Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Guideline on Developing a Departmental Security Plan

Published: Dec 04, 2013

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT39-14/2013E-PDF
ISBN: 978-0-660-09751-0

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Ligne directrice sur l'élaboration d'un plan de sécurité ministériel

Guideline on Developing a Departmental Security Plan

List of Figures

1. Purpose

The purpose of this guideline is to assist departments in meeting the requirements of the *Policy on Government Security (PGS)* and the *Directive on Departmental Security Management (DDSM)* to develop a departmental security plan (DSP) that details decisions for managing security risks and outlines strategies, goals, objectives, priorities and timelines for improving departmental security. It describes an approach to developing the DSP that is based upon a process of security risk management (SRM) to ensure that decisions for managing security risks are substantiated through thorough analyses and supported by processes which are rigorous, repeatable, and documented. This approach is intended to support the development of a DSP that provides Deputy Heads (DH) and senior managers with an integrated view of departmental security requirements that is aligned with the strategic priorities, programs, plans, processes, and other practices within each department.

The guidance is based upon well-recognized principles and best practices related to planning, risk management, and performance measurement. They have been assembled from TB policy instruments and guidelines, reports from jurisdictions, private industry, and other countries, along with standards bodies such as ISO and NIST. The guideline also comprises input from departmental representatives who participated in its development.

2. Audience

The guideline is aimed at departmental security officers (DSO), security practitioners, and managers at all levels. Their specific roles and responsibilities related to departmental security planning and SRM are identified in the PGS and DDSM.

The guideline may also be useful to departmental corporate risk managers, strategic planners, Management Accountability Framework (MAF) coordinators and other subject matter specialists who play an important role in helping to integrate security into corporate risk management, planning and performance measurement practices and whose corporate perspectives should be considered in the development of the DSP.

3. Application

Deputy heads and DSOs of all departments[1] have policy responsibilities related to security planning and SRM. Each department has unique characteristics with respect to mandate, size, programs, internal management processes and practices, along with resources dedicated to security operations. Given these differences each department, including small departments and agencies (SDAs), should determine an approach to developing its DSP that considers their distinct operations, capacity, and risk environment by adopting or adapting this guideline to best suit their business needs.

4. Implementation

The DDSM provides a three year transition period for full implementation of requirements related to the DSP[2] that began July 1, 2009, and will end June 30, 2012. The following sequencing of activities is suggested to help ensure that each step in the SRM process can be completed and the results used as the basis for developing the DSP.

- Analyze and define the context; initiate consultations
- Conduct and/or complete risk assessments
    - Consolidate results from existing security risk assessment and identify gaps in coverage (i.e. program activities that are not covered by current security risk assessments to address all information, assets, or other resources)
    - Identify requirements for additional controls or performance indicators
- Define security priorities based on results of security risk assessments and analysis of treatment options; develop implementation strategy
- Develop DSP and seek DH approval
- Begin implementation and monitor performance
- Conduct and/or complete risk assessments as required to address identified gaps
- Report progress to DH and senior managers
- Update DSP as required
- Continue security risk management activities and implementation and monitoring of controls
- Maintain DSP and report to DH and senior managers

5. An Integrated Approach to Planning

The management of security is most effective when it is systematically woven into the business, programs and culture of a department and the public service as a whole.[3]

The concepts of integrated planning and integrated risk management are not new. The Clerk of the Privy Council, in his *Seventeenth Annual Report to the Prime Minister on the Public Service of Canada*, reaffirmed the importance of integrated planning stating that "planning should be seen as a core business practice for all public servants, one that is necessary to align goals, resources and results."[4] Previous Public Sector Renewal Plans characterized integrated plans as "a foundation for assessing and understanding the current and future needs of departments and the Public Service as a whole. Risk management, since it is directed at the uncertainty related to future events and outcomes, is an integral component of good planning and decision-making at all levels"[5]. The Framework for the Management of Risk recognizes that risk needs to be managed at every level of the Program Activity Architecture (PAA) (e.g. all programs down to the sub-sub activity level) and the results aggregated at the corporate level to facilitate priority setting and improve decision-making.

Integration is the act of bringing together plans, activities and processes so that they work in harmony with each other to achieve common business objectives. Alignment is the act of linking short and long-term objectives to the strategic outcomes and program activities of the department as defined in their PAA. Developing an integrated approach to planning can help reveal interdependencies and horizontal linkages of individual activities, opportunities to streamline work processes and operations, and potential for economies of scale. Aligning plans to the business objectives of the department can help ensure that resources can be effectively allocated to achieve strategic outcomes.

In examining best practices of departments with mature security programs, it has been observed that security is firmly integrated into the internal management functions and aligned with corporate planning and risk management activities. Security policies and SRM processes and plans are well documented, tailored to the unique business activities of the department, and include performance measurement as an integral component of planning. Integration and alignment is further supported through strong governance that uses Management Accountability Framework (MAF) elements[6] to establish expectations for good internal management practices and the departmental PAA as the framework for aligning internal management practices with program delivery outcomes.

An integrated approach to planning and risk management requires the active participation of senior managers and internal stakeholders from corporate and program areas. It is achieved through regular and recurring dialogue, a clear understanding of roles and responsibilities, and a commitment to improved planning and risk management practices at all levels within the department.

6. Documentation

Documenting security processes, policies, and plans is a means to establish a common understanding and frame of reference for security terminology, support internal and external communications, define roles and responsibilities, and build the maturity of security and SRM practices. Documenting the analysis and findings of SRM helps ensure that the results are reproducible and provides evidence of due diligence so that anyone, including managers and auditors, can understand the thinking that led to action being taken, and trace those actions to management decisions, plans, and policies.

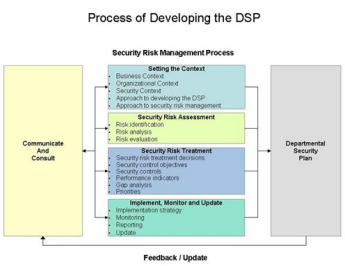
Documentation should be prepared throughout the process of security risk assessment and security risk treatment to capture the analysis, findings and resulting actions, and provide a basis for review, priority setting, decision-making, and performance measurement. This will help demonstrate the relationship from the selected controls back to the results of the security risk assessment and security risk treatment processes.

While the extent and format of documentation will differ from one department to another given each one's size, complexity, operations, and internal management practices, each department should take steps to establish and maintain evidence of the SRM process and findings that are legible, readily identifiable and retrievable[7]. Such documentation should also remain available to those who need it while respecting any policy, legal or regulatory requirements and contractual obligations to protect and control it. (See Section 8.3 - Departmental Security Plan for further detail on documentation).

7. Process of Developing a Departmental Security Plan

The guidance on developing a DSP is laid out according to the process depicted in Figure 2 *Process of Developing a Departmental Security Plan*. The process is a hybrid of various planning and risk management models that are described in reference documents used to develop this guideline (Appendix B - References). Each step in the SRM process has been mapped to the mandatory requirements related to the DSP as described in the PGS and DDSM to help ensure that these can be met.

