Guide to the Risk Management Process for Physical Security

GCPSG-018 (2024)

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

Publication Issued: 2024-03-15
Updated: YYYY-MM-DD

Royal Canadian Mounted Police | Gendarmerie royale du Canada

Canada

Foreword

The Guide to the Risk Management Process for Physical Security 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 to serve as a guideline on considerations specific to the development of risk management processes, including physical security risk management, and the creation of related standard operating procedures (SOP) for departments, agencies and employees of the Government of Canada (GC).

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

Reproduction

Effective Date

The effective date of the Guide to the Risk Management Process for Physical Security is 2024-03-15.

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 guide is to assist GC employees with physical security risk management responsibilities in the development of their own processes related to physical security risk management, risk decision making delegation, and the documenting and monitoring of residual risks. The Policy on Government Security (PGS) requires physical security measures to be implemented, monitored, and maintained. These processes must be formally documented throughout all stages of a measure's life cycle. This document connects existing tools and their uses together to outline effective and clear ways for departments to meet their security requirements outlined in the PGS and the Directive on Security Management (DSM).

The guide contains both required security control safeguards (indicated by use of the word "must") as directed by GC policies and directives, and recommended security control safeguards (indicated by the use of the word "should").

1.2. Applicability

This guide applies to all employees in the GC with physical security risk management decision making authority. The intended audience of this guide is department heads, Chief Security Officers (CSO), managers, and physical security practitioners that have been delegated physical security risk management authority or are responsible for identifying physical security risks to senior managers who have that delegated authority. This document can be applied to risk assessment and acceptance processes related to physical security, and can be used to create or update departmental policy, directives and programs related to physical security risk management.

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

All employees of the Government of Canada (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 Government of Canada 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
CCTV	Closed Circuit Television
DSM	Directive on Security Management
FSA&A	Facility Security Assessment and Authorization
GCPSG	Government of Canada Physical Security Guide
PHYSEC	Physical Security

PGS	Policy on Government Security
SA&A	Security Assessment and Authorization
SOP	Standard Operating Procedures
TBS	Treasury Board Secretariat
TRA	Threat and Risk Assessment

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.
Availability	The condition of being usable on demand to support operations, programs and services.
Breach	An act or omission, deliberate or accidental, that does result in the actual or possible compromise of Classified or Protected information or assets or interruption of service.
Classified Information	Information, whose compromise would reasonably be expected to cause injury to the national interest.
Compromise	Unauthorized disclosure, destruction, removal, modification, interruption or use of information or assets.
Continuous Monitoring	To confirm on a continuous basis that there has not been a breach of security. Examples include electronic intrusion detection systems or someone guarding a particular point on a constant basis.
Facility	Something that is built, installed, or established to serve a particular purpose. A facility may include a specific building (whole or part) or the site or land it is located on. The term encompasses both the physical object and its use (weapons' ranges, agriculture fields).
Facility Security Assessment and Authorization	The process by which organizations ensure that security assessments are performed on new and existing GC facilities and fit-up projects. Appropriate security controls are identified and implemented before authorization is given to allow the facility to be occupied.
Integrity	The accuracy and completeness of assets, and the authenticity of transactions.
Monitoring	To watch for or detect a breach of security.
National Interest	Subjects concerning the defence and maintenance of the social, political and economic stability of Canada.
Need-to-Know	The principle that there is a need for someone to access and know information in order to perform their duties.
Projected Residual Risk	The anticipated risk after the suggested recommendations and

	safeguards have been fully implemented.
Protected Asset	Assets whose compromise would reasonably be expected to cause injury to other than the national interest.
Protected Information	Information whose compromise would reasonably be expected to cause injury to other than the national interest.
Residual Risk	The risk that remains after safeguards have been selected and implemented.
Risk Statement	Description of an event and the potential impact (positive or negative) of that event on achieving an organization's objectives.
Security Assessment	Ongoing process of evaluating security practices and controls to establish the extent to which they are implemented correctly, operating as intended, and achieving the desired outcome with respect to meeting defined organizational security requirements.
Standard Operating Procedures	A written set of instructions outlining step-by-step actions to take in order to complete a task(s) and/or respond to an incident. SOP are intended to standardize performance and compensate for any lack of knowledge or experience.
Threat	Any potential event or act, deliberate or unintentional, or natural hazard that could result in a compromise.
Threat Risk Assessment (TRA)	Assessment of a facility to identify risk, threats and vulnerabilities to assets (information, employees, services).
Unauthorized Access	Access to information or assets by an individual who is not properly security screened and/or does not have a "need-to-know".
Unauthorized Disclosure	An event involving the exposure or disclosure of material to individuals not authorized to access the material.
Vulnerability	An inadequacy related to security that could increase susceptibility to compromise or injury.

