EDI) in the promotion of a fair and equitable work environment for all persons while ensuring they meet their mandated security responsibilities.

Departments and agencies should conduct a risk management exercise to ensure, that while the dignity of all is respected, the protection of GC information, assets, and personnel is maintained. All questions on EDI policies and directives should first be addressed to your responsible departmental authority.

1.4. Information Technology Considerations

With the constantly evolving threat landscape, and the convergence of physical and information technology (IT) security, the requirement to assess the risk of any application and/or software connected to a network to operate and support equipment in GC controlled buildings is critical. Some examples of these control systems could be for items such as, but not limited to, security lighting, perimeter gates, doors, HVAC, etc.

Before implementing any applications and/or software that will control and/or automate certain building functions, your departmental security requires the completion of a Security Assessment and Authorization (SA&A). This will ensure that the integrity and availability of the components the applications and/or software controls are maintained and that any risks highlighted will be mitigated. Starting the SA&A process early is highly recommended to ensure project delivery schedules are not affected. For more information on the SA&A process, please consult your departmental Security.

2. Contact Information

For more information, please contact:

Royal Canadian Mounted Police
Lead Security Agency for Physical Security
73 Leikin Drive, Mailstop #165
Ottawa, ON
K1A 0R2
Email: RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

3. Acronyms

Acronym/Abbreviation	Meaning
AHJ	Authority Having Jurisdiction
ASTRA	Automated Software for Threat and Risk Assessment
CIAV	Confidentiality, Integrity, Availability, and Value
DSM	Directive on Security Management
GC	Government of Canada
PGS	Policy on Government Security
RCMP LSA	RCMP Lead Security Agency for Physical Security
SA&A	Security Assessment and Authorization
TBS	Treasury Board Secretariat of Canada
TRA	Threat and Risk Assessment
PDRR	Protection, Detection, Response, Recover

4. Glossary

Term	Definition
Asset	Tangible or intangible things of the Government of Canada. Assets include but are not limited to information in all forms and media, networks, systems, materiel, real property, financial resources, employee trust, public confidence and international reputation.
Criticality	The degree of injury or importance of an asset, person, function, service, or reputation if lost or unavailable.
Critical Assets	Assets whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, security or economic well-being of Canadians, or to the effective functioning of the government.
Gravity	A metric used to determine the severity of an outcome.
Threat Gravity	The severity of any given threat affecting an asset. This is assessed by using information on a threat agent's capabilities and/or the magnitude of a potential accident or natural threat.
Interdependent	The relationship between any combination of assets, services, or systems in which one is dependent upon another.
Level of Injury	An estimation of what might occur if the asset is compromised and not able to perform its prescribed function.
Injury	Damage or consequence in the event of a compromise.
Likelihood	The probability, or chance, that something will happen.
Threat Likelihood	The probability of a threat compromising an asset.
Residual Risk	Residual risk represents the amount of risk remaining following a determination of values for asset, threat, and vulnerability data.
Risk	The effect of uncertainty on objectives. It is the expression of the likelihood and impact of an event with the potential to affect the achievement of an organization's objectives.
Risk Tolerance	The willingness of an organization to accept or reject a given level of residual risk (exposure). Risk tolerance may differ across the organization, but must be clearly understood by the individuals making risk-related decisions on a given issue.
Safeguards	Assets or external controls that reduce overall risk to employees, other assets or service delivery by decreasing the likelihood of a threat event, reducing the probability of compromise, or mitigating the severity of the outcome through direct or indirect interaction with asset values, threats or vulnerabilities.
Threat	Any potential event or act, deliberate or unintentional, or natural hazard that could result in a compromise.
Threat Actor	An individual or group intentionally harming, directly or indirectly, GC personnel, departments or agencies. Most often this is in the form of trespassing or criminal activity but can also be actions up to & including terror or state-sponsored violence.

Tangible Asset	Any asset that has a physical form and is easy to identify. These may include but are not limited to information in all forms and media, networks, systems, materiel, real property, or financial resources.
Intangible Asset	Any asset that lacks physical form and may be difficult to identify. These include but are not limited to employee trust, public confidence, personal or organizational credibility, and international reputation.
Deliberate Threat	A premeditated, human-caused attempt to interrupt service delivery and/or compromise the confidentially, integrity, availability, value of an asset. These may include but are not limited to theft, sabotage, espionage, or unauthorized alteration/exploitation of information.
Natural Threat	Environmental and natural disturbances that are beyond the scope of human control and can impact service delivery and/or the availability, value of an asset. These may include but are not limited to tornadoes, hurricanes, floods, or blizzards.
Accidental Threat	A compromise to the confidentially, integrity, availability of an asset as a result of human error. These may include but are not limited to accidental physical damage, equipment malfunctions, operational errors, or data corruption.
Vulnerability	An inadequacy related to security that could cause a threat to cause harm/ a factor that could increase susceptibility to compromise.

5. Overview of a Threat and Risk Assessment

TRAs are an analytical tool used to identify and objectively determine the risk level of a particular asset or portfolio of assets. Utilizing collected data about an asset's criticality, threats it may face, and vulnerabilities in the safeguards currently in place; A TRA uses calculations to determine a risk level for each asset. Residual risk is then compared to the department or agency's level of risk tolerance to identify deficiencies that require additional mitigation efforts. This information is then used to generate recommendations to those responsible for the protection of the asset on how to lower the risk to levels deemed acceptable. There are many methodologies that could be used to conduct a TRA however, each of them should follow a similar set of core concepts. There are seven core parts of a TRA, although these can be broken down or combined depending on the methodology being used. Regardless of how the TRA is structured, all methodologies for TRAs contain the processes outlined below.

There are a number of methods to produce a TRA, both manually or with the assistance of software. The RCMP LSA Threat and Risk Assessment course uses the Automated Software for Threat and Risk Assessment (ASTRA) to assist assessors in drafting the TRA. This software does many of the calculations discussed in this guide automatically, reducing the need for assessors to do complicate math. This guide is designed to allow assessors to develop a TRA without the requirement to use software although the use of such technology makes the process much simpler.

5.1. Preparation

The Preparation Phase, further explained in section 6 will identify the scope of the assessment and the acceptable level of residual risk. The scope of the assessment should be determined by a risk management authority which determines what assets will be evaluated in the TRA. The risk management authority should also assign the assessment to a qualified team of security practitioners.

In this phase, the TRA assessor, or team of assessors, should gather enough information to create a work plan outlining the key deliverables at each stage as well as the required resources to complete the TRA. Once a work plan has been completed, it should be reviewed to ensure it, meets the required timelines, respects the appropriate financial authorities, and resources are available for the project. If the TRA work plan is acceptable, management should document their approval and have the team commence the assessment.

5.2. Asset Identification and Valuation

The Asset Identification and Valuation Phase further explained in section 7 will identify all assets within the scope of the TRA. Time and resources should not be expended on assets that are not part of the TRA unless there are interdependencies tied to relevant assets. All assets that are within the parameters designated in the Preparation Phase should be clearly listed and assigned a value. There are several categories each asset may have, rated from Very Low to Very High. For physical security assessments of assets within the GC, all assets are assessed and assigned values based on the three security categories identified in Appendix J of the DSM: confidentiality, availability and integrity. While not explicitly stated in the DSM, Assessors might also consider the value associated with the assets, either the specific monetary value of the asset, or the cultural or social value associated with the assets compromise.

Asset values are also assigned based on a determination of injury, a representation of the damage that could result should the asset be compromised. While assets can be assigned multiple values based on perceived levels of injury, the highest scoring injury category should be prioritized for assessment.

5.3. Threat Assessment

The Threat Assessment Phase further explained in section 8 will identify and list all real and potential threats the assets under evaluation for the TRA may realistically face. Threats can be categorized as either deliberate, accidental, or natural. The threats must be listed and assigned a Threat Level ranging from Very Low to Very High. This value is determined by comparing the likelihood of a threat occurring, with the gravity of the threat; in other words, a determination of what might happen if the threat impacts the asset.

5.4. Vulnerability Assessment

During the vulnerability assessment, the TRA team will assess the assets under evaluation to identify what safeguards are in place to protect them. Once identified, assessors critically determine whether these safeguards are effective based on a probability of compromise and severity of outcome should the identified threats compromise the assets. Vulnerabilities contribute to risks by increasing threat probability, increasing likelihood of compromise, and enabling threats to cause more damage. This is further explained in section 9.

5.5. Calculation of Residual Risks

Residual risk is the remaining level of risk after assets, threats, safeguards and vulnerabilities have been compared against each other. Assessors can determine the residual risk in a TRA by comparing the total values for the assets, threats and vulnerabilities under the scope of the TRA. Various TRA methodologies will prompt assessors to convert each asset, threats and vulnerability value into a number using predefined risk assessment tables. These assigned numbers allow assessors to quickly determine the residual risk for each asset being evaluated by multiplying the asset value with the values for the relevant threat(s) and related vulnerability. The total value represents a score of residual risk for the asset.