Figure 1 - Process of Developing a Departmental Security Plan



[Text version: Figure 1 - Process of Developing a Departmental Security Plan]

7.1 Communicate and Consult

A consistent exchange of pertinent information should take place during all phases of developing the DSP. Communication and consultation demonstrates that stakeholders have been engaged and that their input and concerns have been addressed. It also demonstrates that authoritative sources have been referenced and considered.

It is important that individuals who are responsible for managing security risks are involved in the SRM process as this will help secure endorsement and support for the DSP when approval is sought. Individuals in all areas of the department can contribute significantly at various stages. They include:

- Program and business managers, corporate services, legal services, and regional offices can provide advice and insight into the business context, matters of strategic importance, legal obligations, internal management protocols and processes, and strategic planning and performance measurement. They can contribute to defining the criteria to be used for evaluating the significance of security risks and into the consequences that could result in the event of a compromise.
- Subject matter experts can help identify and characterize security vulnerabilities and threats to information, assets, services, and individuals and contribute to assessing, evaluating and treating security risks. These experts may include individuals well versed in access to information, privacy, corporate risk management, emergency and business continuity management, human resources, occupational health and safety, real property and materiel management, information management, information technology (IT) and finance.
- The DSO together with departmental security practitioners are best placed to provide advice and guidance regarding the threat environment, the overall security risk management process, and security risk treatment options. They can help determine the most appropriate tools to be used in assessing risks (e.g., Threat and Risk Assessments (TRAs), self assessments, other), interpret the results of these risk assessments and provide guidance on what priorities should be in the DSP. The DSO is also responsible for developing, implementing, monitoring and maintaining the DSP and for managing the departmental security program. As such, the DSO is likely to be the central point of coordination for departmental security planning and security risk management. Their responsibilities may include:
    - Defining the approach, resources and capabilities necessary to develop the DSP
    - Coordinating with stakeholders including program managers, departmental planners, subject matter experts, and other individuals involved in the development of the plan
    - Developing the plan including integrating the results of consultations, risk assessments, etc., and
    - Seeking guidance from the ADM champion and supporting executive committees.

Governance is a key element of the consultation as it provides structure and process to engage senior managers, formalize decision-making, and sustain momentum during the planning lifecycle. It may be useful to identify an executive level champion to initiate the development of the DSP and to be a conduit of information and decision-making with the departmental governance structure (i.e., within key departmental standing committees). Including the DSP as part of the management agenda is also a way to ensure that it is results-based and aligned with the business activities and priorities of the department.

All those involved in developing the DSP or conducting SRM should be familiar with key departmental documents that establish the mandate, program structure, priorities, and commitments of the department. Together these documents provide an integrated view of the business environment and will help orient and align the development and implementation of a DSP. They include:

- Instructions to Departments for Developing a Management, Resources and Results Structure
- Departmental Report on Plans and Priorities (RPP)
- Departmental Performance Report (DPR)
- Integrated Business and HR Plans
- Investment Plans
- Policy on Internal Audit, and
- Office of the Auditor General and internal audit reports.

7.2 Security Risk Management

Risk management is an integral component of good management, good planning, and decision-making at all levels. It is evident in virtually every public and private sector organization. SRM is a component of an overall risk management practice. It is an ongoing and iterative process of analyzing and coordinating of activities for controlling security risk. These include identifying and assessing security risks to essential resources (information, assets, individuals, and services) that a department depends on to deliver programs and achieve its business objectives, and implementing measures to reduce security risk to an acceptable level. SRM is important because it links departmental security to the broader management, business planning, and corporate risk management activities, can help build a stronger culture of security, and enable the department to identify and deal with security issues proactively.

Security risks that are not mitigated can impact a department at any level. At the corporate level, they may impede the department from achieving its strategic outcomes. At the program level they may impact the achievement of expected results or service delivery imperatives. At the operational level, they may compromise the confidentially, availability or integrity of departmental information and assets, or expose individuals to workplace violence. SRM should be logically and practically connected to all levels of program activity in order to develop a holistic view of departmental security both in terms of how it enables or impedes the achievement of business objectives. Figure 2 - *Integrated Security Risk Management* illustrates the relationship between departmental, program, and operational activities and security risks to help frame the SRM process.

The SRM process described in the remainder of the guideline deals with initial risk, that is, risk before it has been mitigated. This approach has been taken to help ensure that all risks, including residual risk (i.e. risk after treatment) are identified and documented. In this way, departments will be able to successfully develop an integrated view of all security risks to the department and determine treatment options in consideration of overarching business and legal obligations.

Figure 2 - Integrated Security Risk Management[8]

[Text version: Figure 2 - Integrated Security Risk Management]

7.2.1 Setting the context

The DSO ... is responsible for developing, implementing, monitoring and maintaining a departmental security plan (DSP) that ... provides an integrated view of departmental security requirements.

Directive on Departmental Security Management 6.1.1.1

Setting the context is the first activity of the planning cycle. It is an important aspect of planning as it will allow the department to gain insight into its strengths and weaknesses as well as opportunities and threats posed by the environment within which the department operates. Context analysis focuses mainly on the macro environment both internal and external to the organization. This analysis will help to determine how security interacts with internal operations of the department in order to articulate the role that security plays in enabling the department to achieve its goals as well as helping to identify the parameters and constraints within which security risks should be managed.

The departmental business objectives are the most important driver of the DSP and for the subsequent steps in the SRM process. They are the basis of arguments that may be used to develop any business case for change, will help prioritize initiatives based on business requirements, and establish a common basis for consultations and managing the expectations of partners and stakeholders.

Business Context

Defining the business context should begin with a review of the department's mandate, priorities, strategic outcomes, program activities, and program sub-activities. The departmental PAA, RPP and DPR are useful sources for gathering this information and will help orient and align the development and implementation of a DSP. The PAA in particular provides a structured inventory of all departmental programs[9] and depicts them according to their logical relationships to each other and the strategic outcome(s) to which they contribute. The RPP will be useful for defining the legal and policy framework and obligations. Opportunities to use available information and create linkages with specialists in corporate risk management and departmental planning should be explored as this type of analysis is something typically undertaken by those areas.

The business context can also be used as the basis for identifying the information, assets, individuals and services associated with the program activities and sub-activities, and for describing how their protection enables the department to achieve its mission. This will help structure and scope risk assessments to ensure they are associated with the context of the department's overarching mandate and later in the process, can aid in determining priorities for treating security risks.

Organizational Context

An analysis of the organizational context involves examining the internal workings of the department to identify how individuals and groups operate in order to achieve business outcomes. It considers factors such as the number of employees, location of facilities, management practices and authorities, core competencies (knowledge and skills), technologies, and administrative processes. This analysis will help to define the department's policies, operations, and the strategies that are in place to

achieve business objectives, and will provide insight to the capabilities, limitations, perceptions and values of internal stakeholders.

Organizational contexts will vary significantly between departments depending on the size and complexity of the business. Some departments have only a few business lines that are performed in a single office location and supported by streamlined processes. Other departments are characterized by numerous program activities and sub-activities that involve thousands of people located across the world, are supported by complex processes and decision making authorities, and involve a broad range of skills and competencies.