5. The Risk Informed Decision-Making Process

Being risk informed is understanding the relationship between the likelihood of an event occurring, the possible levels of damage associated to each event, and the harm to the assets, personnel, and/or service deliverables should an event occur. It is essential for decision makers to have a complete understanding of these factors when making decisions that could have an effect on the physical security of critical assets and functions to their department or agency. Having formalised and documented processes, related to the management of risk, is vital for achieving this physical security objective; as decision makers at all levels will not have the time to review and analyse the data, in its entirety, during an event or crisis. This will also allow for greater opportunities to identify vulnerabilities in the physical security apparatus of a department or agency and expedite corrective actions.

In accordance with DSM, Section 4.6.3, individuals designated by the Deputy Head are also required to communicate to client departments the security practices and controls that have been implemented to meet defined security requirements, the security conditions that need to be in place in the client environment, and any remaining residual risks and recommended mitigation measures.

The Framework for the Management of Risk provides guidance to Deputy Heads on the implementation of effective risk management practices at all levels of their organization, ensuring compliance with the DSM. This supports strategic priority setting and informed risk tolerance decisions.

Effective risk management in the federal government should:

- Support whole of government priorities;
- Be tailored to the departmental or agencies' mandate, priorities, risk culture, and stakeholder interests;
- Achieve a balance between risk response/established controls and support for flexibility/innovation to improve outcomes;
- Be transparent, integrated and systematic;
- Continuously improve the culture, capacity, and capability of risk management; and
- These principles should influence and guide the decision-making process when developing and implementing departmental and agency Standard Operating Procedures (SOP) and policy.

When properly implemented the Framework for the Management of Risk helps to ensure physical security measures are properly assessed, implemented, monitored and maintained in compliance with TBS policy and directives. The framework empowers deputy heads to integrate security in a way that ensures the assets in their care are wholly protected and allow for a culture of continuous improvement and vigilance to all aspects of security; including physical security.

A risk-aware culture is when a department or agency, as a whole, understands the importance of all risk management activities and empowers employees to openly participate in the risk management process. Departmental leaders are encouraged to foster this cultural development by collaborating with staff regularly, being available to train and mentor their teams, and by setting a positive example through their own security and risk-aware actions. Supporting accountability also promotes a risk-aware culture, encourages due diligence in all risk management tasks, and, when encouraging employees' improvement of these skills, can promote a commitment to risk awareness in their professional development.

There are mandatory security courses for all government employees, however, it is a best practice to expand on these learning opportunities. This can be achieved through:

- Mentorship programs;
- Round table discussions;

- Department/agency specific training; and
- Integration of security awareness in regular development sessions and onboarding.

The Guide to Integrated Risk Management covers a wide range of topics related to risk management, including areas that directly corresponds and strengthens physical security specific risk management processes. Consult that guide for a more in depth look at the integrated risk management process.

6. Risk Assessment and Acceptance Process

A department or agency's physical security environment must be formally assessed, on a periodic basis, by a member delegated the authority to handle physical security risk decisions (see 8.1.1. Delegation Matrix Example). In events when this risk exceeds their authority to accept, the decision must be escalated (see 8.2.1. Escalation Flowchart Example).

There will be occassions when an established baseline cannot be reasonably achieved. These circumstances can arise due to time limitations, geographic complications, or legal or legislative barriers. The decision to accept any risk, including physical security risks, should not be taken lightly, and in exercising due diligence, the investigation of all alternatives to alleviate the risk must first be completed.

It is encouraged that each department develops a standard approach to evaluating and accepting physical security risk that aligns with their existing processes. Each of the seven phases of a TRA, outlined below, should be understood and considered by the risk owner when assessing and accepting any physical security risk. There are seven phases to a TRA that a risk acceptance authority should understand before assigning a team to conduct a TRA.