Each residual risk can then be compared to the level of risk tolerance determined at the start of the TRA. Those risks that align or fall below the level of risk tolerance do not require risk mitigation; however, those residual risks that exceed the level of risk tolerance will require additional mitigation measures to reduce the residual risk to an acceptable level.

5.6. Recommendations

The Recommendation Phase further explained in section 10 contains the TRA team's comparison of the risks calculated against the acceptable risk level identified in the Preparation Phase. For residual risks that are at or below the target level of risk tolerance, the team should recommend the status quo be maintained, or safeguards be moderated to save resources. In the event safeguards are reduced or removed, a recalculation of the residual risk is required for management consideration. In all cases where residual risk exceeds the acceptable level, the TRA team needs to propose alternative measures to reduce the residual risk to the acceptable level. The TRA risk acceptance authority identified during the preparation phase will then review all proposed safeguards and determine what recommendations will be implemented to reduce residual risk. It is very important to note that the departments overall risk tolerance should not be adjusted to meet the TRAs residual risk score. Rather, safeguards should be employed to adjust the residual risk to a level commensurate with the departments risk tolerance.

5.7. The Final TRA Report

The TRA report further explained in section 11 is the main deliverable of the TRA process. The final report must be well explained and contain enough information to enable the responsible team to initiate the recommended and approved safeguards. A final TRA report will contain a summary of each phase of the TRA:

- Work Plan;
- Asset Assessment;
- Threat Assessment;
- Vulnerability Assessment;
- Prioritized Residual Risk list; and
- Recommendations.

Also included will be management's decision to accept or decline recommended safeguards, maintain, increase, or decrease existing safeguards, and a formal signature acknowledging these decisions. More information on the risk management process can be found within GCPSG-018 Guide to the Risk Management Process for Physical Security. Only after the CSO or their delegate signs the TRA report will this process be complete.

6. Preparation

The Preparation Phase of a TRA will establish signing authorities, identify the scope of the assessment, and the acceptable level of residual risk. The assets to be evaluated must be identified, the timelines of assessment should be determined, and a project team should be delegated with the task of completing the TRA. In this phase, the TRA team should collect enough information to create a work plan. The TRA work plan should be a concise and clearly written document outlining the intended scope of the assessment, the agreed risk tolerances and approval authorities, team composition, forecasted timelines for performing the assessment(s), and additional resources being sought in order to complete the TRA. The work plan must be submitted and approved prior to commencing any assessment of the site; especially if the project team is hiring consultants to assist. This will limit unnecessary delays in the TRA project.

6.1. Establish Approval Authorities

Before initiating a TRA, a risk assessment authority must be identified to approve the allocation of resources necessary for the project and with whom the authority rests to make risk assessment decisions. If these roles are held by different people, all must be informed and approve the commencement of the TRA. The authority to make risk assessment decisions generally belongs to an organization's Chief Security Officer (CSO), who is permitted by the Directive on Security Management 4.1.2.2 (DSM) to delegate this authority. If it is unclear to whom risk management authority has been delegated, assessors should confirm with their CSO office through their appropriate management chain. There will be costs associated with conducting a TRA; staff hours required, as well as additional monetary expenses may be incurred. Ensure there is a commitment from the financial authority to allow these resources to be directed toward the completion of the TRA. The approval authority can also be referred to as the risk owner as they accept any risk that result from the TRA findings.

6.2. Mandate and Project Scope

Once these authorities are identified, a project mandate must be established and agreed upon by the approval authorities. The mandate should include the GC organization's:

- Risk tolerance level;
- Approved resources for the TRA project;
- Budget/time limitations for recommendations; and
- The parameters that will limit the TRA scope in any way.

The mandate should also identify who will sign off on the complete report and if they have been delegated authority by the CSO to accept any residual risk that exceeds the level of risk acceptable to the organization. Before starting the TRA, the project authorities and team members should have a clear understanding of the scope and mandate of the project. This may include assets to be assessed and, based on the assets' current level of criticality, the depth of assessment warranted. The scope of the TRA will vary based on the time needed to complete the assessment and the amount of resources available. The focus of a TRA may vary from a narrow assessment, such as a room housing sensitive documents within a GC facility, to a broad assessment that could encompass all assets in a multi-building portfolio.

When considering the scope of a TRA, assessors should consider if it is a general strategic level assessment which looks at a specific area, or an in depth and detailed assessment that explores various scenarios with only a handful of assets, threat, or vulnerability variables. This will assist in establishing the criteria of the assessment, what is to be assessed, and what is within or beyond the scope of the assessment. It is imperative for project authorities and TRA team members to agree upon clear and defined parameters in order to avoid the scope expanding beyond, or failing to meet, the intended evaluation of the required areas.

6.3. Understanding Management's Level of Risk Tolerance

A Deputy Head is responsible for determining how much overall risk a department is willing to accept and the CSO is delegated to assess the amount of residual risk they are willing to accept from a security perspective. Each organization should establish a level of risk tolerance that reflects the sensitivity of the work they perform and the types of assets they use to perform their key services. The CSO may further delegate risk management decisions, which can result in different units having risk tolerance levels that are different than the baseline. Assessors must identify who is responsible for managing the risk associated to the assets under assessment for the TRA. This individual will be identified as the Authority having Jurisdiction (AHJ). Larger TRA projects may have multiple AHJ responsible for different assets that will be evaluated, you must engage all of them in risk tolerance discussions. There must be consensus between all AHJ and the TRA team regarding the risk tolerance levels. It is imperative the AHJ and TRA team agree on the target level, as well as what that level will look like when implemented. Ensure the AHJ understands the metrics being used to measure residual risk, and confirm this matches their stated risk tolerance level.

It is crucial that management and the assessment team have a common understanding regarding risk tolerance, project sign-off, and any prior assumptions or determinations. If there is any confusion or disagreement, it can delay the project, or lead to inadequate or inappropriate recommendations that do not align with management expectations.

6.4. Team Selection

Having the right team composition greatly improves the efficiency of the TRA process, and contributes to the best possible analysis and recommendations. While many TRAs will likely be done by one or two individuals, the team size and composition will be dictated by the following considerations:

- The scope of assessment;
- Complexity of assets;
- Urgency of the situation;
- Distribution of assets; and
- Availability of qualified personnel.

A team should have at least one (1) member with one or more of the following:

- A strong understanding of the TRA process;
- A detailed understanding of the department/unit's operational requirements;
- A thorough understanding of security standards and other safeguards; and
- The authority and security screening levels to access a facility or location where the assets under assessment are found.

Without appropriately qualified personnel, representing both operational interests and security considerations, the resulting TRA might contain insufficient information to address the concerns that caused the assessment's initiation.

Depending on the scope of the project, the TRA team can also be composed of individuals who can provide details of the assets, threats, or vulnerabilities that the rest of the team can use to efficiently complete the assessment. These resources could include:

- Facility Security Personnel - local guard supervisor, site security manager, or member(s) of the security team;
- Facility Management - members of real property, architects, or engineers to advise on design considerations; and/or
- Subject Matter Experts - specialists responsible for specific systems if these fall within the scope of the TRA being performed (Information Technologists, Custodians of Classified Materials).

Depending on the size and complexity of the TRA, or the number and experience level of the assessment team members, expertise may be acquired from other departments to provide specialized support and guidance on various topics. These specific departments are listed in the Policy on Government Security (PGS) under section 5 "Roles of other government organizations."

7. Asset Identification and Valuation

After completion of the Preparation Phase, the next step of the TRA is to identify all assets to be assessed and, analyze them to determine the level of injury (estimation of what might occur, if these assets are compromised or unable to perform its prescribed function). In the context of a physical security risk assessment within the GC, categories of injury can be assessed in one of four categories: confidentiality, availability, integrity and/or value. Assessors should carefully analyze all assets based on these categories of injury, and determine which injury category best describes how the asset might be compromised.

Assessors should also determine the level of injury associated with each injury category. This can range from Low to Very High with higher levels representing a greater overall level of injury should the asset be subject to compromise. The gravity of each asset's potential compromise can then be organized into a priority list; ranking all assets from the highest to lowest level of potential. A prioritized list of assets at greatest risk of injury will permit focused analysis of potential threats and vulnerabilities during later stages of the TRA process.

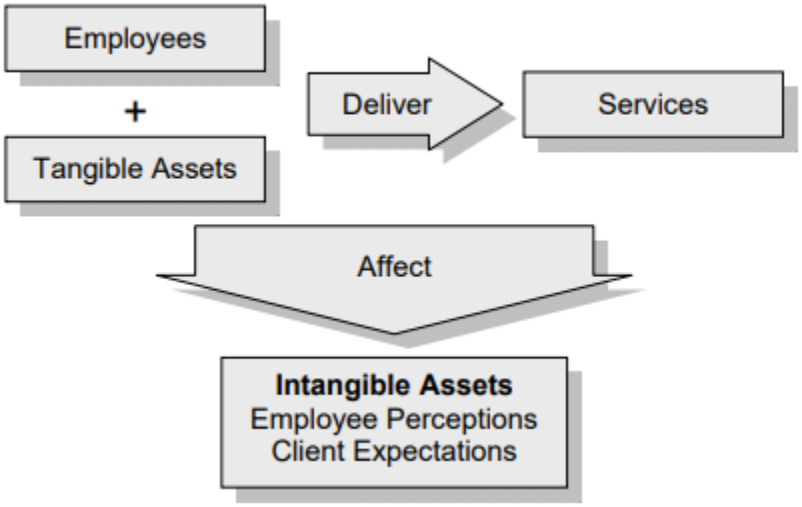
7.1. Identifying Assets

There are two types of assets to consider when conducting a TRA, tangible and intangible.

