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

Guide to the Audit of Security

March 2004

Canada

Acknowledgements

The Security Audit Guide Development Committee would like to specifically acknowledge and thank the following federal departments and agencies for their contribution of materials, information, and expertise in the preparation of this guide:

- Public Works and Government Services Canada
- Health Canada
- Royal Canadian Mounted Police
- Consulting and Audit Canada
- Communications Security Establishment
- Office of the Auditor General of Canada
- National Research Council Canada
- Natural Resources Canada
- National Defence
- Foreign Affairs Canada
- Indian and Northern Affairs Canada
- Transport Canada
- Social Development Canada
- Treasury Board of Canada Secretariat

Table of Contents

PREFACE 1

INTRODUCTION 2

CHAPTER 1—MANAGEMENT ISSUES 5

CHAPTER 2—CONDUCTING THE AUDIT 10

SECURITY PROGRAM 14

SECURITY ORGANIZATION 24

SECURITY ADMINISTRATION 30

ACCESS LIMITATIONS 40

SHARING OF INFORMATION AND OTHER ASSETS 43

PHYSICAL SECURITY 46

PERSONNEL SECURITY 56

PROTECTION OF EMPLOYEES 62

SECURITY AND CONTINGENCY MANAGEMENT 65

SECURITY AND CONTRACTING MANAGEMENT 69

APPENDIX A—AUTHORITIES AND REFERENCES 71

APPENDIX B—GLOSSARY 74

Guide to the Audit of Security

PREFACE

This guide has been prepared by the Centre of Excellence for Internal Audit, Office of the Comptroller General, Treasury Board of Canada Secretariat. It is an update of the *Guide to the Audit of Security* previously produced by the Evaluation Audit and Review Group, Treasury Board of Canada Secretariat, as a result of the changes made to the *Government Security Policy* (GSP) in June 1994.

This new guide is designed to reflect the most recent changes to the GSP, effective February 2002.

The Centre of Excellence for Internal Audit (CEIA) has issued this *Guide to the Audit of Security* pursuant to its objective to support the internal audit community in the development and sharing of internal audit tools.

This document has been developed under the guidance of an advisory committee composed of representatives from both the internal audit community and functional management for a cross-section of departments and agencies, as well as representatives from the Office of the Auditor General, the Treasury Board of Canada Secretariat policy authority and the CEIA. Accordingly, the document provides authoritative guidance.

The CEIA invites individuals and organizations to send written comments on the guide. Comments should be sent to the attention of the Director of Policy and Special Projects, Centre of Excellence for Internal Audit.

INTRODUCTION

Background

The previous *Guide to the Audit of Security* (GAS) served the audit community by providing direction for conducting audits and reviews of compliance with the *Government Security Policy* (GSP) and its attendant operational security standards. In February 2002, the Treasury Board approved further revisions to the GSP to reflect recent changes in the political world order and the Canadian and global economies. Operational security standards were also required to be updated. Because of these changes to the GSP and standards, it was again necessary to update the GAS; this version reflects those changes.

The GAS does not include the *Audit Guide on Information Technology Security* (ITS) that the Treasury Board of Canada Secretariat (the Secretariat) issued in September 1995 and that is currently under revision. The guide for ITS was initially designed to be used as a separate, self-contained document, with the potential to be incorporated into the GAS at a future date.

Purpose

The primary purpose of the GAS is to provide guidance to the internal audit community in conducting audits covering the implementation of and compliance with the GSP and operational security standards. In addition, it is intended to assist security officials and managers in carrying out self-assessments and reviews of their department's security program.

The GAS is designed in a manner that will support the audit or review of selected portions of a security program, based on risk assessment.

While the prime focus is the assessment of implementation and compliance with the GSP and operational security standards, the GAS can also be used as a starting point for identifying opportunities for better co-ordination and more efficient and effective delivery of the security program. Users may, however, wish to consider additional criteria for these aspects of assessment of security programs.

Caution regarding the intended use of the GAS

This document is not intended to serve as a prescriptive guide to the conduct of audits, self-assessments, and reviews of a department's security program. Rather, it is intended to serve as one reference tool to be applied with professional judgment, depending on the nature of examination being made. The audit procedures *suggested* here should not be considered as a recipe. They are suggestions of possible steps to be taken in order to determine whether a particular audit criterion has been satisfied. Taken together, the audit findings for related audit

criteria should enable the auditor to render an opinion regarding the achievement of the associated management objective, as stated in this document.

Professional auditing standards require that auditors duly consider the risk of rendering an incorrect opinion. For this reason, having access to experts in the field of security is highly recommended. Such experts are useful not only in conducting technical tests or assessments, but in the provision of advice. This advice may relate to the design of audit tests and procedures, the suggestion of questions or lines of enquiry, or the interpretation of audit test results or observations, or the framing of recommendations.

It should be remembered that, while an auditor may rely on the views of an expert, in doing so he or she does not transfer responsibility and accountability for the audit opinion rendered. The opinion remains the auditor's responsibility. When using experts, an obligation exists to establish the basis for reliance on them. Please refer to professional auditing standards, if additional guidance is needed.

Scope

The GAS is intended for use in all organizations listed in Schedule I, Schedule I.1, and Schedule II of the *Financial Administration Act* (FAA).

It also applies to:

(a) any commission under the *Inquiries Act* that is designated by order of the Governor in Council as a department for the purposes of the FAA;

(b) the Canadian Forces, with the proviso that any reference in the GSP to employees does not include members of the Canadian Forces.

Certain agencies and Crown corporations can enter into agreements with the Secretariat to adopt the requirements of the GSP and apply them to their organizations.

The GAS deals with the GSP and operational security standards. It does not provide detailed guidance in the analysis of compliance at a technical level. For assistance in auditing compliance at a technical level, consult the lead security agency responsible.

If further assistance is needed in the interpretation of the GSP, its operational security standards, or the GAS, contact:

- the Information, Communications and Security Policy Division of the Secretariat for policy interpretation; or

- the Centre of Excellence for Internal Audit, Office of the Comptroller General of the Secretariat.