6.1. Preparation

The Preparation Phase will identify the scope of the assessment, and the acceptable level of residual risk. The scope of the assessment should be determined by an employee with physical security risk management authority to determine what assets will be evaluated in the TRA. The physical security risk management authority should also assign the assessment to a qualified team of security practitioners. In this phase the TRA team leader should be provided enough information to create a workplan outlining the key deliverables at each stage as well as the required resources to complete a TRA. Once a workplan has been completed it should be reviewed to ensure it remains within budget, maintains the required timelines, and the requested staff can be assigned to the project. If the TRA workplan is acceptable management should document their approval and have the team commence the assessment.

6.2. Asset Identification and Valuation

The Asset Identification and Valuation Phase will identify all assets within the scope of the TRA (Classified assets, firearms, assets for a specific project). 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; the highest scoring category should be identified in the listing. The categories are as follows:

6.2.1. Confidentiality

How much damage would be done should this information be compromised? Aggregation of less sensitive data may increase the value of this score.

6.2.2. Availability

How much damage would be done if this asset was rendered inaccessible to staff or clients?

6.2.3. Integrity

How much damage could be done if the asset was modified and rendered inaccurate, fraudulent, or incomplete?

6.2.4. Replacement cost

How much would it cost to replace the asset? This value should be listed alongside the highest scoring value above.

The deliverable for this phase is an Asset Valuation table/Statement of Sensitivity.

6.3. Threat Assessment

The Threat Assessment Phase will identify and list all real and potential threats the asset may realistically face within the scope of the TRA (hostile intelligence agency, organised crime, accidents, natural disaster). The threats must be listed and assigned a Threat Level from very low to very high. This value is determined by the likelihood of an occurrence and the gravity of the threat. When determining the gravity of the threat calculations should be made for the following categories:

6.3.1. Potential Loss of Life

Is there a risk to life? How many casualties could be expected should an event occur?

6.3.2. Operational Availability

Will this threat effect the reduce or cease the ability for the department or agency to accomplish their mission? How critical is it that the mission is achieved? How long will it

take to regain operational capacity?

6.3.3. Economic Costs

How much money will it take to recover from the event (manpower, repair/replacement, lost revenue)? How many securities could be irrecoverably lost (cash, precious metals, bearer bonds)?

6.3.4. Reputation

Will an event negatively effect stakeholder trust in the department or agency? Would an event negatively effect a client's reputation due to assets they have placed in the care of the department or agency?

Once the Threat Levels have been calculated, by the methodology employed, they are to be used to create this phase's deliverable: A Prioritised Threat List.

6.4. Vulnerability Assessment

The Vulnerability Assessment Phase will have the TRA team evaluate the existing safeguards, or lack thereof, and determine how vulnerable the asset is against the identified threat, based upon predetermined parameters defined for all team members conducting the assessment. The TRA team will measure a safeguards probability of compromise and severity of outcome from low to high. The lack of a safeguard is an automatic high rating. These two values are then used to calculate the vulnerability level from very low to very high. Once all the vulnerabilities within the scope of the TRA have been assessed, they can be compiled into a Prioritised Vulnerability List for this phase's deliverable.

6.5. Calculation of Residual Risks

The outputs from the previous three phases can then be used to calculate residual risk. There may be more than one Residual Risk Score for each asset as some are subject to multiple threats and vulnerabilities. These will all be calculated individually and assigned their own residual risk score. Residual Risk is a numerical calculation that will give a score from very low to very high. This score corresponds with the acceptable risk level identified in phase one of the TRA. The output will be identical regardless of the method used. This phase's deliverable is complete when the team compiles the residual risks cores into a Prioritised List of Residual Risks.

6.6. Recommendations

The Recommendation Phase 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 the team will either recommend the status quo be maintained, or safeguards adjusted to match the risk tolerance. In the event they recommend the safeguard be reduced or removed they must recalculate the residual risk for

the proposal for the designated authority. For all cases where residual risk exceeds the acceptable level, the TRA team will propose alternative measures to reduce the residual risk to the acceptable level. The designated authority can then review all proposed safeguards and their resources costs and determine if they will implement one or more, or refuse and formally accept the above baseline residual risk.