Security Context

The security context provides an overview of the departmental security function and its operations including the constraints and requirements derived from legal, regulatory, policy, contractual, and other obligations. It also explains the threat environment within which security activities are conducted.

An analysis of the security context should consider the relationship between the departmental security and other internal management practices as defined in the organizational context, in order to explain how these activities work in concert to protect departmental resources[10] and support the business of the department. All departments are exposed to a certain level of security threat. For example, the threat of malicious attacks on IT systems is relevant to all departments. However, a limited number of departments are more susceptible to internal espionage or sabotage. These threat characteristics also define and influence the departmental security function.

Approach to developing the DSP

The approach to developing the DSP will vary depending on the business, organizational and security contexts of each department. Some departments will choose to develop a single DSP that details all of the key elements described in this guideline. Larger or more complex departments are more likely to develop a DSP that is supported by detailed plans and risk assessments covering identified regions, programs, services, activities or systems.

The approach defined by each department will help scope and establish a framework for organizing the DSP. It should consider the process for developing the plan, the timelines required to develop the DSP, and how the DSP links to or consolidates other plans and risk assessment to provide a complete and coherent view of departmental security requirements. Defining these linkages will also help ensure that the findings and priorities proposed in the DSP can be traced and linked to more detailed findings in a particular plan or assessment where the analysis of risk assessments and treatment options are documented.

Approach to security risk management

SRM occurs within the business, operational and security context of the department and government in general. Defining the departmental approach to SRM forms the basis for communicating the philosophy, values and practices with respect to security management, and defining the criteria for evaluating security risks and making decisions to treat them. Each department is likely to have a somewhat different approach based on corporate risk management practices, the maturity of the security program, security risk exposure and risk tolerance. The SRM process should also identify the authorities responsible for selecting risk treatment options and accepting the residual risks. Typically, the manager responsible for the program, service activity or system would be the responsible authority.

In defining the department's SRM approach, it may be helpful to consider:

- How are the linkages between SRM and the departments' business objectives and policies determined?
- How are decisions made regarding how risk assessments are conducted as it pertains to the methodologies used, processes followed, and timing for conducting or reviewing risk assessments?
- What is the risk criterion by which the significance of risk is defined and assessed to determine whether it is acceptable or unacceptable?
- Who are the responsible authorities for making decisions regarding the treatment of security risks (i.e. corporate security, risk/business owners, senior managers, etc.)?
- How are the results of risk assessments and risk treatments documented for evidentiary purposes?
- How will the results of risk assessments and risk treatment decisions be combined and summarized in the DSP?
- How are SRM activities monitored, evaluated, and reported?

Defining criteria for evaluating the significance of security risks is an essential element of the SRM process. The criteria should reflect the department's values, business context and objectives, and resources. Some criteria may be imposed by or derived from legal or policy requirements. Decision-making regarding the treatment of security risks often requires weighing multiple criteria to decide on a course of action based upon the degree to which the security risk may impede the achievement of business objectives. Since it can be complex, there is no one decision criterion that must be or is always used. Several criteria recur with some frequency. They include cost-benefit, cost effectiveness, level of risk tolerance, views of stakeholders, and consideration of multiple risks. The use of risk criteria will be important at the risk evaluation stage in order to decide if risks are acceptable or unacceptable and how they should be treated.

7.2.2 Security risk assessment

.. a departmental security plan (DSP) that...identifies security threats, risks and vulnerabilities to determine an appropriate set of control objectives

Directive on Departmental Security Management 6.1.1.2

Security risk assessment is the process of identifying, analyzing, and evaluating security risks to determine the significance of the risk and determine whether the risk is acceptable or not and requires treatment. Security risk assessments should be conducted in a methodical and systematic way and may be conducted at any time independent of the overall SRM process. They should be repeated periodically to address any significant changes in the security environment or when a new service or business practice is introduced.

Security risk assessments are typically conducted on IT systems, critical assets and facilities. In order to provide a consolidated view of security risks, risk assessments should also be conducted at the program activity level and consider other factors such as business processes. Deciding how to organize and approach security risk assessment is something each department will need to decide based on their unique operations and program activities. What should remain paramount is that scope and purpose of the risk assessment is aligned with the business objectives of the department so that the results of each risk assessment can be combined to provide an integrated view of security risks to the department and support informed decision-making at a corporate level.

Consideration should be given to the scope of each risk assessment to ensure that it documents at a sufficient level of detail what is at risk (e.g. information, assets, services, individuals, programs) and how it fits into the PAA of the department. The analysis that leads to conclusions should also be documented so that it can be referenced and re-evaluated if necessary. Since it is likely that multiple risk assessments will be conducted and aggregated to provide a department-wide view, consideration should also be given to describing the linkages between risk assessments and how the results can be documented in a way that allows details to be elaborated on and compared.

Security risk assessments do not always need to be a major undertaking and there is no "one size fits all approach. Each risk assessment should be conducted with full consideration of the need to justify the resources used to carry them out. Various tools and methodologies are commonly used and they vary considerably in complexity, objectivity and subjectivity, the quality of results they yield, along with the relative level of expertise required to use or conduct them. Some commonly used methodologies include: TRAs, audits, Business Impact Analysis (BIA), Privacy Impact Assessments (PIA), self-assessments, monitoring, security investigations, and vulnerability assessments. As some of these will generate the same or similar risk information, departments should endeavour to avoid duplication by requiring that these activities be coordinated and that the information garnered from them be shared (in accordance with laws and policies dealing with the collection, use, disclosure and retention of information). Opportunities to collaborate or use risk assessments produced by other areas (e.g. IT services, corporate risk management) should also be explored.

Departmental level security risk assessments are generally very broad in scope and concentrate on strategic risks related to program activities and their related resources and services. Although they lack the detail of more focused risk assessment that may be devoted to a single facility, network or system, departmental assessments establish a broad contextual framework and a solid foundation for the security program, and will help identify the need for additional program and system level risk assessments and/or prioritize individual risk assessment projects.

Risk assessments for programs or resources that do not represent any specific risk to the organization can be combined, conducted without requiring significant or specialized resources, and documented in a concise manner. Risk assessments of programs or resources that have similar operating environments and security concerns can in many cases be conducted using "generic" risk assessments that can be reused. Programs or resources that are considered at higher risk or higher value will warrant more rigorous and in-depth analysis that are supported by sophisticated methodologies. Conversely, less effort need be expended on the examination of lower value assets, less significant threats and more obscure vulnerabilities.[11]

Risk identification

Identifying security risk is a multifaceted exercise. It involves the identification of risk sources (as a function of threats and vulnerabilities) and their potential consequences. The aim of risk identification is to generate a comprehensive list of security risks that impact departmental resources[12], thereby affecting the achievement of business objectives. Developing a comprehensive inventory of risks (initial risk) is important because risks that are not identified will not be included in further analysis. Identification should include risks whether or not their source is under the control of the organization, even when the risk source or cause may not be evident or the risk may currently be adequately mitigated. An example of risks that are not under the control of the organization might be malicious attacks on information systems resulting in denial of services.