For assistance in auditing or reviewing a department's information technology security (ITS) operations, consult the *Information Technology Security Audit Guide*.

GAS organization

The GAS is organized in the following manner:

Chapter 1—Management Issues provides an overview of the relationship of the GSP to management issues as a whole. In essence, this chapter provides a description of the overall management control framework expected to be in effect for security.

Chapter 2—Conducting the Audit outlines a menu of procedures for auditing the implementation of and compliance with the GSP and the operational security standards. This section of the GAS includes the objectives, criteria, and audit procedures that can be used in conducting audits or reviews. The management objectives described in this chapter represent more detailed and specific statements of requirement, aligning the management control framework, as implemented by management, with the GSP and related operational security standards.

CHAPTER 1—MANAGEMENT ISSUES

Security environment

1.1 Accountability framework

A fundamental principle of the GSP is the accountability of deputy heads for security of government assets and the protection of employees within their departments. This dictates that the deputy implements a departmental security program with clearly identified accountabilities for all personnel. The GSP and operational security standards outline mandatory and discretionary safeguards to ensure the continued provision of services. The discretionary safeguards should be implemented unless a threat and risk assessment indicates otherwise. This will show due diligence on the part of deputy heads and their departmental security officers (DSOs).

If departments are to implement security programs that are efficient and effective, they must be able to administer them within their particular mandates and according to their priorities, budgets, and organizational cultures and environments. The GSP recognizes this by defining broad requirements to ensure a certain baseline level of security within a department and across the government as a whole. At the same time, it allows the discretion needed to respond to specific concerns and other conditions by permitting a risk management approach to security once these security baselines have been met.

1.2 Government security model

Security in the context of the federal government relates to application of safeguards to reduce the risk of injury of employees either from occupational hazards or acts of violence; to preserve the confidentiality, integrity, and accessibility of information; and to protect the value and availability of assets in order to ensure the continuity of public services.

The GSP and operational security standards describe a departmental security program model with the following requirements:

- Departments must appoint a departmental security officer (DSO) to establish and direct a security program. Given the importance of the position, consideration should be given to appointing a DSO with sufficient security experience who is strategically positioned within the organization so as to provide department-wide strategic advice and guidance to senior management (GSP Art. 10.1).
- Departments must develop adequate arrangements with other governments (including foreign, provincial, territorial, and municipal ones), international, educational, and private-sector organizations when sharing Government of Canada information and other assets (GSP Art. 10.2). When some GSP requirements are difficult to apply in certain foreign

environments, special standards may be developed in consultation with Foreign Affairs Canada (GSP Art. 10.3).

- The contracting authority must confirm the security screening of contractors and the safeguarding of government assets, including IT systems, and also specify the necessary security requirements in the terms and conditions in any contractual documentation (GSP Art. 10.4).
- Departments must confirm the appropriate training of security professionals and that a security awareness program is in place and individuals are briefed on access privileges and prohibitions prior to commencement of duties (GSP Art. 10.5).
- Departments must safeguard information in consideration of the interests of confidentiality, as defined in the *Access to Information Act* and the *Privacy Act* and safeguard other assets in consideration of their availability, integrity, and value (GSP Art. 10.6).
- Departments must conduct ongoing assessments of threats and risks to determine safeguards required and continuously monitor the threat environment for changes and make corresponding adjustments to maintain an acceptable level of risk (GSP Art. 10.7).
- Departments must limit access to classified and protected information on a need-to-know basis to individuals who possess the appropriate security screening level. Access to other assets should not compromise safeguards designed to ensure availability, integrity, or value of those assets (GSP Art. 10.8).
- Security screening must confirm that individuals with access to government information and other assets are reliable and trustworthy (GSP Art. 10.9).
- Departments are responsible under the *Canada Labour Code*, Part II, and under Treasury Board policy for the health and safety of employees at work (GSP Art. 10.10).
- Departments must confirm that physical security is fully integrated into the layout and design of facilities, including the use of measures to delay and prevent unauthorized access to government assets and to safeguard employees from violence (GSP Art. 10.11).
- Information systems must be secured against rapidly evolving threats that have the potential to impact on their confidentiality, integrity, availability, intended use, and value (GSP Art. 10.12)[1].
- Departments must develop plans and procedures to move up to heightened security levels in case of emergency and increased threat (GSP Art. 10.13).
- Departments must establish a business continuity planning program to ensure the continued availability of critical services and assets (GSP Art. 10.14).

[1] Information Technology (IT) security involves prevention, detection, response, and recovery controls and strategies. As noted previously, IT security is the subject of a separate audit guide.

- Departments must develop procedures for reporting and investigating security incidents and taking corrective action (GSP Art. 10.15).
- Departments are required to apply sanctions in response to security incidents when in the opinion of the deputy head there has been misconduct or negligence (GSP Art. 10.16).
- Departments are required to conduct active monitoring and internal audits of the security program (GSP Art. 11).

The effectiveness of the security program depends upon the performance of each of these elements in an integrated manner. Therefore, where responsibility for the various sub-elements is assigned to different organizational units within the department, a co-ordinated approach is required for the planning, management, and administration of the security program.

1.3 Roles and responsibilities

Deputy head

Deputy heads are accountable for safeguarding employees and assets under their area of responsibility and for implementing the GSP.[2]

Departmental security officer (DSO)

Departments must also appoint a DSO to establish and direct a security program that ensures co-ordination of all policy functions and implementation of policy requirements.[3] These functions include ensuring that the security requirements of the departmental security program model described above under section 1.2 are effectively implemented and addressed.

Departments and agencies with security responsibilities

The following government departments and agencies are responsible for one or more aspects of security[4]:

- Treasury Board of Canada
- Treasury Board of Canada Secretariat (the Secretariat)
- committees providing advice and guidance to the Secretariat
- Canadian Security Intelligence Service
- Communications Security Establishment
- Foreign Affairs Canada
- National Archives of Canada

2 GSP, Art. 6.

3 GSP, Art. 10.2.

4 More information is found in the GSP, Appendix A—Responsibilities.

- National Defence
- Critical Infrastructure Protection and Emergency Preparedness (part of Public Safety and Emergency Preparedness Canada)
- Privy Council Office
- Public Works and Government Services Canada
- Royal Canadian Mounted Police
- Transport Canada

1.4 Requirement for internal audit in support of security

Current Government of Canada security doctrine advocates a risk-based approach to security, rather than a rules-based approach. Past direction on security suggested that complying with the letter of the GSP would in itself ensure an adequate level of security. The current emphasis requires that those responsible for security should assess the extent to which security measures adequately address risk exposures specific to their department.