6.7. Conclusion

The final Conclusion Phase is where the TRA team will summarise all of the data contained in the report, similar to an executive summary. There should be sufficient information provided for CSOs, or their delegates, to understand the entirety of the report and be enabled to locate additional information for any follow-up calculations. Also included will be management's decisions to accept or decline recommended safeguards, to maintain, increase, or decrease existing safeguards, and a formal signature acknowledging these decisions and the authenticity of the report. Only after the CSO or their delegate signs the TRA report will this process be complete. For more information on TRA in a Government of Canada context, consult GCPSG-022 Threat Risk Assessment Guide.

7. Integration of Countermeasures

After identifying the safeguards and physical security posture appropriate for a department or agency, these functions will need to be integrated into the daily tasks of staff to ensure they are most effective. It is counterproductive to have physical security systems set up as a separate entity to daily operations; protection of assets is a core function of operations and it should be prioritised as such. Ensuring the need to document, review, and update physical security safeguards should be tied into the operational functions of the asset or service. When possible, integrating the physical security safeguard's review into repeated operational functions, such as quarterly audits, will improve the synergy of both functions. Another benefit of a well-planned integration strategy is ensuring the review has the time it needs to be done completely and with due diligence, reducing the risk of it being rushed as deadlines approach.

7.1. Developing Standards and Procedures

Department and agency security standards must support the adoption of integrated processes, ensuring there is oversight and documentation clearly outlining the expectations of senior management; as well as standardizing the manner in which data is collected, analysed and maintained. There are several considerations that should be included in a standard; although the final version will vary greatly from case to case. It is advised these standards clearly identify which positions are responsible for what processes and how the data will be recorded and complied. For example, office staff may be required to report the condition of cable locks securing laptops when signing the equipment in and out. The unit manager may then review the logs and audit the inventory quarterly; compiling a report on the effectiveness and condition of safeguards (Example: No unaccounted inventory, minor

wear and tear on three locks needing attention, safeguard deemed effective with no change advised).

It is advised the final reports of all safeguard monitoring eventually reach a single point, such as the CSO or delegated team member. Integration of this method would be most effective if it follows a pre-established chain of possession, such as the internal escalation / delegation model. The more consistency there is between processes, the easier it will be for staff to navigate them all. This would increase the efficiency of the countermeasures employed, while promoting a recognised process and positive physical security risk culture.

8. Delegation of Risk Management Responsibilities

Individuals who have been designated by the Deputy Head to hold key security roles and responsibilities under DSM Section 4 may further delegate these roles; so long as due diligence and oversight is exercised in every function and task. This can improve efficiency when delegated tasks are assigned to appropriate members who have a working-level understanding of the physical security safeguards and assets involved in their area of responsibility. Poorly implemented delegation strategy, or a lack of oversight, can have the opposite effect; leaving gaps in reporting, escalation, and exposing departments and agencies to unnecessary vulnerabilities and liabilities. A clear and conducive delegation strategy supports staff in meeting their responsibilities related to physical security risk management. The following are best practices for a department or agency's physical security risk strategy and culture.

8.1. Standardizing the Delegation of Responsibilities

A standardized delegation strategy is prescribed by the PGS and supports critical data reaching senior management to inform their physical security risk management decisions. Departments and agencies are permitted to develop a delegation process for all security risk management roles that suit their unique operating environment within the GC. Developing a corporate risk profile will provide a strategic overview of the assets and functions that require protection and identify which physical security risk management responsibilities may be candidates for delegation.

Ideally, the delegation of physical security risk management oversight should be prioritized to individuals already involved in overseeing the security governance of the department, agency, or facility; with a preference afforded to personnel that have a background or previous training in physical security. A baseline level of training should be provided to all staff who have been delegated to handle any risk management responsibilities to ensure they can properly execute the required functions. Considerations should also be given to the pre-existing organizational structure and, if possible, delegated duties should utilize the same configuration. This integrates the physical security risk management delegation process into the structure of the department or agency and ensures personnel are aware of the appropriate communication channels for the approval of different queries and tasks.