- Tangible assets are easier to identify and evaluate as they encompass things that can be physically touched and damage to them is easier to measure. Computer servers and equipment, documents, and vehicles are all examples of tangible assets; and
- Intangible assets, which can be harder to identify. Levels of injury for intangible assets are often subjective and are open to interpretation by assessors and stakeholders. These assets include concepts such as public trust in an organization, reputation, and confidence in the department or agency's ability to deliver critical services.

Personnel are also assets to an organization, as they interact with tangible assets to deliver services. Service delivery can have an effect on intangible assets such as employee perceptions and client expectations. The ability for employees to deliver services using tangible assets has a direct effect on these intangible assets. Personnel value can be measured by using their intrinsic value, or their operational value, whichever is higher. Personnel who can prevent wide-scale death by completing their operational duties would have a higher operational value than measuring the intrinsic value of their life alone. When assessing assets, carefully consider the services the assets are responsible for delivering, as this can help guide analysis of assets and potential levels of injury based on the criticality of the service being provided. The greater the impact on the assets, the greater the disruption to the service delivery, which in turn, affects those intangible assets like employee perceptions or client expectations. The relationship between assets, personnel, and the delivery of service is highlighted in the graphic below.

Table 1: Employees, Assets, and Services Relation Chart



Alt Text: The above graphic depicts the aspects that can make up an intangible asset

It is vital that all categories of assets are considered when determining which assets are within the TRA scope, and when determining interdependencies. When conducting a TRA, there is a high probability that there will be additional assets found that are not within the defined scope of the TRA. Resources should not be expended unnecessarily for any assets that are not within the scope of the assessment, or do not have valid interdependencies unless these have been established through the assessment process.

7.1.1. Interdependent Relationships

When conducting a TRA, the analysis of assets should identify any interdependent relationships with other assets within the scope of the TRA. Depending on the timing and resources available, interdependencies should also be considered based on the level of injury should the assets be compromised and the level of service interruption that could result.

Example: A TRA is being conducted on a facility that houses gold bullion, an asset with monetary value. The facility also has specialized printers that can produce traceable certificates of authenticity with anti-fraud markings and a serial number. In this case the specialized printer may not have a significant monetary value, and therefore if analyzed independently may not be considered within the TRA scope. However, the main asset (the gold bullion) is reliant on the printer to create certificates of authenticity to facilitate trade which makes the two assets interdependent. This means the printer should be listed and analyzed as an asset in the TRA because a threat could undermine the public trust of the gold bullion being traded. If the printer were compromised, this might allow the gold bullion to be issued fraudulent certificates of authenticity. The printer allows for the bullion to be traded with confidence when uncompromised, and therefore should be evaluated alongside the bullion.

7.1.2. Asset Criticality

When assessing an asset, it is important to consider its relation to the organization's business objectives and the services they deliver. Asset criticality rates how important an asset is to the delivery of critical services, with a higher score meaning a compromise to the asset will have a more severe impact on operational functions. Determining an asset's criticality is vital, as some assets may receive low scores in other metrics such as sensitivity or value, but could be essential for the department to continue operations.

Example: A licensing department's IT server stack that processes registration requests. This Commercial-Off-The-Shelf (COTS) server stack may have a low monetary value and does not store or process sensitive information. These factors would rank this asset relatively low on many metrics however, a compromise may halt service delivery which may require a higher score or value on the metric of criticality.

7.2. Assessing Asset Injury

Following the identification of all assets within the scope of the TRA, assessors need to determine the level of injury for each asset. Asset injury represents a determination of what might happen if the asset is subject to compromise and not able to contribute to the delivery of the organization's critical services. Injury can be assessed based on several categories: physical harm, psychological harm, environmental damage, diminished reputation, and loss of trust in the institution.

Most TRA methodologies have a system for assigning injury scores based on the potential harm caused by a compromise. While the specific calculation formulas vary depending on the TRA methodology, the underlying principles remain the same - the higher the level of compromise for the asset, the higher the asset will be scored for potential injury.

The DSM provides specific criteria for determining injury. As outlined in Appendix J of the DSM, injury results from an asset losing one or more of the following criteria:

7.2.1. Confidentiality

Confidentiality is how sensitive the information is regarding the asset and the degree of injury that could reasonably be expected in the event of unauthorized disclosure. The GC utilizes a system to categorize the sensitivity of assets that is independent of any TRA methodology used. TRA methodologies may convert the GC sensitivity level to a numeric value for use in calculations, or assign a generic score such as Very Low to Very High. More information can be found on the GC classification system here: Levels of Security.

7.2.2. Availability

Availability scores the possible degree of injury arising from unauthorized destruction, interruption, or denial of use of an asset. Availability scores could apply to tangible or intangible assets, personnel and services and represents the impact on the asset's ability

to deliver services. The higher the impact of an asset becoming unavailable, the higher the asset's availability score will be.

Example: An essential worker that cannot work remotely could have a high availability rating. If a protest denied the employee access to the facility, it could completely halt operations until availability of the workforce is restored.

7.2.3. Integrity

An integrity score measures the possible degree of injury should information be modified without authorization. Examples could be, financial information, medical treatment data, and polling results. The worse the impact the unauthorized modification could have, the higher the Asset's integrity score will be.

Example: Financial data related to international infrastructure projects would have a Very High integrity score, as unauthorized modification of the data could facilitate massive fraud, cover up embezzlement, and greatly damage international partners trust in Canada's ability to conduct international projects.

7.2.4. Value

Value is the monetary worth of the asset or the revenue the asset may generate. This can be recorded as a dollar value or converted into a rating such as Very Low to Very High value. While monetary value is not specifically mentioned in Appendix J of the DSM, an assessment of confidentiality, availability, or integrity indirectly considers monetary value as a criterion.

When assessing monetary value associated with the compromise of an asset, the following is important to consider. Value is calculated by determining the replacement cost of the asset itself, as well as any lost revenue from service being denied for a period of time. The higher the replacement cost or loss of revenue following a compromise, the higher the value score for the asset.

7.2.5. Assigning Injury Levels

All assets within the scope of the TRA are to be evaluated to determine their injury level. It is possible for assets to have more than one injury level and each asset should have a brief narrative describing the reasoning for its assigned value. At minimum, the narrative should capture the highest value assigned, but additional values may be presented if the TRA team deems the information is relevant for the assessment.

The TRA team should focus on and prioritize the category that represents the greatest overall impact to the asset. While TRA methodologies have differing scales to gauge compromise to assets, the HTRA defines asset injury based on confidentiality, integrity, availability, and value (CIAV), thereby bringing the process more in line with the DSM compared to other methodologies.

The assessment tables from the HTRA are presented and explained in Tables 2 and 3:

Table 2: HTRA Injury Assessment: Confidentiality, Availability, Integrity, and Value

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

Alt Text: The above chart assigns an injury level for each category of CIAV.

Determining the confidentiality assessment for GC assets is tied directly to their level of sensitivity. For information on determining an asset's level of sensitivity, refer to TBS guidance. Table 2 above provides general metrics for assessing injury to information-based assets through CIAV.

Assessors are to determine the most severe compromise should the assets CIAV be affected. Each of the CIAV injury categories are analyzed and assigned a level. Assessors wishing to understand and quantify injury to people or the monetary value should refer to table 3.

Table 3: HTRA Injury Assessment: Human and Financial Impacts

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

Alt Text: The above chart is used to determine the level of injury based on the impact of a compromise.

Example 1: A water purification vat in a treatment plant. Unauthorized tampering with the equipment, either malicious or incompetent, could severely affect the health of residents that are within the utilities service area. Due to this, the risk to injury if the asset is compromised is Very High.

Example 2: A list of patients at an alcohol rehabilitation centre would receive a score of Medium, as a compromise could seriously embarrass patients and negatively affect the public's trust in the organization to safeguard sensitive information.

7.3. Prioritized Asset List

Once all assets have been assessed and have values, they may be compiled in a Prioritized Asset List starting with the assets of highest injury value (highest priority) and in descending order to the lowest value (lowest priority).

In cases where multiple assets hold identical numerical scores, the TRA team will have to re-evaluate and select the order in which they will be listed. This can be done by comparing the second-highest values if applicable. If the assets have equal scores in subsequent values the team may make a subjective call on the order the assets are prioritized and include an explanation for the decision. When making a subjective call to rank these assets, the TRA team should align these with the overall objectives of the TRA, the organization's mandate, and any service deliverables that may be affected. Consideration can also be given to which asset is more likely to be targeted or affected by a compromise. The asset that is more likely to be targeted or affected should be placed at a higher priority.