Consistent with this expectation, a variety of security oversight activities occur to confirm the ongoing effectiveness of a department's security practices. Examples include:

- threat and risk assessments (TRAs);
- intrusion detection;
- technical vulnerability assessments;
- supervision by managers at all levels;
- spot checking and inspection for compliance by security specialists;
- investigations of suspected security incidents;
- active monitoring of user activity; and
- technical audits of user activity.

Each of these activities helps to ensure that departmental staff, facilities, and other assets are being protected adequately, in accordance with the specific security risks associated with the operations of a specific department.

In addition to the risk management activities of those directly involved in security oversight, management, through the implementation of an integrated risk management regime, and internal audit, as part of its risk-based planning activities, continuously monitor and assess risk exposures, including those posed to departmental security.

The GSP requires departments to undertake internal audits of security (GSP Art. 11). The specific aspects to be examined (full life cycle or a specific area of security, threat, or vulnerability) will be a decision based on risk and the requirements of the department.

The conduct of audits or any form of independent examination represents a cost over and above the resources already invested by management in security. The internal audit community needs to be mindful of the benefits to be derived relative to the costs, including the opportunity costs to security operations and performance of ongoing oversight activities.

1.5 Interpretation of the results of the internal audit

It must be realized that the answer to a question regarding security will not always be straightforward. Security is a complex discipline that often requires significant expertise and experience to properly interpret the results of audit tests and procedures. Further, the appropriateness of the security program within a department at a particular time needs to be judged in the context of both the programs and operations of that department and the prevailing environment. For these reasons, the assistance of a security specialist is highly recommended. Ideally, the security audit would be a collaborative effort between an audit specialist and a security specialist, with the auditor assuming full accountability and responsibility for the audit.

1.6 Audit reports and working paper files

The contents of the GAS are unclassified. However, audit reports, related working paper files, and documentation obtained from management will likely contain sensitive information on security practices and arrangements, related deficiencies, risk exposures in protection of valued departmental assets, or other examples of non-compliance with the GSP. Auditors must exercise due care to ensure that their e-mail messages, working papers, and reports are appropriately classified and protected. Both the DSO and ATIP Co-ordinator can be consulted for guidance.

CHAPTER 2—CONDUCTING THE AUDIT

Introduction

This chapter identifies specific audit objectives, criteria, and audit procedures for use by auditors conducting security audits. They reflect the requirements of the new GSP and operational security standards for implementing and maintaining an effective security program. In addition, they represent best practices borrowed from previous audits of security programs. Auditors may be required to add to, modify, or delete the specific objectives, criteria, and audit procedures to adapt the audit process to their organization, depending on unique threat and risk environments or unique vulnerabilities within a specific operational environment.

Audit objectives

The following audit objectives are grouped based on the new GSP and related operational security standards. Objectives, like criteria, are stated goals that are to be achieved under an effective security program.

All objectives emanate from requirements of the GSP. Some of the general headings, such as security organization and security administration, contain objectives that are referred to throughout the GSP. Others, such as access limitations and protection of employees, are concentrated in one specific area of the GSP. For ease of referral by auditors, the specific reference to the GSP for each objective is annotated in parentheses.

Security program

1. The department has implemented a security program design that ensures co-ordination of all policy functions and complies with the security baselines of the GSP (GSP Art. 10.1).
2. Threat and risk assessments (TRAs) are conducted and applied in accordance with the GSP (GSP Art. 10.7).
3. The security program has been designed to complement the management of emergency situations (e.g. fire, bomb threats, hazardous materials, power failures, evacuations, civil emergencies, etc.) (GSP Art. 10.13).
4. The security program as applied outside of Canada duly considers risk exposures, as identified and revised by Foreign Affairs Canada (GSP Art. 10.3).
5. Active monitoring occurs as part of the security program (GSP Art. 11).

Security organization

6. The mandate and experience of the DSO correspond with the scale and complexity of the department’s operations (GSP Art. 10.1).

7. A security management structure is in place that encompasses responsibility for the overall management of the department's security program, including administrative, physical, information technology, and personnel security, as well as security for contingency and contracting management and that meets the needs of the department (GSP Arts. 10.1, 10.7, 11).

Security administration

8. The security program has been integrated into the overall departmental planning process (GSP Art. 10.1).
9. Appropriate security training is provided to security specialists: routine periodic awareness sessions are provided to inform and remind individuals of their security responsibilities, issues, and concerns and briefings are conducted regarding responsibilities and accountabilities attached to security screening levels (GSP Art. 10.5).
10. Sensitive information and assets are identified as CLASSIFIED or PROTECTED, according to the GSP and operational security standards (considering confidentiality, integrity, availability, and value), and sensitivity labels are downgraded or removed when the information and assets are less, or no longer, sensitive (GSP Art. 10.6).
11. Violations and breaches of security and other security incidents are investigated, action is taken to minimize loss, and appropriate administrative, corrective, or disciplinary action is taken (GSP Arts.10.15 and 10.16).

Access limitations

12. Access to sensitive information and assets is limited to those individuals with formal access approval, requisite security clearance, and the need to know (GSP Art. 10.8).
13. No one individual can independently control all aspects of a process or system (especially a security safeguard) (GSP Art. 10.8).

Sharing of information and other assets

14. Appropriate safeguards are applied to sensitive information shared with or received from official sources outside the department. These official sources include foreign, provincial, territorial, and municipal governments and international, educational, and private-sector organizations (GSP Art. 10.2).
15. Processes and agreements are in place to ensure that information received from other official sources is protected, in accordance with the security policies and standards of the parties concerned (GSP Art. 10.2).