8.1.1. Delegation Matrix Example

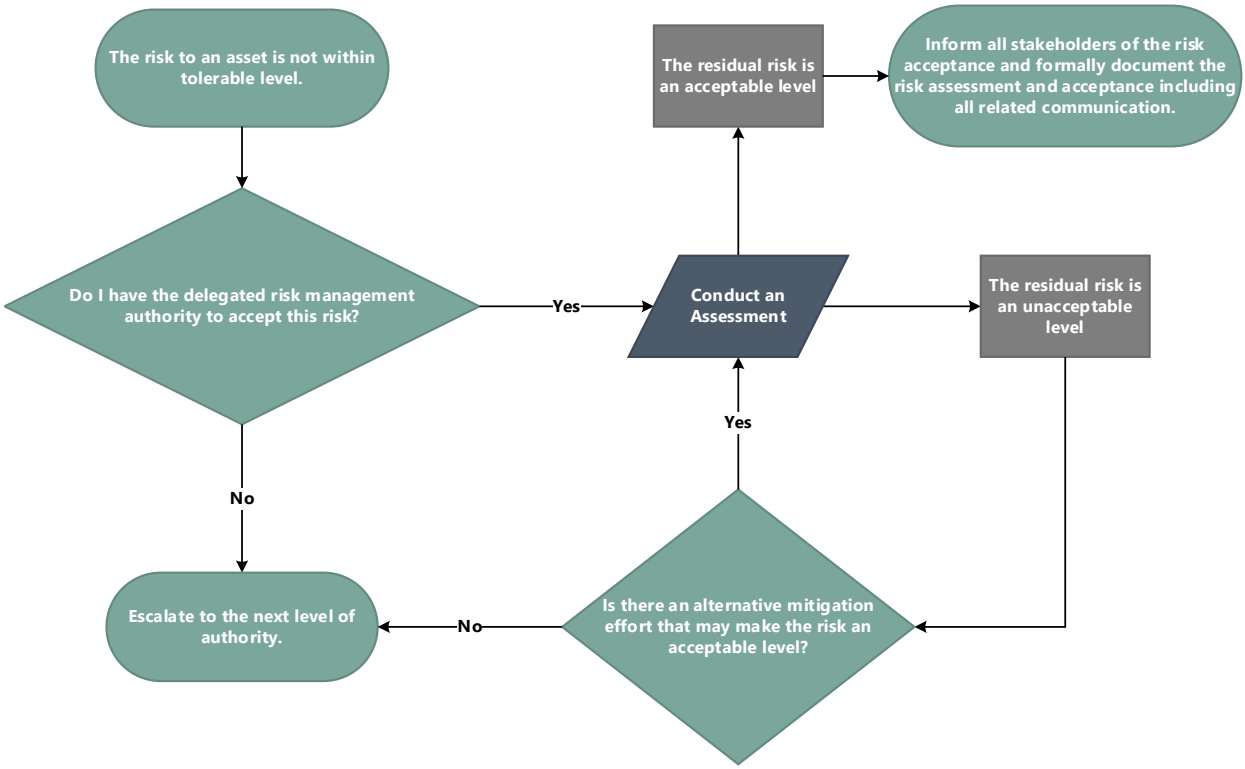
Example Task Actions	Management Levels (ML)					
	ML 0	ML 1	ML 2	ML 3	ML 4	ML 5
Deputy Head / Commissioner	**ML 0**	**ML 1**	**ML 2**	**ML 3**	**ML 4**	**ML 5**
Designate Chief Security Officer (CSO)	**ML 0**					
Approve security-related directives and standards	**ML 0**	**ML 1**	**ML 2**			
Approve Risk Delegation (ML 2- ML 5)	**ML 0**	**ML 1**	**ML 2**			
Approve security-related procedures and guidelines	**ML 0**	**ML 1**	**ML 2**	**ML 3**		
Approve physical security controls (access control, CCTV)	**ML 0**	**ML 1**	**ML 2**	**ML 3**		
Approve High Risk deviations from physical security standards	**ML 0**	**ML 1**				
Approve Medium Risk deviations from physical security standards	**ML 0**	**ML 1**	**ML 2**	**ML 3**		
Approve Low Risk deviations from physical security standards	**ML 0**	**ML 1**	**ML 2**	**ML 3**	**ML 4**	
Approve security awareness and training requirements, practices, and plans	**ML 0**	**ML 1**	**ML 2**	**ML 3**	**ML 4**	
Submit a request to Accept a Risk		**ML 1**	**ML 2**	**ML 3**	**ML 4**	**ML 5**

Level	Employee Positions
ML 0	Deputy Head / Commissioner
ML 1	ADM, Director General, CSO (reporting to Deputy Head)
ML 2	Region Directors, CSO / DCSO, Region Managers (reporting to Level One)
ML 3	Regional Managers, Managers (reporting to a Level Two)
ML 4	Managers or Supervisors (reporting to a Level Three)
ML 5	Managers or Supervisors (reporting to a Level Four)