8. Threat Assessment

The purpose of the threat assessment phase is to identify any potential threats for which an asset subject, and rank them based on the likelihood of occurrence, and the severity of outcome caused by the threat. TRA assessors should analyze how a threat will affect the assets within the assessment scope. This is done through the creation of threat scenarios, specific chronological descriptions of how a threat might affect an asset based on available threat data. It is possible for a threat to affect multiple assets, in this case a threat scenario will be generated for each asset subject to the threat. Conversely, assets can be affected by multiple threats, and will therefore be included in multiple threat scenarios.

In completing a threat assessment, regardless of the methodology employed, TRA assessors need to determine the likelihood of a threat taking place, and the impact of the threat should it manifest. The United Kingdom (UK) uses a system similar to the HTRA methodology for assessing threat. The National Risk Register (NRR) is the external version of the National Security Risk Assessment (NSRA), which the UK government utilizes to assess the most serious risks facing their country. The NRR contains a list where many common threats are analyzed and updated annually. This method determines likelihood using a matrix which will assign a numeric level from one (1) to five (5). Likelihood in the NRR Methodology is separated between deliberate and accidental threats, and will employ only one of the two. Gravity/impact is determined on a scale, being assigned a numeric value from one (1) to five (5) based on any of three (3) metrics: fatalities, casualties, and/or financial cost. These two numeric values are then visualized on a graph, that will contain all analyzed threats and allow assessors to quickly determine the most severe threats that require attention.

8.1. Threat Categories

Threats can stem from a variety of sources. Various TRA methodologies breakdown threats into one of three common categories: deliberate, accidental, and natural hazards. Each category should be evaluated unless excluded by the scope of the TRA. Working through each category individually is advised, as it can be easy to overlook natural and accidental threats with the greatest attention being paid to deliberate threats.

8.1.1. Deliberate

Deliberate threats are planned out and malicious attempts to harm an asset such as theft, unauthorized alteration, exploitation of information, or other such malicious activity. Deliberate threats can be undertaken by a wide range of actors, such as; state actors, organized crime, crimes of opportunity, insider threats, or ideologically motivated actors. Local police data can provide insight into what potential criminal elements may pose a threat in the area, this information should be collected and analyzed. Checking local, regional, or national news resources can assist in identifying groups who may be ideologically driven to disrupt an asset which can be cross-referenced with law enforcement partners to determine their prominence in the area.

Threats posed by state actors can be more difficult to determine as there will be limited data available that is directly linked to their motives or capabilities. When assessing state actor threats, it can be beneficial to develop design-based threat (DBT) lists using what data is available, with any gaps being filled by predictions of motives and capabilities. DBT is a profile of the type, composition, capability, method, projected harm, or intensity of a deliberate, accidental, or natural threat on the security and operations of a facility. DBTs can be used in conjunction with a TRA to determine specific characteristics of threats requiring mitigation. If the assessment encompasses assets that have value and may potentially be targeted by hostile states, it is recommended to consult with the information and contacts found on Canada's National Security page.

Insider risk is especially dangerous, as the threat actor will have intimate knowledge of the organization and may be able to leverage the trust of colleagues to circumvent safeguards. Insider risks will often show warning signs such as staff entering facilities outside of working hours, attempting to access information on assets that are not part of their daily duties, and disgruntled behaviour towards superiors or the government. Insider risk can also be otherwise loyal employees who are subject to blackmail, manipulation, or coercion from a threat actor to force the employee to compromise assets. Public Safety Canada has several online resources on insider risk available here.

8.1.2. Natural

Natural threats can be easier to identify thanks to a wealth of meteorological data that is openly available to the public. Public Safety Canada has resources available for use however, the effects of natural threats are notoriously difficult to accurately determine. When assessing natural threats, use local historic data to determine a baseline severity

for when these events occur, and use that info in your TRA calculations. Given the potential damage to assets or interruption to services, and the unpredictability associated with natural hazards, assessors should carefully consider natural hazard threats in their assessment criteria where possible based on assessment scope.

8.1.3. Accidental

Accidental threats are compromises caused by human error such as; accidental physical, mechanical or electrical damage, and software malfunctions. The threat of accidents is the most common in day-to-day operations and the impact can be multiplied by a lack of training or poor security culture. A key element for accidental threats is the lack of malicious intent, however the potential impact on assets could be just as severe as any other category. Deliberate threat actors may exploit accidental threats to mask malicious actions. Accidental threats are identified by reviewing incident data, interviewing team leaders and staff, and assessing safeguards to determine their effectiveness.

8.2. Assessing Threat Likelihood

Threat likelihood is the probability that a threat will compromise an asset, and can be difficult to accurately determine given the uncertainties around particular threats. TRA methodologies will generally include matrices to help determine a likelihood score to be used in their calculations. Inputs can include regional data, such as incidents involving similar facilities or assets, frequency of criminal events, historic weather data and other such info.

Table 4 is a likelihood assessment tool used in HTRA Methodology. The assessor will collect data to determine the frequency of a threat, where the threat has taken place and compare the location where the assets are located, other assets at the same location or similar assets at alternate locations. These values are then used to determine an overall likelihood value for the specific threat. This table should be used for critically thinking through threat scenarios.

Table 4: HTRA Threat Likelihood Matrix

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

Alt Text: This is a chart from the HTRA Methodology for determining a threat's Likelihood.

Example: A federal ballot counting facility. The scope is specifically evaluating the risk when a count is taking place. An identified threat is anti-government protestors attempting to disrupt the ballots from being counted. Data shows this is an incident type that happens regularly and during every election for this location. Elections are only held every four years, so using the chart, the past frequency would be every 1,000-10,000 days. With this data input, the likelihood output would assessed as Low. This score however is not reflective of the actual likelihood, as the incident occurs every time the ballots are counted. Considering the scope of the assessment, it is more accurate to determine the past frequency as daily, given similar incidents have occurred at this location every time the parameters of the assessment are present. Recalculating the likelihood with this more accurate information would give the more reflective likelihood rating of High. This reasoning should be explained in the TRA to demonstrate how the likelihood score was determined.

8.3. Assessing Threat Gravity

The gravity of a threat reflects the consequence of the threat affecting the asset under evaluation, and the level of damage that can occur. To assess the threat's gravity, compare it to each asset's highest scoring injury categories identified in Section 7: Asset Identification and valuation. Next, analyze the amount of damage that a threat could cause, should the threat compromise the asset. The more harm a threat can potentially cause, the higher the threats gravity. Consider the threat's effect on an asset's criticality, confidentiality, availability, integrity, monetary value and potential casualties if an incident occurs. Each methodology determines the gravity of a threat, usually in a matrix such as that used by HTRA. The example in 8.2 Assessing Threat Likelihood is expanded on below using this chart to demonstrate the practical application of assessing gravity.

Table 5: HTRA Threat Gravity Matrix

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

Alt Text: The above graphics depict a chart from the HTRA Methodology for determining a Threats Gravity

Example: Local law enforcement has shared data from previous encounters with this anti-government group. Data suggests they are associated ideologically with an international protest movement. The group operates exclusively in local cells, with no direct cooperation with any sibling groups. Communication between groups is limited to easily monitored public social media pages. A review of incident reports at this location involving the group suggest they are willing to cause minor damage to property (graffiti), and will conduct low skill denial of service tactics (gluing locks, obstructing roadways, blocking staff access, etc). A review of data shows the group does not have any violent intentions but will passively resist arrest if police become involved. Local police and private security services have managed to contain and control the group within three hours in all recorded incidents at this location. When using this information to determine the group's capabilities, they portray limited resources and skill. When determining the impact of incidents caused by the group, data suggests the group is modestly destructive and causes interruption of service, usually no longer than three hours. This data corresponds to a gravity level of Low, in the HTRA matrix.

8.4. Calculating Threat Levels

Overall threat levels can be determined by comparing threat levels associated with the likelihood a threat will occur and the impacts of what happens if the threat does occur, the threat's gravity. The higher the score, the more serious the threat. These scores will generally use the potential casualties, loss of financial value, damage to reputation or denial of service severity to allocate a threat score. The chosen TRA methodology will generally have a calculation or matrix that will compare likelihood and gravity scores/levels to generate an overall threat level. Below is an example from the HTRA Methodology using data collected in the example case in 8.2 Assessing Threat Likelihood and 8.3 Assessing Threat Gravity a threat level will be generated using the matrix.

Table 6: HTRA Threat Level Matrix

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

Alt Text: The above graphics depicts a matrix from the HTRA Methodology for determining Threat Levels

Example: The anti-government group has received a likelihood score of High and a gravity score of Low. When this data is input to the HTRA Matrix, it generates a final threat score of Medium. Based on the analyzed information this output is reflective of the situation and will be recorded with any supporting data in the final TRA report. Once all threats have been addressed, the final step of this phase is to create a prioritized threat list beginning with the highest threat level to the lowest. This provides decision makers a snapshot of all the threats that have been identified including notes on each, and the calculation it received.