Physical security

16. An appropriate security assessment is conducted prior to locating and designing facilities to reduce or eliminate the threats and risks to sensitive information, assets, and employees in the facilities (GSP Art. 10.11).
17. Appropriate physical safeguards are in place at facilities to provide for the safeguarding of sensitive information and assets, as well as the safety and security of employees (GSP Art. 10.11).
18. A series of increasingly restrictive physical security zones is established and maintained with appropriate access control mechanisms to protect sensitive information and assets (GSP Art. 10.11).
19. A continuous review of physical security safeguards is conducted to reflect changes in the threat environment and to take advantage of new cost-effective technologies (GSP Art. 10.11).

Personnel security

20. All individuals with access to government assets (except for Governor in Council appointees) must have at least reliability status (GSP Art. 10.9).
21. The security screening of individuals is carried out according to the GSP and the Personnel Security Standard (GSP Art. 10.9).
22. Termination of an individual's employment is undertaken in a way that reduces or eliminates any risk to the department's sensitive information, systems, assets, or personnel (implied in GSP Art. 10.9).

Protection of employees

23. A TRA has been conducted to identify situations where employees are under threat of violence because of their duties or because of situations to which they are exposed (GSP Art. 10.10).
24. Mechanisms are in effect to identify, protect, and support employees (and their families, as appropriate) under threat of violence or working in high-risk areas (GSP Art. 10.10).

Security and contingency management

25. Managers of facilities throughout the department have developed plans to protect sensitive information, assets, and employees during all types of emergencies and increased threat situations (GSP Art. 10.14).
26. Department-wide plans are developed to provide for the continuity of critical business operations, services, and assets following an unplanned interruption (GSP Art. 10.14).

Security and contracting management

27. Security requirements for the protection of information, assets, and personnel are adequately addressed as part of the contracting process (GSP Art. 10.4).

SECURITY PROGRAM

Objective 1

The department has implemented a security program design that ensures co-ordination functions of all policy functions and complies with the security baselines of the GSP (GSP Art. 10.1).

Criterion 1.1 A departmental security policy and supporting documentation (standards, directives, guidelines, and procedures) have been developed and disseminated and are maintained.

Audit procedures:

1.1.1 Review documentation for currency and accuracy.

1.1.2 Confirm that the departmental security policy and supporting standards reflect the current GSP.

1.1.3 Confirm that the security policy and standards are consolidated in a security manual or distributed throughout other manuals and/or files. Identify manuals and/or files.

1.1.4 Confirm information is readily available (either on-line or in hard copy) throughout the department.

1.1.5 Confirm updates are disseminated, advertised, and available to all employees on a timely basis.

1.1.6 Interview managers to confirm that they have a copy of the policy and procedures supporting documentation or that they know where copies are readily available and assess their awareness of the contents of these documents.

1.1.7 Ask employees on a random basis to provide you with access to the departmental security policy and standards.

Criterion 1.2 Security guidance is department-specific.

Audit procedures:

1.2.1 Confirm that the security objectives in the departmental security policy and supporting documentation are consistent with the objectives, mandate, mission and risk profile of the department.

Criterion 1.3 Security guidance is compliant with the GSP and its supporting documentation.

Audit procedures:

1.3.1. Analyze the departmental security policy in direct comparison to the GSP and its operational security standards.

1.3.2 Confirm that specific security standards, directives, orders, and procedures are consistent with the mandatory requirements of the GSP.

Criterion 1.4 Supporting government and departmental documentation is available to security specialists.

Audit procedures:

1.4.1 Interview the principal security officers (the Departmental Security Officer (DSO), as well as representatives from Corporate Security, IT Security, Business Continuity Planning, and Occupational Safety and Health) to confirm that they have access to copies of pertinent government operational security standards and technical documentation available from the Secretariat and other leading departments. This also includes technical security standards, specifications, best practices, and guidelines developed and issued by lead security departments.

Criterion 1.5 Individuals employed by or doing business with the department are subject to the departmental security policy and supporting documentation.

Audit procedures:

1.5.1 Confirm that individuals employed by or doing business with the department are listed in the departmental security policy as being obliged to follow its direction as a condition of access to sensitive information and valued assets.

1.5.2 Confirm that such individuals have access to the security policy and are provided with information relevant to their responsibilities.

1.5.3 Confirm that individuals have acknowledged their understanding and acceptance of their security obligations in a signed statement, as may be required.

1.5.4 Confirm that individuals have attended mandatory security training.

Criterion 1.6 The deputy head has overall accountability for security.

Audit procedures:

1.6.1 Confirm that a clear statement exists, such that the deputy head (or equivalent) has overall accountability for safeguarding employees and assets in his or her area of responsibility and for implementing a departmental security program.

1.6.2 Confirm that security responsibilities delegated by the deputy head are documented and are assigned to a specific position for a specified time period.

Objective 2

Threat and risk assessments (TRAs) are conducted and applied in accordance with the GSP (GSP Art. 10.7).

Criterion 2.1 Employees are familiar with the TRA process and the role it plays in selecting cost-effective safeguards.

Audit procedures:

2.1.1 Review the departmental policy and procedures to determine that information is provided explaining the risk management and TRA process. (Does the policy indicate the scope of individual TRAs by business line, function, facility, directorate, branch, or a combination of these or some other organizational structure that meets the needs of the department?)

2.1.2 Assess whether procedures adequately explain how to carry out a TRA and recommend a format for TRA reports.

2.1.3 Examine planning material to confirm that risk management is a component part of the DSO's security awareness strategy.

2.1.4 Interview a sample of employees, both at the managerial and line level, to assess their awareness and understanding of the TRA process.

Criterion 2.2 TRAs are completed by the managers assigned this responsibility.

Audit procedures:

2.2.1 Confirm that TRA reports have been completed by the managers required to do so by the policy. If TRAs have not been completed by all managers, obtain an explanation from the DSO.

2.2.2 Confirm that senior management makes decisions for amendments to baseline requirements arising from the recommendations of TRAs after receiving input from the DSO.

Criterion 2.3 TRAs are conducted as a means to determine security safeguards.