8.2. Standardizing Escalation of Security Reporting/Incidents

The timely communication of security incidents to responsible decisions makers, or to escalate, is the responsibility of all GC employees. Failure to properly escalate a situation may have catastrophic implications to a department or agency's business goals and harm their image in the eyes of stakeholders. Every department and agency must have processes for the escalation and documentation of security breaches and incidents as per DSM Appendix G where a formal Threat and Risk Assessment may not be warranted. When standardizing an escalation process it should follow the same channels as the delegation process, up to the level that has the authority to action a response to the incident. The individual for whom the escalation process will end shall largely depend on the severity of the incident and the amount of autonomy granted to each level by leadership. A risk taxonomy can provide a list of the most likely or damaging threats each protected asset may face. These risks can then be tied to a position on the delegation flowchart that has the authority to action a response. Incidents that could have varying levels of severity should clearly define thresholds of when escalation must exceed the standard level identified by the department or agency matrix.

8.2.1. Escalation Flowchart Example



Alt text: The above image shows an example of an escalation process flowchart

9. Guides and Tools

Various GC departments and agencies have developed tools that are applicable for physical security risk management. Understanding the tools available, and their applicability, are vital in designing and maintaining an effective physical security program. The following publications can be utilized in conjunction with the advice contained in this guide.

9.1. Guide to Integrated Risk Management

The Guide to Integrated Risk Management is intended to assist departments and agencies with strengthening their overall integrated risk management practices. The Guide to Integrated Risk Management does not provide specific physical security risk management practices; as these will be specific to each organization dependent upon their unique mandate, risk exposure, risk management capacity and other factors. It does support a wholistic approach to the management of all risk, including physical security risk, for departments and agencies.

9.2. Guide to Corporate Risk Profiles

A Guide to Corporate Risk Profiles enables departments and agencies to obtain an overview of its key risks including an understanding of the operational context and objectives with respect to managing risk. A corporate risk profile is an output from the risk assessment process that enhances senior management's ability to analyze, prioritize, and budget their risk management strategy. These can also be used to provide a clear snapshot of the department or agencies' key risks and mitigation efforts to staff, practitioners, and stakeholders. A corporate risk profile supports strategic priority setting, allows for informed decision making, and demonstrates a department's or agency's risk tolerance level.

9.3. Guide to Risk Taxonomies

A Guide to Risk Taxonomy is a comprehensive, common, and stable set of risk categories that are used within departments and agencies. This document includes considerations for developing and using a risk taxonomy. It outlines an approach to categorizing and aggregating risks that may be tailored to the specific needs of a department or agency. Risk taxonomies support standardizing systems and help foster a risk aware culture. Risk taxonomies and their complimentary tasks are important to developing a "risk aware" culture by allowing for standard terminology and understanding by employees.

9.4. Guide to Risk Statements

The Guide to Risk Statements is meant to help strengthen risk management practices by elaborating on how to develop risk statements. Risk statements are an essential component in articulating identified threats and opportunities, which are fundamental in supporting the risk management process. A standardized presentation of risk statements improves integration of security processes throughout a department or agency.

9.5. Risk Management Capability Model

The Risk Management Capability Model is a diagnostic tool that allows departments and agencies to benchmark their current risk management capability. This tool may be used to initiate an informed discussion on whether resources need to be allocated or diverted to fill risk management gaps or to improve capability in key areas of the department or agency's risk management priorities.

9.6. RCMP Lead Security Agency Publications

The RCMP LSA, as mandated by TBS, publishes and manages a catalogue of guidance documents covering specific areas of physical security. These documents leverage the professional input of subject matter experts in many fields and are peer-reviewed by the GC Physical Security community to incorporate lessons learned and best practices from across the entire GC. It is worthwhile to review these publications to determine if there are any impacts to a department or agency's physical security risk, especially when considering modifying existing, or developing new, facilities.

10. Continued Monitoring of Risk Mitigation

Proper monitoring and reporting on safeguards are critical components of a successful physical security risk management strategy and ensures legislative obligations are met within the GC. Security plans must be monitored routinely to determine if the physical security risk mitigation strategy is still maintaining an acceptable level of residual risks to assets in a dynamic threat environment. If the effectiveness of mitigation measures employed become questionable, due to a change in risk factors or available resources, then a formal TRA may be warranted to identify any needed amendments to the mitigation strategy.