9. Risk Assessment Phase

Following the determination of assets and the threats that might negatively impact those assets, assessors now need to critically analyze whether the mechanisms in place to protect their assets from the identified threats are sufficient. This is known as a risk assessment. Some TRA methodologies consider the determination of vulnerabilities as a separate analytical process while others consider vulnerabilities and safeguard performance as part of the risk assessment phase. No matter the order, assessors performing TRAs should always consider where the assets under evaluation are most vulnerable to the threats identified. Once vulnerabilities have been identified alongside the assets and threats, their values are then multiplied to achieve a risk level or score.

During the vulnerability assessment, the TRA team will assess the assets that have been identified in order to determine what safeguards are in place to protect them. Safeguards are security measures or controls that perform one or more functions to mitigate overall risk by reducing asset values, threats, or vulnerabilities within the scope of a TRA project. Once identified, assessors critically determine whether these safeguards are effective based on whether the identified threats compromise the assets (probability of compromise) and how severely (severity of outcome), which results in a vulnerability. Assessors can then use safeguard evaluation criteria to compare all known information about safeguard performance, and any associated vulnerabilities, to produce a prioritized list of vulnerabilities. After those values have been identified, they are then compared with the asset and threat data together to obtain a calculation of residual risk.

There are other ways to calculate risks using different TRA methodologies. The Protective Security Risk Management Methodology (NPSA, UK) and FEMA 430 Risk Management Series (FEMA, USA) are some examples. Under NPSAs methodology (Protective Security Risk Management PSRM | NPSA), threats and vulnerabilities must be identified, aligning them to assets. All of which have been assessed for their likelihood (of the threat event occurring) and impact (to the organization and/or third parties) should the threat transpire. Then risks are assessed, calculated, and compiled to build a risk register. The Risk Register should contain enough detailed information that senior decision makers are able to make informed decisions and judgments on risk appetite, resource allocation and, for security practitioners, develop and implement any risk mitigation measures that may be required.

Under the FEMA 430 Risk Management Series (FEMA 430: Site and Urban Design for Security), tasks in the Vulnerability Assessment include; collecting information about the site and building into a vulnerability portfolio that included GIS maps and other pertinent information, identifying the layers of defence (safeguards), evaluating the site and building, and determining the vulnerability rating. FEMA 452 also has a Vulnerability Assessment Checklist that can be a helpful tool for assessors determine vulnerabilities: a brief overview is contained in the FEMA 430 document – Section 2.2.4. It contains a list of questions to determine the vulnerabilities present for the assets and to guide the preparation of the overall risk assessment. FEMA's Risk Assessment process will analyze the threat (probability of occurrence), asset value, and vulnerabilities (consequences of occurrence) to determine the risk level. The process consists of preparing risk assessment matrices, determining the risk ratings (threat x asset value x vulnerability), and prioritizing the higher-risk ratings based on observed vulnerabilities to target potential mitigation measures.

These methodologies each take different approaches when conducting a TRA, but the baseline standards are similar. The goal for HTRA, FEMA and PSRM is to identify risk by observing threats that could affect assets and determine what the likelihood and impact would be on those assets. Each of these TRA methodologies can be used independently when conducting your analysis, but the goal is to understand how to calculate risk. The steps of this phase will be focusing on the HTRA methodology.

9.1. Vulnerability Assessment

A vulnerability assessment evaluates the potential susceptibility to compromise of the asset against the identified threats and provides a basis for determining mitigation measures for the protection of those assets. The purpose is to analyze the effectiveness of safeguards, as opposed to analyzing the threat for which the safeguards are intended to protect. This is the difference between doing just a vulnerability assessment and looking at vulnerabilities for a wider risk assessment.

Unlike with the threat or the asset, security professionals can have a greater influence over the vulnerability in the TRA process. It is always possible to alter or correct the vulnerability as a pre-emptive approach to a threat. The vulnerability assessment phase is comprised of five sequential steps:

9.1.1. Safeguard Identification/Listing

Identifying safeguards which are present during the assessment is the crucial first step when performing a vulnerability assessment. The goal is to list, at an appropriate level of detail, all existing safeguards that fall within the scope of the assessment. These can be safeguards that are currently in operation, or those being considered or proposed for immediate implementation (for example, those being installed as part of a building retrofit or security design process). In order to assess vulnerabilities that expose assets within the scope of a TRA project to greater risk, existing and proposed safeguards must first be identified and then later analyzed to determine their relative effectiveness.

Safeguards can also be viewed as the 'defensive layers' for the protection of any critical assets. Most pieces of security equipment are better assessed as safeguards rather than as assets. Knowing how to identify safeguards can be simplified if they are broken down by layers. A layered approach such as zone selection for instance, can be used when determining which safeguards are most appropriate per zone in a GC facility. In order to better understand this process, refer to GCPSG-015 (2023) - Guide to the Application of Physical Security Zones as this can help when dividing certain areas into groupings, rather than evaluating a facility as a whole. It may allow for more focused data collection when identifying safeguards zone-by-zone.

9.1.2. Assess Safeguard Effectiveness

When assessing safeguards and determining vulnerabilities, it is important to remember that risk and causal vulnerabilities are inversely proportional to safeguard effectiveness. In other words, the more effective the safeguard is at protecting the asset, the fewer vulnerabilities exist. As more robust security measures are implemented to protect assets, both vulnerabilities and the associated risks decrease accordingly. If these types of safeguards are performing their function and ensuring assets, people, and information are protected, fewer vulnerabilities could result. If their function is being hampered or exploited, their effectiveness decreases, and more vulnerabilities could result.

Most safeguards perform one or more of the basic security functions; protection, detection, response, and recovery ("PDRR") For more information, refer to GCPSG-019 (2023) - Protection, Detection, Response, and Recovery Guide. Safeguards impact all risk variables (assets, threat and vulnerabilities), but deal mostly with vulnerabilities. Avoidance and deterrence should also be considered, but deal mostly with mitigating potential threats and not vulnerabilities directly. Ultimately, safeguards that aid in reducing the primary risk variables can be attributed to a decrease in the likelihood of a threat event occurring. While we cannot always control the sensitivity of our assets, or control how, and why our threats manifest, security practitioners have the greatest control over how we respond to those threats. The HTRA methodology table, D-1 illustrates how safeguards impact risk variables, and how they impact threats events.

Based on the concepts of PDRR, the following security functions can assist the assessor to measure safeguard effectiveness:

- **Avoidance -** By using avoidance as a security function, the primary impact would be protecting the asset value and lowering the likelihood of a threat taking place. It would reduce or avoid risk, and could potentially lower the asset value. For example, many convenience stores limit cash on hand to a small amount after normal working hours. It doesn't prevent someone coming in to steal money, but it mitigates the loss of large sums of money;
- **Deterrence -** By using deterrence as a security function, the primary impact would be lowering the likelihood of a threat taking place. The aim is to dissuade deliberate threat agents who may be contemplating an attack, thereby

decreasing threat agent intentions and, the probability of occurrence. The installation of warning signs (CCTV operations, alarms, or guard dogs) could serve as a deterrent but do not address vulnerabilities directly;

- **Prevention -** When targeting against specific types of threats to reduce the likelihood of occurrence, most preventive measures tend to address specific vulnerabilities, decreasing the probability of compromise should a threat actually arise. These can be both physical and virtual barriers (walls, doors, gates, locks, passwords). Robust identification and authentication mechanisms reduce the probability or attempts to gain unauthorized access to a building but for a dedicated threat actor, these mechanisms alone may not dissuade their efforts;
- **Detection -** Detecting threat events can address certain vulnerabilities and permit rapid response to contain, limit damage, and limit severity of outcome if an event occurs. For example, guard patrols, CCTV, and motion sensors;
- **Response -** When coupled with detection, the security function of response mitigates vulnerabilities. If there are no proper response mechanisms in place, prevention and detection serve only as limited deterrence. If prevention and detection are coupled with a quick response, the combination of safeguards can significantly reduce potential vulnerabilities and mitigate risk by reducing the amount of harm arising from a compromise; and
- **Recovery -** Recovery mechanisms can offset other vulnerabilities and promote a quicker return to normal operations. Recovery may also mitigate the severity of the outcome. This security function could include; backup procedures, offsite storage of critical data, etc.

Once the safeguards have been identified, their effectiveness needs to be determined in order to mitigate potential risks. Calculating safeguard effectiveness includes:

- The security functions performed by all protective measures that indicate how they interact with the primary risk variables, namely asset values, threats, and vulnerabilities; and
- Stating the impact of the safeguards on threat events.

Table 7: Safeguard Impact on Risk Variables and Threat Events

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

Legend

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

Alt Text: The above graphics depicts a table from the HTRA Methodology as a visual example of determining safeguard impacts and how they interact with the risk variables, as well as with the threat events.

While safeguards and safeguard effectiveness can be measured based on how the safeguards impact risk variables, namely vulnerabilities, safeguard effectiveness can also be measured based on variables associated with a threat event itself; what might occur if a threat attempts to directly impact an asset. The impact of threat events on safeguard performance can be measured through three criteria; the Likelihood of Occurrence (LoO) which is already computed in the previous phase, Probability of Compromise (PoC), and Severity of the Outcome.