Audit procedures:

2.3.1 Confirm that there is an inventory of baseline security safeguards (personnel, physical, technical, and procedural).

2.3.2 Confirm that the implementation of additional or amended safeguards is based on an informed decision by senior departmental management as a result of a current TRA.

- Identify additional security safeguards from records or interviews with security specialists and map safeguards to TRAs on file.
- Where safeguards are not mapped to a TRA, confirm the basis upon which the decision was made to amend the security baseline.

2.3.3 Confirm that the department conducts ongoing formal and informal assessments of threats and risks to determine whether additional security safeguards (beyond baseline) are required.

2.3.4 Confirm that the department uses established TRA methodologies (e.g. CSE, RCMP, DND, COBITS, etc.) or has developed a departmental template. If so, confirm that it meets the intent and risk elements of established TRA methodologies.

2.3.5 Establish if TRAs are conducted in-house or by third-party consultants. Confirm that in-house assessors and third-party consultants have been adequately trained to conduct TRAs.

2.3.6 Review a sample of TRA reports and interview the managers responsible for them to confirm that the TRAs were completed following the process set out in the policy and procedures and that the reports are complete and comprehensive. As part of this review, determine the sources contacted to obtain information on threats. Also determine the options that were considered to reduce risks when selecting appropriate safeguards.

2.3.7 Review a list of the security incidents that have occurred at facilities and select the more serious ones. Obtain the reports covering the incidents and the TRA reports covering the same facilities. Review both documents and confirm whether there were any weaknesses in the TRA process.

2.3.8 Confirm what process the DSO has in place to monitor TRA reports to confirm that:

- they are complete, comprehensive, and adhere to policy and procedures;
- action was taken on recommendations in the reports; and
- there are possible weaknesses in the department's security program.

2.3.9 Confirm that a policy exists on the updating of TRA reports and ensure that they are current. For example, determine whether they are updated when there has been:

- a breach of security or other serious security incident;
- a change in the operational mission of the department or the addition of new mandates;
- a significant change in sensitive information and assets, information systems, infrastructure, or employees;
- a change in threats to sensitive information or assets or employees or a change in the probability of such threats occurring; and
- major construction or renovations at the facility.

Criterion 2.4 The department maintains past TRAs and has implemented their recommendations.

Audit procedures:

2.4.1 Obtain a listing of all TRAs on file and confirm with the DSO that the list is complete.

2.4.2. Confirm that they are available to functional or regional security specialists, as required.

2.4.3 Examine records of recent (i.e. since the last TRA) security incidents and actions taken to confirm that records are properly maintained.

2.4.4 Conduct tests to confirm that recommendations have been implemented or that there is a record of decision (minutes of meetings, e-mails, memoranda, etc.) from senior management that a recommendation will not be implemented.

Objective 3

The security program has been designed to complement the management of emergency situations (e.g. fire, bomb threats, hazardous materials, power failures, evacuations, civil emergencies, etc.) (GSP Art. 10.13).

Criterion 3.1 Security risk management duly considers emergency situations and measures to respond to emergencies.

Audit procedures:

3.1.1 Obtain an overview from the DSO on how the security program addresses emergency situations and complements emergency management activities.

3.1.2 Confirm representations made by the DSO by reviewing emergency policies, plans, and/or procedures.

3.1.3 Analyze, through comparison of selected plans and security procedures, the departmental security policy, supporting documentation, and other mandatory plans or procedures to confirm that they complement each other.

Criterion 3.2 Co-ordination of the departmental security program with other departmental organizations, including interdepartmental emergency organizations, is adequate.

Audit procedures:

3.2.1 Obtain a listing of the Office(s) of Primary Interest (OPIs) for emergency plans that fall outside of the strict scope of the departmental security program. Confirm that roles and responsibilities are clearly defined.

3.2.2 Obtain an overview of the mandate of each organization, a delineation of respective roles and responsibilities, and the approach used to keep OPIs duly informed, including the use of committees.

3.2.3 Confirm that lines of communication have been established between the DSO and the other OPIs to harmonize the respective roles, policies, programs, and procedures.

3.2.4 Through the interview of selected OPIs, ascertain whether they are appropriately involved in or consulted on decisions of mutual interest and receive information when and as required to fulfil their respective duties.

Objective 4

The security program as applied outside of Canada duly considers risk exposures, as identified and revised by Foreign Affairs Canada (GSP Art. 10.3).

Criterion 4.1 The DSO is aware of risk exposures related to international operations and security arrangements and any special security standards have been reviewed and developed in consultation with Foreign Affairs Canada.

Audit procedures:

4.1.1 Review departmental mission statements and supporting documentation and confirm the DSO's understanding of any operations conducted outside of Canada.

4.1.2 Confirm that security arrangements and standards (operational, physical, personnel, technical, procedural, etc.) for foreign environments have been reviewed and adapted in consultation with Foreign Affairs Canada.

4.1.3 Review the DSO's planning documentation or activities to confirm that foreign operations are duly considered.

Criterion 4.2 Personnel working outside of Canada have been made aware of special security requirements and any restrictions placed on personal activities.

Audit procedures:

4.2.1 Confirm that the DSO has ensured that personnel working outside of Canada have received adequate and timely notification of special security requirements by such mechanisms as:

- formal security briefings;
- security bulletins;
- country fact sheets; and/or
- intelligence reports.

4.2.2 Interview a sample of employees to confirm that personnel have been made aware of local conditions and appropriate security practices to ensure their personal security.

Objective 5

Active monitoring occurs as part of the security program (GSP Art. 11).

Criterion 5.1 Appropriate security monitoring processes are implemented.

Audit procedures:

5.1.1 Obtain an overview of the approach taken and information used by the DSO to monitor departmental practices and detect anomalies.

5.1.2 Determine the existence and purpose of manual and/or automated security monitoring processes (intrusion detection systems, technical vulnerability assessment tools, etc.).

5.1.3 Where active monitoring devices have been implemented, confirm their use (e.g. misuse detection vs. anomaly detection, active vs. passive, host-based vs. network-based, etc.) is governed by or based on the results of a TRA.