Security threats typically fall into three categories: deliberate, accidental or natural hazard. They may be generic or specific and require analysis on a case-by-case basis. Relevant and up-to-date information is important in identifying risk sources. Some methods to consider in defining risk sources include brainstorming, acquiring threat and vulnerability information from lead security agencies (LSAs) or other sources, and consulting with people who have appropriate knowledge such as corporate risk managers, program and system owners, and other stakeholders.

Some examples of security risks common to most departments include:

- Financial and non-financial losses resulting from theft, destruction or vandalism of physical assets
- Fraud, network damage, disclosure, misuse resulting from insider threats
- Harm to employees or their families whose jobs expose them to increased risk of workplace violence (e.g. contact with the public, exposure to volatile or unstable people, guarding valuable assets, etc.)
- Interruption to service delivery due to loss or unavailability of human resources (e.g. affected by pandemic flu, extreme weather conditions, natural disasters)
- Compromise of sensitive information or assets shared with business partners or service providers due to inadequate application of security controls
- Financial and reputation costs related to data breaches or loss of information integrity
- Interruption to critical service delivery due to natural disaster or cyber attack affecting critical infrastructure or communications

Given that this is not an exhaustive list each department should take steps to identify risks that may be unique to their own business and operating environment.

Risk analysis

The purpose of risk analysis is to assess the likelihood and impact of security risks that could affect the achievement of strategic and business outcomes. It involves understanding the nature and severity of the risk and provides the information and analysis necessary to decide whether or not risks need to be treated, and on the most appropriate risk treatment approach. The analysis process is typically supported by the use of various models and tools and can be conducted at varying levels of

detail depending on the risk and the information available. Tools may use qualitative or quantitative approaches, or a combination of both.

Following are examples of qualitative matrices that can be adapted by departments to aid in the analysis process. These examples demonstrate a simple way of assessing impact and likelihood to help assess the severity of the risk. They can be expanded by adding rows or columns and customizing descriptions to the department's decision making criteria. These examples do not advocate a particular dimension and departments are encouraged to adapt such matrices to be consistent with other internal risk analysis practices (i.e. those used by corporate risk management). This will help compare and assess risks using a common tool and point of reference.

Examples of Qualitative Risk Analysis Matrices

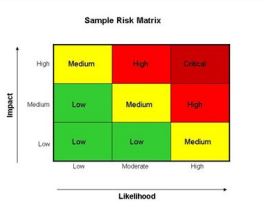
Impact

Level	Description
High	Major losses; ongoing disruption to service delivery, major impact on government reputation or the health and well being of Canadians; temporary or permanent loss of critical infrastructure
Medium	Some ongoing disruption to service delivery; medium impact on well being of Canadians
Low	Minor disruption to service delivery; low impact on well being of Canadians

Likelihood

Level	Description
High	Will probably occur in most circumstances
Medium	Might occur at some time
Low	May occur only in exceptional circumstances

Figure 3 - Sample Risk Matrix



Text version: Figure 3 - Sample Risk Matrix

Risk Evaluation

Risk evaluation is the process of determining whether the risks are acceptable or unacceptable and need treatment. These decisions should be guided by established risk criteria and be made by the person(s) with the appropriate authority. Decisions should also take into account the context of the risk, the tolerance of the department, risk owners and other stakeholders that may be impacted by the risk.

If the level of risk is determined to be acceptable, it may be accepted with no further treatment. Risks that are determined to be acceptable should still be documented, monitored and periodically reviewed to ensure they remain acceptable.

If the level of risk is determined as unacceptable, options for treating the risk should be identified. These may include reducing the risk, avoiding the risk, or transferring the risk.

Risk reduction may be achieved by implementing controls to effectively reduce or eliminate the risk. Controls that most effectively reduce risk at a reasonable cost to the department are the controls that are most likely to be recommended for implementation.

Risk avoidance may be achieved by not undertaking any activity that is likely to trigger the risk. It may not always be a practical option but can form an important part of the overall consideration of how to manage the risk and may form part of the treatment option.

Transferring risk may be achieved by moving the responsibility to another party or sharing the risk through a contract, partnership, or joint venture. Note that new risks may arise from transferring the risk if it is not adequately managed by the party to whom the risk is transferred.

Some risk evaluations can lead to decisions to undertake further analysis. The evaluation, along with the reasons or rationale for arriving at the decision, should be documented to provide a record of the thinking that led to the decision as it will provide useful context for future risk assessments.

7.2.3 Security risk treatment

... identifies and establishes minimum and additional controls when necessary to meet control objectives and achieve an acceptable level of residual risk

Directive on Departmental Security Management 6.1.1.3

Decisions on how to treat security risks are management's prerogative. The criteria defined as part of the department's approach to SRM along with legal, policy, or regulations by which the department is bound, will serve to guide decision-making. The willingness of the department to accept or manage risk will also be a factor in decision making. The risk remaining after security controls have been applied or a decision has been made to accept the risk is known as residual risk.

Security Risk Treatment Decision

For each security risk, the DSP should record the decision regarding the selection of risk treatment option (e.g. reduce, avoid, transfer). Security risks for which the selected treatment option is to avoid or transfer should detail the mechanisms that will be used to adequately manage the risk and ensure on-going monitoring.

Security Control objectives

Security control objectives are the desired result or purpose to be achieved by treating security risks. They serve to guide the selection of controls to treat the risk along with the determination of performance indicators to measure the achievement of the objective.

Security control objectives should be defined for each security risk that is evaluated as unacceptable and for which the selected treatment option is to reduce the risk. The control objectives form the basis for measuring the effectiveness of controls at managing security risks.

Security Controls

Security controls are those administrative, operational, technical, physical or legal measures applied to manage and reduce security risk to an acceptable level. They should be selected and implemented for each risk for which a control objective has been determined. Controls may be categorized as common government-wide controls or department-specific.

Common government-wide controls are defined in Appendix C of the DDSM and apply to all aspects of departmental security. These controls are related to activities that include:

- Information Assurance
- Security Screening of Individuals
- Physical Security
- IT Security
- Security in Contracting
- Sharing Information and assets with other organizations or departments
- Obtaining Security Services from other organizations
- Security awareness
- Security Training
- Security incident management
- Protection of employees from workplace violence
- Security inspections
- Administrative investigations related to security incidents
- Security in emergency and increased threat situations
- Business continuity planning

Department-specific controls are defined by the department based upon their business objectives. As such they are likely to be unique to each department. While they may be articulated at a very high level in the DSP, they provide a framework for identifying more specific controls unique to the department. This will typically be necessary for departments that need to achieve a greater level of security based upon their particular operations or other constraints. An example of a department-specific control might be "protective measures to safeguard employees outside of the work environment due to the increased security risks to which they are exposed. When defining controls unique to the department, it is important to keep in mind the impact that applied controls could have on other government departments.