Probability of Compromise (PoC): is the chance of unauthorized access, disclosure, destruction, removal, modification, use or interruption of assets or information. A compromise would result in a high degree of injury to the health, safety, security or economic well-being of Canadians or to the effective functioning of the government. PoC can be evaluated through the security function of prevention as effective preventive measures to reduce the likelihood that a threat event will compromise an asset.

Severity of the Outcome (SoO): is the ensuing damage that could result if a threat event were to be successful at compromising any safeguards in place by exposing vulnerabilities. The SoO depends on how effective the safeguards in place are, and can be evaluated through the safeguard functions of detection, response, and recovery. When safeguards are effective, they can reduce the amount of damage arising from a compromising threat event.

When assessing safeguards, the best practice is to directly view existing safeguards, instead of relying on reports or photographs. Observing how the safeguards operate and interact with personnel, and other assets, provides assessors a realistic perspective and whether there are any related vulnerabilities that might stem from that safeguard's operation. For example, is a high-quality combination lock performing an effective prevention function by keeping information secure if an incorrect combination is entered or if the container is left unlocked? Is an access control system performing an effective detection function as it measures unauthorized access to a facility?

9.1.3. Vulnerability Identification

Once safeguards have been identified and evaluated for effectiveness, assessors should identify vulnerabilities that are present. Vulnerabilities can be derived from lapses in safeguard performance or related vulnerabilities. Just like assessing safeguard performance, TRA teams should carefully consider all assets in the scope, and use the information gathered as part of their threat scenario conclusions to critically determine if the safeguards in place can protect the assets.

One method to help with this analysis can be to divide vulnerabilities into vulnerability classes, which are generic groupings based upon the broad security policy requirements defined in the PGS and the mandatory procedures for physical security control (Appendix C) of the Directive on Security Management. These should be considered when assembling the data previously collected, to have a more focused scope for later analysis. The HTRA methodology lists 17 classes of vulnerabilities to help assessors determine vulnerabilities for consideration; however, not all classes will be necessary in every security environment. In addition, not all vulnerability classes would be most relevant to physical security environments. Departments that deal primarily with Information Technology (IT) security or business continuity planning have potentially different vulnerabilities versus vulnerabilities faced by physical security practitioners. Types of safeguards that are already in place, the department's primary function, and information being processed would be good indicators of vulnerability classes to which a department could be more susceptible.

Example: An access card reader allows authorized persons to access certain areas of a building. It is effective in it that it denies entry to those without a pass and authorization for the area. Vulnerabilities may include another person following behind the authorized person, or an authorized person holding the door for someone that didn't scan their card, whom they don't know if that person has access to the area or not. Both these vulnerabilities can lead to compromised and the impact could be severe.

9.1.4. Vulnerability Impact Analysis

After vulnerabilities have been identified, their impacts need to be assessed based on Probability of Compromise (PoC) and/or Severity of Outcome (SoO). HTRA recommends using PoC and SoO as the metrics for analyzing the impacts of vulnerabilities as they provide a basis when performing comparative analysis of all the different vulnerabilities

that result and could expose the assets to harm. The assessors need to determine the impact on the PoC based upon the relative effectiveness of associated prevention mechanisms, and the impact on the SoO based upon the relative effectiveness of associated detection, response, and recovery mechanisms. These impacts should be categorized into individual calculations for PoC and SoO respectively that will both range from Low to High. Once PoC and SoO are determined separately, assessors can then compare the two values using a comparison table in HTRA to determine the overall vulnerability rating.

They are divided into two separate calculations based on their security functions. Each function leads to a different level based on the safeguard's effectiveness; not all safeguards perform the same security function, and therefore should be separated to indicate such. Effective preventive measures reduce the probability that a threat event will compromise an asset. Prevention measures are coupled with PoC, which could include having an effective lock on a secure cabinet, as it reduces the probability of someone successfully accessing the information contained within the locked cabinet.

Effective detection, response and recovery measures, which are coupled with SoO, reduce the amount of damage or level of impact arising from a compromising threat event. For example, having an alarm system in an office space which is able to detect when an alarm code entered incorrectly, or if unauthorized access to the space is detected. This would create an audible alarm and generate a response, which allows for conformation of an unauthorized entry or if the door just wasn't closed properly. This allows for recovery to be quick and complete and work to resume in a timely manner.

Table 8: HTRA Probability of Compromise Chart

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

Alt Text: The above graphics depicts a chart from the HTRA Methodology for understanding Probability of Compromise based on either the effectiveness of the safeguard, or any associated vulnerabilities resulting from the poor implementation of safeguards.

Safeguard effectiveness and associated vulnerabilities are determined by the poor implementation of safeguards. If there were no preventive measures in place, or they were largely ineffective, the associated PoC would be elevated. Mechanisms that prevent some threats from occurring, while allowing others to cause harm, are only moderately effective. While safeguards that reduce the probability of most threats taking place are very effective. The more efficient the safeguard is at protecting an asset or a group of assets, the less chance there is of a complete compromise. The less effective a safeguard is at fulfilling its prescribed purpose, and the more associated vulnerabilities exist, the higher the PoC. For each asset with an identified vulnerability, determine the impact of the PoC based upon the relative effectiveness of any associated prevention mechanisms, the ease of exploitation, and other identified factors. Assign a level of Low, Medium, or High from table 9 above. Select Not Applicable if the vulnerability relates only to detection, response and recovery measures.

Example: A high-quality combination lock performs a prevention function; it prevents an individual from accessing information or permitting entry to a cabinet, door, fence, etc. If the lock is a very effective safeguard with a prevention function, this would result in a PoC of Low.

Table 9: HTRA Severity of Outcome Chart

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

Alt Text: The above graphics depicts a chart from the HTRA Methodology for understanding Severity of Outcome based on either the effectiveness of the safeguard, or any associated vulnerabilities resulting from the poor implementation of safeguards.

Safeguard effectiveness and associated vulnerabilities are determined by the poor implementation of safeguards. Inadequacies or vulnerabilities could increase the SoO by allowing a threat to continue unnoticed and unchecked. The more efficient the safeguard is at detecting if an asset or a group of assets might be compromised, coupled with response and recovery measures in place, the lower the chance there will be a severe impact. The less effective a safeguard is at doing its prescribed purpose and the more

associated vulnerabilities exist, the higher the SoO. For each vulnerability exposing assets within the scope of the assessment, assessors determine the impact on the SoO based upon the relative effectiveness of the associated detection, response and recovery mechanisms. Assign a level of Low, Medium or High from table 10 above. Select Not Applicable if the vulnerability relates only to prevention measures.

Example: An alarm system performs a detection, response, and recovery function as it creates an alarm to alert that an unauthorized entry has occurred. If the alarm system is a largely ineffective safeguard with a detection, response, or recover function and was unable to detect a potential compromise if someone disabled the alarm code keypad, this could lead to more damage, resulting in a SoO of High.

9.1.5. Assigning Vulnerability Level

After assessing the PoC and the SoO individually, those assessing vulnerabilities can compare these values together to generate an overall calculation of a vulnerability level. Within HTRA, vulnerability ratings can be ranked from Very Low to Very High using the comparison table below.

Example: A combination lock for a security container performs a prevention function as it reduces the likelihood of the contents, Secret information, from being stolen or compromised. If the lock is broken and not effective, that would generate a vulnerability level of High, however because the combination lock does not perform a detection, response, or recovery function, it would be assessed as Low or N/A. When combining the two scores: High x Low or N/A, generates a level of Medium. That is the highest overall vulnerability level that can be calculated based on the safeguard-only performance of a prevention function.

This example demonstrates that vulnerability assessments of safeguards, if performed individually rather than interdependently, can lead to potential problems. When there are separate but interconnected weaknesses related to PDRR functions, the Basic Vulnerability Assessment calculations should be extended to examine these cooperative relationships in order to determine, more holistically, the level of vulnerability.

Table 10: HTRA Vulnerability Level Matrix

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

Alt Text: The above graphics depicts the process for calculating Vulnerability Levels from the HTRA Methodology using the Basic Vulnerability Assessment table

9.1.6. Extended Vulnerability Assessment

There are unfortunately some limitations when performing a basic vulnerability assessment. A basic assessment looks at identification and evaluation of safeguards through only one dimension, Probability of Compromise (Prevention) or Severity of Outcome (Detection, Response, Recovery). Not all safeguards independently impact both. When a safeguard only performs one of the above functions (PoC or SoO), the function that it does not perform is always assessed at a level (Low or Not Applicable). Thus, according to the vulnerability assessment table 10 above, the highest vulnerability can only reach Medium. An extended vulnerability assessment looks at the bigger picture by re-evaluating safeguards with only one function by considering safeguards together and how cascading vulnerabilities can impact that safeguard's function. This allows for a more accurate determination of that safeguard's performance and corresponding vulnerability level.