5.1.4 Confirm that anomalies are brought to the attention of the DSO.

5.1.5 Confirm that the DSO periodically reviews security-monitoring reports.

Criterion 5.2 An effective security oversight process is in place.

Audit procedures:

5.2.1 Describe the governance framework used by the deputy to provide oversight of the management of the department's security program.

5.2.2 Obtain examples of reports prepared by the DSO on program activities, including spot checks by security staff, active IT system monitoring devices, annual reviews, investigation of anomalies, etc. to demonstrate due diligence.

5.2.3 Confirm the integrity of reports attesting to the degree of intervention by the DSO and security specialists (Corporate Security, IT Security, Business Continuity Planning, Occupational Safety and Health).

Criterion 5.3 Internal audits of security occur, as required.

Audit procedures:

5.3.1 Confirm that the risk-based planning methodology used by the Internal Audit function duly considers risk exposures related to security.

5.3.2 Obtain a copy of recent audits related to security issues and compare their scope and objectives to the GSP to determine the coverage provided by internal audits.

5.3.3 Discuss results of the audit and document how the deputy and DSO were involved in clearing the findings of the audit.

5.3.4 Confirm that the audit reports and related action plans are on the department's Web site (depending on sensitivity) and have been distributed to Secretariat officials responsible for security and that adequate follow-up has occurred.

Note: Criterion 5.3 should be assessed by the Secretariat directly, as the Internal Audit function cannot independently and objectively assess its own performance and the effectiveness of its practices.

SECURITY ORGANIZATION

Objective 6

The mandate and experience of the DSO correspond with the scale and complexity of the department's operations (GSP Art. 10.1).

Criterion 6.1 A DSO has been appointed with the authority to establish and direct a departmental security program.

Audit procedures:

6.1.1 Confirm that a full-time DSO has been appointed.

6.1.2 Obtain the DSO's mandate statement explaining the DSO's responsibilities for direction of the complete departmental security program. Note if any key security responsibilities have been delegated to other entities (e.g. IT security to the Chief Information Officer), and confirm that there is at least a functional reporting relationship between these security entities (e.g. Corporate Security, IT Security, Occupational Safety and Health, Internal Affairs, Business Continuity, etc.) and the DSO.

6.1.3 Confirm that the DSO has been appointed as a single point of contact to address enquiries regarding the departmental security program and supporting documentation. If it is not the DSO, confirm who it is. Confirm that the DSO has a functional responsibility to assist the other points of contact.

6.1.4 Confirm that there is a succession of security responsibilities for the DSO and principal security specialists, should someone become unavailable. Confirm that the DSO and principal security specialists provide ongoing counselling, training, and guidance to subordinates to prepare them to assume higher-level security duties. Confirm that the subordinates have the opportunity routinely and during heightened security situations to assume additional security responsibilities.

Criterion 6.2 The DSO's experience corresponds with the scale and complexity of the department's operations.

Audit procedures:

Determine the level of security expertise and experience of the DSO in consideration of competencies required, given the scale and complexity of the department's operations.

6.2.1. Consider such indicators as:

- years in security positions;
- professional certifications;
- education;
- conferences attended; and
- membership and participation in professional associations.

6.2.2 Confirm that the DSO has a budget for professional development of key security specialists. Assess its adequacy, given the security scope of the department.

Objective 7

A security management structure is in place that encompasses responsibility for the overall management of the department's security program (including administrative, physical, information technology, and personnel security, as well as security, contingency, and contracting management) and that it meets the needs of the department (GSP Art. 10.1, 10.7, 11).

Criterion 7.1 The DSO is strategically placed within the organization so as to provide department-wide guidance to senior management.

Audit procedures:

7.1.1 Confirm that the DSO is considered a senior manager in the department according to the government personnel classification system.

7.1.2 Assess the adequacy of the organizational status of the DSO and the reporting relationship between the DSO and deputy head (using the organization chart, if possible) for both routine and emergency situations.

7.1.3 Confirm that the DSO has direct access to the deputy head for cause.

Criterion 7.2 A security representative has been appointed at each functional or regional level and effectively manages the applicable elements of the departmental security program within his or her area.

Audit procedures:

7.2.1 Confirm that an individual has been appointed as the functional/regional security representative of the DSO.

7.2.2 Confirm that the representative has received adequate training upon appointment. Note courses, seminars, and awareness sessions attended in the past year.

Criterion 7.3 There is a clear and documented reporting structure and information flow between the DSO and the functional/regional security representative.

7.3.1 Confirm that there is a process for routine and exceptional reporting to the DSO. Confirm the process is documented and understood by the functional/regional security representative.

Criterion 7.4 Security responsibilities are established, defined, and assigned.

Audit procedures:

7.4.1 Confirm that a departmental security officer (DSO) has been appointed with responsibility and accountability for developing, implementing, maintaining, co-ordinating, and monitoring the department's security program.

7.4.2 Confirm that there are key positions established with responsibility for Corporate Security (i.e. physical, personnel, and administrative security), IT Security, Business Continuity Planning investigations, and Occupational Safety and Health.

7.4.3 Confirm that there is a functional or line relationship between the DSO and the key security positions, that the DSO meets with the incumbents of these positions on a regular basis and, through interviews with the DSO and the incumbents of the positions, that the functional relationships are contributing to an efficient and effective security program.

7.4.4 Review the most recent organizational charts and confirm that they show all line and functional relationships of the security structure. If the functional relationships are not shown on the organizational charts, are they documented in the departmental security policy?

7.4.5 Review the position descriptions of the key security personnel and confirm that the required duties and responsibilities have been included. If a position is responsible for duties other than security, what priority and percentage of time are shown for security duties? Are the priority and percentage of time allocated satisfactory for someone in a key security position?

7.4.6 Interview key security personnel to confirm their knowledge of their security duties and responsibilities.

7.4.7 Confirm that the departmental security policy has assigned responsibility and accountability for the security specialties at the regional, branch, and unit levels and that the duties are reflected in the position descriptions. Confirm the functional and reporting relationships between these positions and both the key security specialists and the DSO.