The selection of controls should be aimed at achieving the control objectives identified in the previous step. It should involve balancing the costs and efforts of treating the risk against the benefits to be derived and compliance requirements. Any opportunity to minimize resource requirements while maximizing benefits to the department should be considered.

The PGS, DDSM and associated standards identify security controls that are intended to maintain a general operating environment that is suitable to most programs, services, activities or systems. Depending on the nature and level of risk to be treated, departments may choose to apply additional controls to address their unique or heightened requirements. Security controls may also be found in various guidelines produced by lead security agencies (LSA) based on their area of expertise. These include: Royal Canadian Mounted Police (RCMP) for physical security, Communications Security Establishment Canada (CSEC) for information technology security, Public Works and Government Services Canada (PWGSC) for contract security, Public Safety Canada for emergency management and business continuity planning, and Treasury Board Secretariat (TBS) and Canadian Security and Intelligence Service (CSIS) for security screening of individuals.

Performance Indicators

Performance indicators are the basis for assessing the effectiveness of controls at achieving control objectives. Through the systematic and ongoing process of collecting and analyzing performance indicators, departments can assess and report on how well controls are doing at achieving intended results.

A performance indicator can be quantitative or qualitative. Quantitative performance indicators are composed of a number and a unit. The number indicates the magnitude (how much) and the unit gives the number its meaning (what), e.g. the number of documented cases of theft. In contrast, qualitative indicators are more subjective or relative, e.g. assessment of the quality of

an investigation. As much as possible, qualitative indicators should be summarized into a rating scale, e.g. research quality is rated as "excellent," "average," or "below average."[13]

A minimum of one and maximum of three performance indicators should be identified for each control to help ensure that the amount of information to be tracked, collected and maintained remains manageable. When selecting or developing performance indicators, it is important to consider:

- Will the performance indicator clearly demonstrate and appropriately reflect the achievement of control objectives?
- Are the performance indicators simple and easy to measure?
- Is it possible to use information that is already available in the department, other departments, statistical agencies, international organizations, etc.?
- Can the performance indicators be tracked and compared over time to allow for year-to-year comparisons?
- How difficult or expensive will it be to capture the information?

For each performance indicator, it is important to identify:

- Sources of data or information to be captured, created, or available on a regular basis
- Frequency at which the data will be collected and evaluated (e.g. annually, biannually, monthly), and
- Targets (or level of success) to be achieved within a specified time.

The TBS document entitled *Instructions to Departments on Developing a Management Resources and Results Structure* provides good guidance on developing performance indicators and can be referenced for further information. While security performance indicators are unlikely to be added to the departmental PMF as this level of detail is usually not captured as part of the PAA, it may be useful for achieving consistency.

Gap Analysis

The purpose of assessing gaps is to identify security control objectives that remain unmet, for which controls need to be implemented, improved, or otherwise adjusted, and/or for which performance indicators have not yet been established. It will help confirm which risks are already being managed to an acceptable level. For each identified risk that has been determined to be unacceptable and for which a control objective(s) has been identified, a gap analysis should seek to determine:

- Are controls currently in place to achieve the control objective and manage security risks?
- Are the controls effectively managing the risk and achieving the control objectives (as demonstrated by the performance indicators)?
- Are the performance indicators sufficient / appropriate for measuring the effectiveness of the control?

The results of a gap analysis form the basis for establishing a list of relative priorities for implementing additional controls and establishing performance indicators. They may also indicate where controls may be deemed excessive and should be reduced, eliminated or otherwise replaced.

Priorities

Priorities should focus on broad areas that are critical to the success of the department or to ensure compliance with legal and policy obligations. A determination of priorities should be confirmed against known and stated departmental priorities and it may be helpful to consult with other internal stakeholders to determine opportunities for alignment or collaboration. As there are always many more issues vying for attention than there are resources to address them, it may be helpful to consider:

- Is the security priority linked to departmental priorities and strategic outcomes?
- Does this priority address compliance requirements defined in policy, legislation, contractual or other obligations?
- How does this priority relate to government priorities?
- What are the availability or limitations of departmental or government resources?
- Does this priority address stakeholder expectations or possible negative consequences to reputation?
- Have opportunities to collaborate with, or consolidate priorities with other departmental plans and initiatives been considered?
- What is the residual risk that will remain if the risk remains untreated and how will it be addressed?

7.2.4 Implement, monitor and update

... outlines security strategies, objectives, priorities and timelines for improving the department's security posture

Directive on Departmental Security Management 6.1.1.4

The final stage in the SRM process involves elaborating a strategy to implement security controls and performance indicators, monitor progress, and report on results achieved. An implementation strategy is a means to manage process and resources, focus on the achievement of desired outcomes, and strengthen partnerships with departmental stakeholders, and focus on assessing the achievement of outcomes. The details of implementation are what is typically captured in work plans and project plans.

Implementation Strategy

An implementation strategy details activities and assigns responsibility to specific individuals for accomplishing those activities. It also establishes timelines, estimates resource requirements, and describes how progress will be assessed and monitored. Consultation remains important in developing an implementation strategy as it affords a means to align goals, timelines, and resource requirement with other departmental plans.

A typical implementation strategy will identify:

- short term (one - two years) and long term (three - five years) goals for implementing security controls and performance indicators, in line with established priorities
- activities, roles and responsibilities for implementing additional controls and establishing performance indicators (where each activity may in turn be translated into a number of specific work plans)
- timelines and milestones to sequence activities
- resources necessary to implement controls and monitor their effectiveness[14], and
- risks and controls that will remain during the transition period.

Monitoring

Monitoring entails gathering and analyzing information to gauge progress in implementing controls and establishing performance indicators, to ensure that planned activities and implementation of controls remain on schedule and within allocated resources. It also entails monitoring the effectiveness of the controls at achieving control objectives (using the performance indicators). Managers at all levels and security practitioners have a responsibility for monitoring the implementation and effectiveness of security controls and reporting accordingly to the DSO[15].

Monitoring can also include maintaining an awareness of the threat and operating environment so that emerging risks can be identified, assessed and managed on an ongoing basis. Regular consultation with stakeholders and risk owners should help in maintaining awareness of changes to the business of the department and periodic environmental scanning will aid in monitoring the threat environment. Consulting with risk owners is also an opportunity to inform them of progress, and seek decisions should any changes be required. As with previous steps, the results of monitoring should be documented for evidentiary purposes and used to facilitate reporting progress to senior management.

Consideration may be given to whether or not an independent review (audit) would be useful for evaluating the effectiveness of the SRM process and activities along with progress at implementing the DSP. Any such plan should be consulted internally, undertaken with the awareness of associated costs, and balanced with other departmental audit and evaluation priorities.

Reporting

Periodic reporting is useful for seeking management input or decisions to address emerging issues and an opportunity to demonstrate progress towards expected results. Reporting improves decision-making by assessing both successes and failures, monitoring the use of resources, and disseminating information on best practices and lessons learned. Departments should evaluate the effectiveness of their SRM processes on a periodic basis[16] to facilitate learning and continuous improvement.