If a safeguard such as a locked gate only has a security function for limiting individuals into an area (prevention), it is lacking in the case of Detection, Response, and Recovery, giving it a low or N/A rating using a basic vulnerability assessment. Using the extended vulnerability assessment, the PoC and SoO that would result, based on that safeguard's function, would also consider the other metrics, labelling them high as well, just like under the prevention function for PoC.

Simple Scenario

The first way to consider applying an extended vulnerability assessment, is to develop a simple scenario. In a simple scenario, retain the original vulnerability rating for the primary function the safeguard performs, either PoC or SoO, and reassess the Low or N/A vulnerability rating based on the missing or deficient criteria using the other safeguard vulnerability data collected for the assessment. If a safeguard only performs a prevention function (PoC) but no detection, response, or recover function (SoO), do other safeguards under assessment, perform the missing detection, response or recover function? The bigger picture needs to be considered for how the safeguards are performing, and what other deficiencies or vulnerabilities might be leveraged by threats to compromise the assets under evaluation. Assessors are often able to determine that the related vulnerabilities associated with the safeguard, not performing a specific function, will give a more reliable vulnerability rating for that missing function. By combining the previous primary vulnerability with this new rating (a newly determined PoC or SoO rating) allows for a determination of the actual vulnerability.

Table 11: HTRA Vulnerability Table – Simple Scenario

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

Alt Text: The above graphics depicts the process for calculating Vulnerability Levels from the HTRA Methodology using the Basic Vulnerability Assessment table

Example: The safeguard in use is an inadequate lock on a door to prevent access to a warehouse which does little to prevent unauthorized access and theft. It can be determined this ineffective safeguard has a weak prevention function, giving a PoC value of High. The lock on its own does not perform a detection, response or recovery function. This means that under the criteria of a basic vulnerability assessment, this weakness would warrant a Low or N/A for SoO. This means the total vulnerability rating would be capped at Medium. This is not a reliable calculation for the overall or actual vulnerability rating of the warehouse because the big picture was not considered, such as any other safeguards (or lack thereof) to properly achieve this vulnerability rating. Let's assume the warehouse does not have security guards nor intrusion alarms to detect unauthorized entry. When applying the extended vulnerability assessment criteria, you need to consider any other mechanisms that could fulfill the missing SoO value and since there are none that could influence SoO for the warehouse, and complement the lock's safeguarding capacity, this would result in a rating of High for SoO. When considering the previously identified PoC as High (the weak lock) with the newly calculated value of High for the SoO (no other safeguards in place) produces a calculation of High x High = Very High vulnerability rating results overall, a much more realistic conclusion.

Compound Scenario

Unlike the simple scenario which considers only one missing value for the vulnerability calculations (either PoC or SoO), it becomes a little complicated when vulnerabilities can affect both the PoC and the SoO. When this is the case, assessors should consider the following when recalculating a low or N/A value for a missing PoC or SoO value:

- Start by identifying the Low or NA value for the missing vulnerability or safeguard function (either PoC or SoO). This missing value represents the value that the safeguard does not perform - the value you will determine through the extended vulnerability assessment;
- After identifying the missing value for either PoC or SoO, consider the primary value the safeguard performs (a prevention function (POC) or detection, response, or recover function (SoO). Are there other safeguards that perform the same function? If so, what are those values? (Low, Medium or High);
- If the ratings of these other safeguards are the same as the safeguard you are assessing (the same levels for the safeguards primary function (either PoC or

SoO)), analyze the missing vulnerability value (the Low or N/A PoC or SoO) using the same format of the simple scenario – consider other safeguards that perform only the Low or N/A value and keep the primary safeguard value the same; and

- If the primary values of the safeguards differ (the safeguard being analyzed for the extended vulnerability is more or less effective in its primary function compared to other safeguards that perform similar functions), assessors will need to prioritize either the higher or lower value (the most or least effective safeguard - the lowest or highest vulnerability) for the extended vulnerability assessment. The following criteria can help determine which values to prioritize under these circumstances:
    - If the more serious vulnerability is offset by a more effective safeguard with a lower vulnerability rating, use the lower value for the calculation of the primary value in the extended vulnerability assessment; and
    - If the more serious vulnerability undermines the effectiveness of the less vulnerable safeguard, use the higher value for the calculation of the primary value in the extended vulnerability assessment.

Example: Consider again the warehouse with ineffective lock, it had a Medium vulnerability using the Basic Vulnerability Assessment, and now add a well-trained security guard. The new safeguard might individually be assessed as Low for the vulnerability assessment as it offers very effective detection and response capability. If the guard provided moderately effective prevention capability, Medium, and a very effective detection and response capability, Low, the overall vulnerability rating for the guard safeguard would be Low (Medium x Low = Low).

While the guard performs both a prevention (PoC) function, and a Detection, Response and Recovery function (SoO), our lock-set only performs one of those functions (SoO). If the lock was also moderately effective at preventing unauthorized access to the warehouse, a rating of Medium for PoC, the same as the guard, we could apply a simple scenario to calculate the missing Detection, Response or Recovery function for the lock by using the guard's value. If this case, assessors have two different primary values for PoC (High for the lock-set and Medium for the guard), and only one can be selected for the Extended Vulnerability Assessment of the lock's SoO impact. If the weak lock is unlikely to affect the guard's ability to perform a moderately effective prevention function, the lower rating of Medium should be employed (the guard's prevention security function). If the lock might be exploited, and the guard was unable to intervene, which undermines the guard's effectiveness, the rating of High should be used (the lock's prevention security function).

The calculation for the overall vulnerability level based on the Extended Vulnerability Assessment would be either Low or Medium for the related vulnerabilities. This depends upon how the prevention functions interact based on the two different safeguards. It is not always easy to determine or clear how the vulnerabilities interact, and most safeguards should be assessed in tandem because a building, zone, or area will likely

have multiple safeguards in place. This process highlights the importance of considering vulnerabilities and safeguards as a whole, instead of looking at them individually. The performance of one safeguard could be undermined by a less effective safeguard, or a series of safeguards together provide the best overall protection for assets from threats.

Once all vulnerabilities are assigned a rating based on a comparison of PoC and SoO, all of the information is compiled to produce a comprehensive list of vulnerabilities which may be ranked from the most to least serious. By sorting the vulnerability levels from Very High down to Very Low, you can quickly prioritize individual vulnerabilities and identify those of greatest significance which needs to be addressed first.

Table 12: HTRA Vulnerability Table – Compound Scenario

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

Alt Text: The above graphics depicts the process for calculating Vulnerability Levels from the HTRA Methodology using the Basic Vulnerability Assessment table

Table 13: Extended Vulnerability Calculation Table

Safeguard	PoC Impact (Prevention)		SoO Impact (Detection, Response, Recovery)		Vulnerability Level
Lock	High	x	Low (or N/A)	=	Medium
Guard	Medium	x	Low	=	Low

Alt text: The above graphic depicts the chosen safeguards to consider in the compound scenario in order to conduct an Extended Vulnerability Assessment when they affect both the PoC and SoO

9.2. Calculation of Residual Risk

Residual risk represents the amount of risk remaining, following a determination of values for asset, threat, and vulnerability data. A residual risk calculation is to determine residual risk levels ranging from Very Low to Very High based upon the value of assets identified during the assessment, the threats that might compromise these assets, employees and services, and any related vulnerabilities. Various TRA methodologies will prompt assessors to use a basic mathematical calculation to convert risk levels into numerical values which can be compared together to express a total level of residual risk. In HTRA, risk is a function of asset, threat, and vulnerability values or R = f (Aval, T, V). Each value is multiplied together to give an overall risk score. This allows for more accuracy when determining which risk to address first, and how each risk should be handled accordingly based on the prioritized list.

Table 14: Residual Risks Alpha Values to Numeric Risk Scores

Asset, Threat, and Vulnerability Values	Very Low	Low	Medium	High	Very High
Scores for Risk Calculation	1	2	3	4	5

Basic Risk Score	1-4	5-12	15-32	36-75	80-125
Risk Level	Very Low	Low	Medium	High	Very High

Alt Text: The above graphics depict charts from the HTRA Methodology for calculating Risk Scores and aligning with the Alpha Values

As part of the analysis, each of the three variables (Assets, Threats and Vulnerabilities) have been assigned a level from Very Low to Very High. To determine the residual risk, each of the three factors Asset, Threat and Vulnerability values should be assigned a numeric score from one to five in accordance with the first half of table 16 above. Once the risk levels are given numeric scores from one to five for each variable, the final results for residual risk may range from 1 to 125 (Asset x Threat x Vulnerability).

An example would be an Asset's value of (5) x the Threat value (5) x the Vulnerability value (5), produces an overall risk score of 125.