10.1. Importance of Continued Monitoring

In addition to the mandated monitoring of physical security risk mitigation strategies and physical security safeguards, a standardized system of continued monitoring ensures staff understand their role in mitigating physical security risk to the organization. Clear and concise documentation outlining the monitoring strategy, as well as data on the outcomes and periodic reviews, provides valuable information in a post-compromise investigation. The more forthright the collected data, the easier it will be to identify the breakdown in the system that allowed a vulnerability to be exploited.

Continued monitoring facilitates harm reduction and the ability to proactively identify opportunities to increase the physical safety and security of staff and assets. When this review includes examining new best practices from industry partners and other government departments and agencies, new mitigation strategies can be adopted in to existing safeguards. This may result in increased physical security measures, improved operational

efficiency, potential cost savings, and improved recovery.

10.2. Periodic Assessment

Assessment standards should be set with clear deadlines for the data to be fully compiled, when the review and analysis of the data will occur, and then when the results will be made available. An annual review of a department or agency's Departmental Security Plan or physical security annual workplan should be conducted; however, departments and agencies would benefit from setting their own targets that:

- Allow for the mandatory data to be ready in advance; and
- Review and examine their own policies and procedures to proactively evaluate their initiatives and ensure compliance.

While some timelines are non-negotiable, many that allow flexibility can be linked to operational timelines to encourage operational efficiency and synergy with pre-established milestones. When physical security is integrated into operational requirements it enables an efficient evaluation of a department or agency's entire risk management posture.

10.3. Developing Physical Security Performance Measures

Physical security performance should be measured as part of the periodic assessment to ensure these remain efficient and are still achieving the intended goal. Performance measures will vary between safeguards and will need to be customised based upon assessments by physical security practitioners. When deciding on how to measure the effectiveness of a safeguard, there are several key considerations that should influence the decision:

- What is the safeguard's intended purpose;
- How does the safeguard fit into operational functions;
- Does the safeguard track data or produce a record; and
- Is the safeguard overbearing and at risk of circumvention by staff?

Additional indicators to monitor may include dramatic changes in observed data possibly indicating the following:

- Underreporting of incidents;
- New exploitation techniques employed against vulnerabilities; and
- Non-compliance with current procedures.

While not always negative, a lack of minor incidents may indicate the safeguard is inefficient; however, this alone should not be considered as proof but may indicate that an investigation to confirm the data is warranted.

11. Reference and Source Documents

- Policy on Government Security- Canada.ca
- Directive on Security Management- Canada.ca
- Directive on the Duty to Accommodate
- Appointment Delegation and Accountability Instrument - Canada.ca
- Framework for the Management of Risk- Canada.ca
- Guide to Integrated Risk Management - Canada.ca
- Framework for the Management of Compliance- Canada.ca
- Guide to Corporate Risk Profiles - Canada.ca
- Guide to Risk Taxonomies - Canada.ca
- Guide to Risk Statements - Canada.ca
- Harmonized TRA Methodology (TRA-1) - Canadian Centre for Cyber Security
- Risk Management Capability Model - Canada.ca
- Publications - Royal Canadian Mounted Police (rcmp-grc.gc.ca)
- Guideline for Employees of the Government of Canada: Information Management (IM) Basics- Canada.ca
- Call to Action on Anti-Racism, Equity, and Inclusion in the Federal Public Service
- Guide for Two-Spirit, Transgender, Non-Binary, and Gender-Diverse Employees

12. Promulgation

Reviewed and recommended for approval.

I have reviewed and hereby recommend, GCPSG-018 (2024) – Guide to the Risk Management Process for Physical Security, for approval.

Nattress,Shawn Thomas,000302786

Digitally signed by Nattress,Shawn Thomas,000302786
Date: 2024.03.26 12:09:03 -04'00'

Shawn Nattress,
Manager
RCMP Lead Security Agency

Date

Approved

I hereby approve, GCPSG-018 (2024) – Guide to the Risk Management Process for Physical Security.

St-Pierre,Andre Vincent,000171484

Digitally signed by St-Pierre,Andre Vincent,000171484
Date: 2024.03.26 15:19:08 -04'00'

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

Date