Reporting should be based on reliable and accurate information to demonstrate that planned activities are achieving expected results effectively and efficiently. Providing that findings and decisions have been documented throughout the SRM process, and progress information gathered through monitoring activities is recorded, reporting need not be an arduous task.

Update

The DSP and supporting risk assessments should be updated and revised regularly or when circumstances change significantly.

7.3 Departmental Security Plan Template

Deputy heads ... approve the departmental security plan that details decisions for managing security risks and outlines strategies, goals, objectives, priorities and timelines for improving departmental security and supporting its implementation

Policy on Government Security, 6.1.3

A well-prepared plan demonstrates that managers have thought through the business of the organization, understand what they need to achieve to support that business, and how to accomplish it. The DSP formalizes the linkage between business objectives and the management of security risks to achieve those objectives. It supports the deputy head and senior managers in achieving management excellence by providing a means to identify and manage operational security risks proactively.

The DSP details decisions for managing security risks based on their relative priority, timelines for implementing additional controls to improve departmental security, and performance indicators to evaluate the achievement of results. While the management of all security risks are within scope of SRM, the DSP should concentrate on those risks that have the most potential to impact the department's ability to fulfill its mandate, significantly impact human or financial, resources, may prevent compliance with security requirements outlined in policy or legislation, or may result in disruption of critical services.

The DSP is a strategic document that provides the deputy head and senior managers with "an integrated view of security risks to the department. While it is understood that the format and structure of the document, along with any evidentiary documents may vary from one department to another, the following template is recommended to help ensure that elements of a DSP remain somewhat consistent from one department to another and reflect the results of SRM.

The DSP can also be used as the basis for developing annual work plans and project plans that support the implementation of department-wide security goals and objectives approved in the DSP.

The first three sections are intended to provide the reader with an introduction and orientation to the DSP itself. The remaining sections map to the SRM process and the requirements of the PGS and DDSM.

DSP Element	Description
Approval	• A statement from the DH (or equivalent), to endorse decisions regarding risk treatment and support the implementation of controls and performance indicators.
Executive Summary	• Non-technical synopsis of the DSP that highlights the main points, issues, and conclusions and contains enough information to familiarize the reader with what is discussed in the full plan.

Communications and Consultations	• Brief description of the governance structure and process associated with the development of the DSP (i.e. who was engaged and how, roles, responsibilities and authorities of key stakeholders) • Identification of individuals and organizations that were consulted and/or who participated in the development of the DSP • List of reference documents/authoritative sources that were consulted in the development of the DSP

Context	• Business context
	  ◦ A brief description of department's mandate, priorities, strategic outcomes, program activities and program sub-activities
	  ◦ An overview of departmental resources and services associated with these program activities and sub-activities
	• Organizational context
	  ◦ A brief description of the departmental organizational, geographical and governance structure
	  ◦ A brief description of internal policies, processes and operations in place to help the department achieve its business objectives
	• Security context
	  ◦ A general description of the role that security plays in enabling the department to achieve its mission and support government priorities
	  ◦ A brief description of security constraints and requirements derived from legal, regulatory, policy, contractual or other obligations
	  ◦ An overview of security threats that are specific to the organization's business and organizational context
	  ◦ May include a description of other factors or constraints that may impact security risk decisions
	  ◦ May include a description of the relationship between the departmental security and other internal management practices and program activities
	• Approach to developing the DSP
	  ◦ Description of the scope of the DSP (i.e. department-wide or pertaining to only a subset of the department or programs).
	  ◦ Description of the structure and organization of plans and security risk assessment that collectively provide a consolidated view of security risks to the department (e.g. for large departments where the DSP may actually consist of a set of plans)
	• Approach to SRM
	  ◦ Brief description of the department's approach to SRM (including description of alignment between the SRM process and the department's program activities)
	  ◦ Criteria for evaluating significance of security risks
	  ◦ Description of how the results of risk assessments and risk treatment considerations are documented to ensure traceability

	Note: parts of this section and the following section may be best summarized in a matrix

Security Risk Assessment	• Risk Identification
	  ◦ List of the key security risks to departmental resources and services (based upon risk assessments conducted)
	  ◦ Should include identification of risk owners and stakeholders
	• Risk Analysis
	  ◦ Identification of the likelihood and impact of security risks
	• Risk Evaluation
	  ◦ Identification of risks that have been deemed unacceptable (along with rationale)
	  ◦ Identification of risks that have been deemed acceptable and approach that will be used for monitoring and periodic review

Security Risk Treatment	• Security Risk Treatment Decision
	  ◦ Identification of selected risk treatment option for each risk
	• Security Control Objectives
	  ◦ Description of the control objectives for risks for which the selected treatment option is to apply controls
	• Security Controls
	  ◦ Description of security controls for achieving the control objectives
	  ◦ Controls may be categorized as either administrative, technical or physical, or as common to all departments or department-specific
	• Performance Indicators
	  ◦ Description of performance indicators for monitoring the effectiveness of security controls
	  ◦ For each performance indicator, identify the sources of data, frequency and targets
	• Gap Analysis
	  ◦ An identification of security control objectives that remain unmet and for which controls need to be implemented, improved, or otherwise adjusted, or for which performance indicators have not yet been established
	  ◦ May include identification of controls that are deemed excessive and will be eliminated
	• Priorities
	  ◦ A list of recommended priorities for implementing additional controls and establishing performance indicators

Implementation	• Implementation Strategy
	  ◦ A summary of short and long term goals for implementing security controls and performance indicators
	  ◦ Activities and roles and responsibilities
	  ◦ Timelines and milestones
	  ◦ Resources
	  ◦ Considerations for transition period
	• Monitoring and reporting
	  ◦ Description of approach for monitoring and reporting on:
	  ▪ Progress at implementing controls and performance indicators
	  ▪ Effectiveness of security controls at achieving control objectives (using the performance indicators)
	  ▪ Changes in the business, organizational and security environment
	  ▪ Effectiveness of SRM processes
	  ◦ Description of how residual risks will be monitored
	• Update
	  ◦ Description of process and timelines for updating the DSP

7.3.1 Evidentiary Documents

All security risks should be documented in evidentiary documents used to record the analysis and findings of each step in the SRM process. Together with appropriately documented polices and processes they establish a record of SRM activities for ongoing reference, review and decision-making and can be used to guide the day to day SRM activities. Evidentiary documents could include:

Security risk management process

- Establishes the department's approach to SRM and may include policy, procedural, and practical descriptions for assessing, evaluating, treating and monitoring security risks
- Establishes the department's criteria for deciding if security risks are acceptable or unacceptable (tools, methodologies, etc.)
- Explains relationship between DSP and evidentiary documents

Security environmental scan

- Analysis of the internal and external threat environment and assessment of the department's current risk exposure

Communication and consultation report

- Documents the approach to and/or results of consultations with internal and external stakeholders

Departmental Security Program documentation / policy

- Document(s) describing the departmental security program activities and management practices related to all aspects of departmental security.
- Describes governance, delegation, coordination and reporting mechanisms within the security program, and between the security program and other groups with security related responsibilities (e.g. emergency preparedness, occupational health and safety, IM, IT, regions, etc.), and security services provided by or to another party, such as a portfolio department or shared services provider

Security risk assessment reports

- Details the results of security risk assessments together with their analysis and decisions on how those risks are to be managed based on the establish SRM criteria
- This information may also be captured in a Security Risk Register (SRR) (see below)

Security risk treatment reports

- Detailed analysis and decisions related to the selection of risk treatment options, the identification of control objectives, the selection of controls and performance indicators, the conduct of gap analysis and the establishment of priorities
- This information may also be captured in a SRR (see below)

Security Performance Measurement Framework

- Describes roles and responsibilities, tools, methods, processes, and frequency for evaluating the performance of the security program, assessing the effectiveness of SRM practices, assessing effectiveness of controls at achieving control objectives, and reporting to senior management

Annual Work Plans and Project Plans

- Describes focussed activities and assignments that support the implementation of priorities approved in the DSP along with activities related to the administration of the departmental security program.