When calculating residual risk using HTRA, there are few things assessors should remember to keep in mind when selecting levels to use in HTRA's residual risk formula:

- **Multiple threats affecting the same asset:** Since assets can be affected by multiple threats (sometimes with different overall threat levels), assessors should create separate entries for assets based on which threat is affecting them. This will allow for one overall asset and threat level to be used for the calculation and vulnerabilities specifically selected for the threat scenario; and

- **Multiple vulnerabilities affecting the same asset:** It is often the case that an asset could be exposed to injury based on multiple vulnerabilities, either involving deficient safeguards, and related vulnerabilities. When selecting from multiple vulnerabilities to determine an overall vulnerability level for the asset, assessors should prioritize the highest overall vulnerabilities based on the threat scenario under analysis. If there is

more than one vulnerability with the highest level for the scenario, assessors can use this level and explain in their rationale that the highest vulnerability level represents the various elevated vulnerabilities and then provide a description of those vulnerabilities.

When considering which vulnerabilities represent the highest overall vulnerability levels, assessors should make sure to carefully consider safeguard performance and extended vulnerability assessment when determining and prioritizing vulnerabilities.

There are instances when using the previous levels from Very Low to Very High, that would allow for improper prioritization of risks to address first. For example, if you have two risks that are at the High level, it might be difficult to determine which risk to prioritize over the other. If one high-risk level translates to a risk score of 36, and the other translates to a risk score of 45, the risk score of 45 (risk level of High) should be prioritized first in the list.

Table 15: Residual Risk Calculation

Alt Text: The above graphic presents the calculation to determine residual risk levels

9.2.1. Prioritized List of Residual Risk

The last step of the residual risk calculation is to compile all the data into a prioritized list. This list of residual risks should be ranked from the most serious to the least (Very High to Very Low). As previously discussed, assigning a numeric value will allow for more accuracy, as the higher residual risks would need to be addressed first and will be referenced during any recommendations, addressed in the next phase of the assessment.

10. Recommendations

Recommendations, when approved and implemented, should reduce unacceptable levels of residual risks to acceptable levels. In concluding the TRA process, assessors compare their residual risk score with the level of risk tolerance that has been established for the assessment. If there are any risks that fall outside of the acceptable thresholds, assessors should perform additional analysis to modify existing or add supplementary safeguards to improve either identified vulnerabilities, or reduce the severity of threats against the assets. Assessors should rank their recommendations based on the impact they will have on residual risk.

It is important to note the risk authority may choose to reject a recommendation to reduce residual risk and accept a higher level of residual risk. This should be recorded for reference. The Recommendations Phase of a TRA project comprises the following:

- Identification of unacceptable risks;
- Selection of potential safeguards; and
- Assessment of projected residual risks.

10.1. Identification of Unacceptable Risks

To determine if a risk is unacceptable, the defined risk tolerance identified in the preparation phase is compared against the prioritized list of residual risks. Any residual risk that exceeds the defined risk tolerance level are unacceptable and require mitigation recommendations that can lower the risk level to the approved risk tolerance level.

10.2. Selection of Potential Safeguards

Each unacceptable risk identified should recommend one or more strategies to mitigate the risk. One of the most effective ways at reducing residual risk is by adding supplementary or modifying existing safeguards for all assets under evaluation for the assessment. Effective safeguards will perform proper PDRR functions, reduce vulnerabilities and threat impacts and serve to mitigate multiple vulnerabilities at the same time is possible. Assessor must ensure the proposed mitigation recommendations are **reasonable**. This information is necessary for the signing authority to make an informed decision regarding implementation. They will assess the possibility of accepting higher risk, increasing the budget or extending the timeline of the project.

10.3. Assessment of Projected Residual Risk

Once the TRA team has identified and proposed safeguards to mitigate any risks that exceed established levels of risk tolerance, these recommendations are assessed to determine their projected residual risk once implemented. To determine this, return to 9.1 Vulnerability Assessment and 9.2 Calculation of Residual Risk and complete these phases again using the data from the proposed safeguards. Proposed safeguards are unlikely to have historic data available on site, and will therefore require collection using alterative means. This can be through specifications provided by the manufacturer, reviewing service offerings from contract companies, or analyzing data from similar facilities that are utilizing the safeguard in their operations. This will give you a projection of the residual risk in the event the proposed safeguards are implemented.

If the proposed safeguards do not bring the projected residual risk equal to or lower than the risk tolerance level repeat section 10.2 Selection of Potential Safeguards, and 10.3 Assessment of Projected Residual Risk until a proposed safeguard brings the residual risk within acceptable levels, or all plausible mitigation efforts have been explored. The point of this process is to reduce the level of risk to the lowest level possible, ideally at or below the established risk tolerance level. There may be cases where the threat or vulnerabilities present may make achieving the desired risk tolerance level unfeasible; in these cases, those sponsoring the project may need to consider formally accepting a higher level of risk. All assessments and recommendations, including ones that do not achieve the desired residual risk score, should be included in the final report. The possibility of reducing risk even if the target level is not achieved can be beneficial to an organizations overall total risk score.

11. Conclusion - Final TRA Report

This final output is a compilation of all the information gathered thus far, into one document that is to be presented to the risk acceptance authorities. The information presented should be concise to justify the need for any recommendations. Each section should focus on the most prominent issues to present to management to review, leaving more detailed information into any summary tables and supporting documentation.

The outline of the final TRA Report should include:

- **Executive Summary-** a summary of all phases of the TRA and their outcomes. An executive summary should be as concise as possible while still conveying the outcome of each phase to provide the relevant information at a glance;
- **Background-** provide information on about the organization, their mandate and service deliveries, the location(s) being evaluated, and any other information that would provide necessary context;
- **Aim-** an explanation of the reason why the TRA is being initiated and how the final report is being utilized;
- **Mandate-** a compilation of the information collected in Section 6.2 Mandate and Project Scope;
- **Scope-** a detailed breakdown of the scope of the assessment as explained in Section 6.2 Mandate and Project Scope;
- **Asset Identification and Valuation-** a detailed description of all assets within the scope of the assessment and their values as described in Section 7.0 Asset Identification and Valuation;
- **Threat Assessment-** a detailed description of all threats identified and their impacts on service delivery as described in Section 8.0 Threat Assessment;
- **Vulnerability Assessment-** a comprehensive description of the vulnerabilities as determined through the vulnerability assessment phase as described in Section 10.1 Vulnerability Assessment Sub-Phase;
- **Residual Risk Assessment-** a detailed breakdown of the residual risk assessment, how it was determined and any supporting information required as described in Section 10.2 Calculation of Residual Risk Sub-Phase;
- **Recommendations-** a description of all recommendations, what they are, why they were chosen and what they are meant to address. Simply stating what needs to be done without details of how, why and the results will not be sufficient to have your recommendations accepted and implemented. This is described in Section 12.0 Recommendations; and
- **Any attachments/cross-references or supporting documentation-** any and all information and documents that were used to complete the TRA, including but not limited to interview minutes, police report data, research documents, product information.

11.1. Report Sign Off - Risk Acceptance Authorities' Role(s)

Once all information has been compiled into a final report the Risk Acceptance Authority, as identified in the Preparation Phase signs off to complete the TRA. The TRA is not considered final until this step is complete.

When signing final TRA report, the signing authority identifies which recommendations, if any, will be initiated. If the selected recommendations do not bring the residual risk to within the risk tolerance level, the signing authority should then accept the higher residual risk and record this for future reference. For information on the risk acceptance process consult GCPSG-018 Guide to the Risk Management Process for Physical Security.

For all approved recommendations, steps should be put in place to ensure they are completed within the timelines determined in the TRA. A plan should also be developed to review and evaluate the implemented recommendations after an appropriate length of time to assess how effective they are reducing the residual risk to the acceptable level. Details on this process can be found in GCPSG-016 Guide to the Facility Assessment and Authorization Process.

12. Reference and Source Documents

- Policy on Government Security- Canada.ca
- Directive on Security Management- Canada.ca
- Levels of security – Canada.ca
- Harmonized TRA Methodology (TRA-1)
- Canada's National Security
- International Atomic Energy Agency - Design Basis Threat
- FEMA 430 Risk Management Series: Site And Urban Design For Security
- FEMA 452 Risk Assessment: A How-To Guide To Mitigate Potential Terrorist Attacks Against Buildings
- National Protective Security Authority (UK)- Protective Security Risk Management
- The National Risk Register (NRR) – (UK)
- GCPSG-015 (2023) - Guide to the Application of Physical Security Zones
- GCPSG-018 Guide to the Risk Management Process for Physical Security
- GCPSG-019 (2023) - Protection, Detection, Response, and Recovery Guide
- GCPSG-016 Guide to the Facility Assessment and Authorization Process.

13. Promulgation

Reviewed and recommended for approval.

I have reviewed and hereby recommend, GCPSG-022 (2025) – Threat and Risk Assessment Guide, for approval.

Nattress,Shawn Thomas,000302786

Digitally signed by Nattress,Shawn Thomas,000302786
Date: 2025.01.17 08:25:18 -05'00'

Shawn Nattress,
Manager
RCMP Lead Security Agency

Date

Approved

I have reviewed and hereby approve, GCPSG-022 (2025) – Threat and Risk Assessment Guide.

St-Pierre,Andre Vincent,000171484

Digitally signed by St-Pierre,Andre Vincent,000171484
Date: 2025.01.31 13:54:09 -05'00'

Andre St-Pierre,
Director, Physical Security
Royal Canadian Mounted Police

Date