Criterion 7.5 Linkages exist with administrative functions.

Audit procedures:

7.5.1 Obtain an overview of the internal linkages and ongoing working relationship between the DSO/key security specialists and the following areas within the department, confirm the frequency of contact and meetings, and assess their adequacy. Consider:

- Access to Information and Privacy;
- Internal Audit;
- Occupational Health and Safety;
- Informatics (including telecommunications);
- Legal Services;
- Minister's Office;
- Human Resources;
- Materiel Management;
- Property Management; and
- Records Management.

7.5.2 Interview managers in the above areas and confirm that the working relationships with key security specialists are functioning properly and contribute to an efficient and effective security program.

7.5.3 Confirm the participation of the DSO and other key security specialists in inter-departmental security committees, working groups, and projects. Provide a list of committees.

7.5.4 Obtain an overview of the department's external linkages and the ongoing working relationship between the DSO/key security specialists and the following areas (confirm the frequency of contact and meetings and assess their adequacy).

- Treasury Board of Canada Secretariat—central agency for security and service delivery issues for the Government of Canada, including the GSP;
- committees supporting the Secretariat—provide advice and guidance on implementation of the GSP, review and recommend operational security standards;
- Canadian Security Intelligence Service—threat assessment information and personnel security screening;
- Communications Security Establishment—cryptology and IT security technical authority, inspecting, testing, and evaluating COMSEC systems and procedures;

- Foreign Affairs Canada—lead department for conducting foreign relations;
- National Archives of Canada—lead organization responsible for the management of government records;
- National Defence—lead department for advice on military intelligence and protection of NATO atomic information;
- Critical Infrastructure Protection and Emergency Preparedness—lead entity for effective emergency management, incidents, and threats affecting the availability of critical assets and services;
- Privy Council Office—overall policy direction for security and intelligence in the federal government and for incidents involving the compromise of Cabinet confidences;
- Public Works and Government Services Canada—common service department for contracting, real property management, information technology, and communications;
- RCMP—lead organization for physical and information technology security and contributing organization for security screening;
- Transport Canada—lead department for land, air, and maritime security;
- Health and Safety officers appointed under the *Canada Labour Code*—for incidents considered as "hazardous occurrences" or that involve employee injury; and
- local police and fire departments—for threat assessment information.

7.5.5. Interview the DSO and key security personnel concerning recent contacts or meetings that they have had with officials in the above departments and agencies.

SECURITY ADMINISTRATION

Objective 8

The security program has been integrated into the overall departmental planning process (GSP Art. 10.1).

Audit procedures:

8.1.1 Obtain an overview of security planning activities and how they relate to corporate planning.

8.1.2 Confirm that short- and long-term plans and goals have been developed for the departmental security program. Review these and confirm that they are complete, reasonable as to time frames and the availability of resources, consistent with the department's strategic plans, and approved by senior management.

8.1.3 Confirm that the funding of the security program is an identifiable item in the department's budget.

8.1.4 Review the level of funding of the security program and discuss with the DSO the adequacy of the funding and the implications of any significant reductions in the funding level.

Objective 9

Appropriate security training is provided to security specialists: routine periodic awareness sessions are provided to inform and remind individuals of their security responsibilities, issues, and concerns and briefings are conducted regarding responsibilities and accountabilities attached to security screening levels (GSP Art. 10.5).

Criterion 9.1 Full- or part-time security specialists receive effective and timely security training and professional development.

Audit procedures:

9.1.1 Confirm what security training courses and security seminars were made available to key security specialists during the previous two years. This should be based on required competencies and the information should be available from the following organizations:

- Information, Communications and Security Policy Division of the Secretariat;
- Federal Association of Security Officials;
- Training Branch of the Public Service Commission (Training and Development Canada);
- the lead security agencies;
- other professional security organizations;
- Royal Canadian Mounted Police training branch;
- community colleges and universities; and
- other professional security organizations, such as the American Society for Industrial Security, Canadian Society for Industrial Security, High Tech Crime Investigation Association, Information System Security Association, Disaster Recovery Institute, etc.

9.1.2 Determine how the DSO:

- keeps informed of the training courses and seminars that are available for security personnel;
- ensures that security specialists and other employees are aware of available training sessions; and
- monitors training received and security orientation provided to other employees and contract personnel.

9.1.3 Confirm what security training has been provided to key security specialists in the past two years to assist them in carrying out their duties.

9.1.4 Confirm that security specialists receive advanced security training and professional development external to the department. Confirm if provisions have been made for security specialists to achieve professional security certifications and participate in security seminars and professional security associations.

9.1.5 Obtain an overview of how the training needs of other employees performing full- or part-time security duties are identified. (Consider whether the DSO is the primary point of contact for security training. If not, confirm who is.)

9.1.6 Confirm what security training has been given in the previous 12 months to other employees performing full- or part-time security duties.

9.1.7 Confirm that the DSO staff receives security periodicals and attends vendor presentations, product seminars, and other professional presentations in order to remain current on emerging technologies.

Criterion 9.2 The DSO has an adequately funded and appropriate security awareness strategy.

Audit procedures:

9.2.1 Obtain an overview of the DSO's activities related to the security awareness strategy and the means used to identify issues requiring reinforcement.

9.2.2 Confirm that the DSO has a process in place to monitor the effectiveness of the security education program and strategy. Consider such items as:

- statistics of security incidents (breaches and violations);
- amount of security awareness correspondence disseminated;
- number of security awareness sessions held; and
- topics covered in security awareness correspondence and sessions (for appropriateness and timeliness).

9.2.3 Review the security incidents (breaches and violations) for the past 12 months to confirm the effectiveness of the security awareness strategy.

9.2.4 Confirm, in discussion with the DSO, the adequacy of the DSO's budget available for the security awareness program.

Objective 10

Sensitive information and assets are identified as CLASSIFIED or PROTECTED according to the GSP and operational security standards (considering confidentiality, integrity, availability, and value) and sensitivity labels are downgraded or removed when the information and assets are less, or no longer, sensitive (GSP Art. 10.6).