7.3.2 Security Risk Register

A risk register is a tool commonly used by many corporate risk managers and by some security organizations to document the results of risk management. A SRR is used to record the results of SRM. This type of tool may be referred to as a corporate risk register (CRR), secuard, or security risk log. A SRR can be used to record the same information as may otherwise be documented in some of the evidentiary documents described above (policy type documents excepted) A comprehensive SRR would capture the details of risks that have been identified, together with their analysis and plans for how those risks are to be treated. One of the advantages of a SRR is that it provides a means to consolidate and synthesize a great deal of information in a relevant, consistent, and concise manner, and allows for comparisons across multiple programs to support decision-making.

A SRR can be maintained as a simple document in a word-processing or spreadsheet format, or can be developed as database. An example of a SRR in the form of a table is shown in Appendix C - Sample Security Risk Register.

Evidentiary documents and the SRR should be updated on a routine basis, including instances where emerging information or issues would make it appropriate, there are changes or adjustments in the business or security exposure of the department, or updates to the departmental PAA.

8. Enquiries

For enquiries regarding this policy instrument, please contact the Security and Identity Management Division.

Appendix A — Definitions

Availability (*disponibilité*)
The state of being accessible and usable in a timely and reliable manner
Compromise (*compromission*)
The unauthorized access to, disclosure, destruction, removal, modification, use or interruption of assets or information
Confidentiality (*confidentialité*)
A characteristic applied to information to signify that it can only be disclosed to authorized individuals to prevent injury to national or other interests
Control objective (*Objectif de contrôle*)
A statements of desired results or purposes to be achieved by implementing y controls (adapted from COBIT)
Department (*ministère*)
All departments named in Schedule I, divisions or branches of the federal public administration set out in column I of Schedule I.1, corporations named in Schedule II, and portions of the federal public administration named in schedules IV and V of the *Financial Administration Act (FAA),* unless excluded by specific acts, regulations or Orders in Council
Executive (*cadre supérieure*)
An employee appointed to the executive group (EX-01 to EX-05 levels), i.e., director, director general, assistant deputy minister or equivalent
Integrated risk management (*Gestion intégrée des risques*)
A continuous, proactive and systematic process to understand, manage and communicate risk from an organization-wide perspective to support strategic decision making that contributes to the achievement of an organization's overall corporate objectives (adapted from IRMF)
Integrity (*intégrité*)
The state of being accurate, complete, authentic and intact
Interoperability (*interopérabilité*)
The ability of federal government departments to operate synergistically through consistent security and identity management practices
Managers at all levels (*gestionnaires à tous les niveaux*)
Includes supervisors, managers and executives
Privacy impact assessment (PIA) (*Évaluation des facteurs relatifs à la vie privée (EFVP)*)
A policy process for identifying, assessing and mitigating privacy risks. Government institutions are to develop and maintain privacy impact assessments for all new or modified programs and activities that involve the use of personal information for an administrative purpose (from Policy on Privacy Protection)
Program Activity Architecture (PAA) (*Architecture des activités de programmes (AAP)*)
An inventory of all the programs and activities undertaken by a department or agency. The programs and activities are depicted in their logical relationship to each other and to the strategic outcome(s) to which they contribute. The PAA is the initial document for the establishment of a Management, Resources, and Results Structure (MRRS)
Residual Risk (*risque résiduel*)
Level of risk remaining after security measures (controls) have been applied
Risk (*risque*)
The uncertainty that can create exposure to undesired future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to impede the achievement of an organization's objectives
Risk criteria(*Critères de risque*)
Terms of reference by which the significance of risk is defined and assessed by a department to determine whether it is acceptable or unacceptable (NEW)
Risk management (*Gestion des risques*)
A systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk issues (FROM IRMF)
Security control (*mesure de sécurité*)
An administrative, operational, technical, physical or legal measure for managing security risk. This term is synonymous with safeguard
Security program (*programme de sécurité*)
A group of security-related resource inputs and activities that are managed to address a specific need or needs and to achieve intended results
Security risk (*Risque pour la sécurité*)
An expression of the likelihood and impact of events with the potential to cause injury to information, assets, individuals or services (NEW)
Security risk management (*Gestion des risques pour la sécurité*)
a component of an overall risk management process involving the organization and coordination of activities and processes for controlling security risk (MITS)
Security risk register (*Registre des risques pour la sécurité*)
A consolidated record of identified security risks resulting from a risk assessment that provides a summary of their analysis and treatment decisions. The consolidation may be at a corporate, branch, regional or program level. This term is synonymous with "security risk log, "security risk scorecard" or "security risk inventory as defined by departmental risk management practices.(NEW)
Strategic Outcome (*Résultat stratégique*)
A long-term and enduring benefit to Canadians that stems from a department or agency's mandate and vision. It represents the difference a department or agency intends to make for Canadians and should be measurable and within the department's sphere of influence (MRRS)
Sub Activity (*Sous-activité*)
A group of related activities below the Program Activity level (second level of the PAA structure) (MRRS)
Sub-Sub Activity (*Sous-sous-activité*)
A group of related activities below the Sub-Activity (third level of the PAA structure) (MRRS)
Threat (*menace*)
An event or act, deliberate or accidental, that could cause injury to information, assets or individuals.
Vulnerability (*vulnérabilité*)
An inadequacy related to security that could increase susceptibility to compromise or injury.
Workplace violence (*violence dans le lieu de travail*)
An action, conduct, threat or gesture that can reasonably be expected to cause harm, injury or illness to an employee in the workplace

Appendix B — References

Federal Government

- Annual Reports to the Prime Minister on the Public Service of Canada
- Auditor General Reports and Publications
- Directive on Departmental Security Management (DDSM)
- Departmental Performance Reports (DPRs)
- Harmonized Threat and Risk Assessment Methodology
- Integrated Planning Guide
- Framework for the Management of Risk
- Instructions to Departments for Developing a Management, Resources and Results Structure
- Management Accountability Framework
- Policy on Government Security (PGS)
- Policy on Management Resources and Results Structures (MRRS)
- *Public Service Modernization Act (PSMA)*
- Reports on Plans and Priorities (RPP)
- Treasury Board Policy Frameworks
- Treasury Board Policy Suite
- Whole-of-Government Framework

Provincial Government

- Results Oriented Government A Guide to Strategic Planning and Performance Measurement in the Alberta Government
- Government of British Columbia - Enterprise Risk Management (ERM) Guideline (PDF 850 KB)

Other Government

- Australian National Audit Office - Security Risk Management (report number 44, conducted 2008-09)
- Department of Homeland Security - National Infrastructure Protection Plan - Partnering to Enhance Protection and Resiliency (PDF 4.54 MB)
- UK National Risk Register
- NIST Special Publication 800-18 - Guide for Developing Security Plans for Federal Information Systems
- NIST Special Publication 800-30 - Risk Management Guide for Information Technology Systems
- NIST Special Publication 800-37 - Guide for Applying the Risk Management Framework to Federal Information Systems - A Security Lifecycle Approach (Final Draft 2009)
- NIST Special Publication 800-39 - Managing Risk from Information Systems

International References

- ISO 31000:2009 (Final Draft) - Risk management - Principles and guidelines
- ISO/IEC 27001:2005 - Information technology - Security techniques - Information security management systems - Requirements
- ISO/IEC 27002:2005 - Information technology - Security techniques - Code of practice for information security management

Appendix C — Sample Security Risk Register

Scope: (department-level or identification of programs or resources covered by the risk assessment / risk register)

					Risk Assessment			Risk Treatment						Implementation			Monitoring			
Risk identifier (unique ID)	**Risk Statement**	**Alignment with PAA**	**Risk owner / Authority for approving risk treatment**	**Stakeholders**	**Risk Identification**	**Risk analysis**	**Risk evaluation**	**Risk Treatment Decision**	**Control Objective(s)**	**Control(s)**	**Performance Indicator**	**Gap Analysis**	**Priority**	**Timelines / Milestones**	**Resource allocation**	**Transition**	**Data source(s)**	**Frequency**	**Target**	**Report / Update**
A unique identifier for risk. The reference can be useful for cross referencing the SRR to other risk registers, logs or CRP	Brief description of the resources affected, the value of the resource to the department, and the impact to the business should the risk materialize Structured sentence that conveys clearly both elements of risk (likelihood and impact) to the business or resources of the department in the current environment	Specify PA, PSA, or PSSA impacted by the risk	Name(s) or title(s) individual responsible for managing risk.	Name(s) or title(s) or organization(s) affected by risk.	Risk source (e.g. internal or external); potential consequence (e.g. compromise of confidentiality, integrity, availability; safety of individuals; lack of compliance); root cause (e.g. fundamental condition causing risk / vulnerability). In cases where a risk is solely routed in legislation, policy, regulation or contractual obligation, it may be identified as a "compliance risk, with a pointer to the applicable legislation, policy, regulation or contract.	Likelihood and impact of risk (based on risk assessment methodology, should include an overall risk rating, e.g. High, Medium, Low)	Identification if risk is acceptable or unacceptable and rationale for decision	Decision regarding treatment of unacceptable risks (i.e. avoid, reduce, transfer)	Statement of intent with respect to addressing the identified risk. In some cases, more than one control objective may be established for a given risk.	Description of security control(s) selected to achieve the stated control objective(s). More than one control may be necessary to achieve a given control objective.	Qualitative or quantitative means of measuring how well control is achieving control objective (minimum 1 - maximum 3)	Identification of controls that have not yet been implemented, require improvement, or for which performance indicators have not been established.	Priority for implementing additional control and performance indicators (based on analysis of cost, benefit, alignment with departmental priorities, etc.)	Timelines for establishing, implementing, or improving existing controls or establishing performance indicators (including sequencing of activities, dependencies, or other alignment considerations if applicable, and the date for achieving specified objectives).	Management resources for implementing controls and monitoring effectiveness	Risks and controls that will remain in place during transition, including: compensatory controls that need to be implemented in the period prior to full implementation of the selected	Source from which performance data will be captured, created, or available on a regular basis.	The frequency with which performance data will be collected for reporting on progress (e.g. annually, biannually).	Level of performance the department aims to achieve within a specified timeframe. Targets should be quantifiable	Additional descriptive information that may be useful including: • references to other plans or documents where source information or additional details can be found (e.g. detailed risk assessments, corporate risk profile, etc.)controls • cascading commitments in Performance Management Agreements, work plans, etc.

Footnotes

Footnote ftn1

The requirements to develop a DSP applies to deputy heads of all departments within the meaning of Schedules I, I.1, II, IV and V of the *Financial Administration Act* (FAA), unless excluded by specific acts, regulations or Orders in Council, as specified in section 2 of the Policy on Government Security.

Return to footnote [1] referrer

Footnote ftn2

Directive on Departmental Security Management, section 1.2, Treasury Board Secretariat

Return to footnote [2] referrer

Footnote ftn3

Policy on Government Security, section 3.5, Treasury Board Secretariat

Return to footnote [3] referrer

Footnote ftn4

Seventeenth Annual Report to the Prime Minister on the Public Service of Canada

Return to footnote [4] referrer

Footnote ftn5

Integrated Risk Management Framework, Treasury Board Secretariat

Return to footnote [5] referrer

Footnote ftn6

Management Accountability Framework is structured around ten key elements that collectively define "management" and establish the expectations for good management of a department or agency

Return to footnote [6] referrer

Footnote ftn7

ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems - Requirements, section 4.3

Return to footnote [7] referrer

Footnote ftn8

Adapted from NIST Special Publication 800-39, Integrated Enterprise-Wide Risk Management: Organization, Mission, and Information System View (projected for publication in 2010).

Return to footnote [8] referrer

Footnote ftn9

Policy on Management, Resources and Results Structures

Return to footnote [9] referrer

Footnote ftn10

Resources refers to information, assets, services and individuals that departments rely upon to achieve their overall mission

Return to footnote [10] referrer

Footnote ftn11

Harmonized Threat and Risk Assessment Methodology, October 23, 2007, issued under the authority of the Chief, Communications Security Establishment (CSE) and the Commissioner, Royal Canadian Mounted Police (RCMP)

Return to footnote [11] referrer

Footnote ftn12

Resources refers to information, assets, services and individuals that departments rely upon to achieve their overall mission

Return to footnote [12] referrer

Footnote ftn13

Instructions to Departments for Developing a Management, Resources and Results Structure, section 7.2.3, Treasury Board Secretariat

Return to footnote [13] referrer

Footnote ftn14

The *DSP* only identifies resources at a high level, to enable decision making and prioritization. More details on projects, resources and timelines for implementing security controls and monitoring their effectiveness would be contained in the work plans.

Return to footnote [14] referrer

Footnote ftn15

Directive on Departmental Security Management, Treasury Board Secretariat

Return to footnote [15] referrer

Footnote ftn16

Integrated Risk Management Framework, Treasury Board Secretariat

Return to footnote [16] referrer