Criterion 10.1 Sensitive information and assets are classified and designated using a departmental *Information Classification Guide* or by officials authorized by the deputy head to do so or by both.

Audit procedures:

10.1.1 Obtain an overview of practices in place to identify sensitive information and determine its classification.

10.1.2 Review departmental procedures and practices to determine if they address the following requirements:

- Sensitive information and other assets that must be protected from unauthorized disclosure are identified and categorized either in the national interest or non-national interest (but subject to the provisions of the *Access to Information Act* and the *Privacy Act* in order to meet confidentiality requirements).
- Information and valued assets are identified and categorized according to the degree of injury that would accrue if they were modified in order to meet integrity requirements.
- Information and valued assets are identified and categorized according to the degree of injury that would accrue if they were lost in order to meet availability requirements.
- Information and other assets are assigned a monetary, cultural, good will, or other value should they be modified or lost in order to meet asset value requirements.
- The department has produced an *Information Classification Guide* for assigning labels to sensitive information and valued assets.

10.1.3 If a departmental guide is used, review it and confirm that:

- it accurately reflects the type of sensitive information created within the department in terms of confidentiality, integrity, availability, and value;
- the guide is consistent with and complies with the GSP and operational security standards and sets out clearly how to assign security classifications to documents;

- the guide has been updated to reflect changes in the GSP of February 2002; determine who is responsible for updating the guide and what process is in place to confirm that it is kept up-to-date; and
- employees whose duties include the creation and collection of sensitive information have ready access to a copy of the guide.

10.1.4 Interview employees whose duties include the creation and collection of sensitive information and confirm that they are familiar with the process to be followed when they want to classify sensitive information.

10.1.5 If certain positions and appointments are authorized to classify sensitive information, review a list of the positions and confirm that:

- the DSO maintains a current list of those positions and appointments;
- the positions are strategically located throughout the department so that they are readily accessible by all employees; and
- the list is reviewed periodically by the DSO to ensure that the positions have a demonstrable and continuing need to have this authority and that the incumbents are adequately trained to carry out this duty.

10.1.6 Interview officials occupying positions that are authorized to classify sensitive information and confirm that they are familiar with their responsibilities in this regard. Confirm that they have a functional line to the DSO for specialist advice.

Criterion 10.2 Classified and protected information is marked with the appropriate security labels to indicate the minimum safeguards that are to be applied to protect the information.

Audit procedures:

10.2.1 Confirm that procedures have been issued that explain how security markings are to be applied to file folders, documents, manuals, microform devices, and other valued assets containing sensitive information. Confirm that the procedures are readily accessible by all employees whose duties require the creation and collection of sensitive information. It is most appropriate to include this guidance in an *Information Classification Guide*.

10.2.2 Confirm that there are procedures for marking sensitive and valued assets for availability, integrity, or value, even if there are no confidentiality concerns.

10.2.3 Examine several types of sensitive material and confirm that they have been marked in accordance with written direction and the operational standard on identification of assets. If there are inconsistencies, determine if possible who applied the marking and confirm that they are aware of the guidance on how to mark sensitive information and valued assets.

Criterion 10.3 Sensitivity labels (CLASSIFIED or PROTECTED) given to sensitive information are removed or changed when the information is no longer sensitive or is less sensitive and does not require the safeguards applied at the higher level.

Audit procedures:

10.3.1 Confirm that procedures (typically an *Information Classification Guide*) have been issued that explain the declassification and downgrading of sensitive information and assets. Confirm that classification guidance encourages authors to add time limitations or other caveats that permit automatic downgrading or declassification.

10.3.2 Review the procedures on declassification and downgrading to confirm that they are easily understood and provide sufficient direction on the process. Determine if classification guidance explains the rationale and process in clear terms for declassification and downgrading of sensitive information and assets.

10.3.3 Confirm which positions are authorized to declassify and downgrade sensitive information and that these positions are identified in the policy and procedures. Confirm that the procedures are readily accessible by the incumbents in these positions.

10.3.4 Determine frequency and procedures followed to upgrade the assignment of sensitivity levels.

10.3.5 Confirm that the policy states that sensitive information received from sources outside the department is not to be declassified or downgraded without the prior approval[5] of the owners or originators of the information.[6]

10.3.6 Confirm from incumbents of positions that are authorized to declassify and downgrade sensitive information which information they have declassified or downgraded during the previous year.

---

5 Approval can be obtained on a case-by-case basis or through written agreements or understandings between the parties concerned.

6 The department should also issue procedures on the action to be taken when it is not possible to consult with the owners or originators of the information.

10.3.7 Determine whether information that has been declassified and downgraded is clearly marked to show that it is no longer classified or designated or that it has a lower classification or designation along with the date or caveat that led to its downgrading.

Note: The requirements for declassifying and downgrading sensitive information are needed, because the over-classification of large volumes of information results in costly mandatory safeguards being kept in place to protect the information long after such protection is warranted. The declassification and downgrading of sensitive information distributed throughout large volumes of files may have greater resource implications than leaving the information classified or designated at the level at which it was marked in the first instance. The intent of the security policy might be met through compensating measures, such as the routine destruction of files in accordance with the retention and disposal schedule of the National Archives of Canada.

Criterion 10.4 Information that has been declassified and downgraded is clearly marked to show that it is no longer classified or designated or that it has a lower classification or designation.

Audit procedures:

10.4.1 Confirm that procedures have been issued that explain how security markings are to be changed on material containing information that has been declassified or downgraded. Confirm the procedures are readily accessible by all positions authorized to declassify or downgrade sensitive information.

10.4.2 Examine several types of sensitive material that have been declassified or downgraded and confirm that they were marked in the proper way at the time they were declassified or downgraded.

Objective 11

Violations and breaches of security and other security incidents are investigated, action is taken to minimize loss, and appropriate administrative, corrective, or disciplinary action is taken (GSP Arts. 10.15 and 10.16).

Criterion 11.1 There is an investigative body to conduct security investigations.

Audit procedures:

11.1.1 Obtain an overview of the organizational arrangements in place regarding the investigation of possible security breaches, security violations, and other security incidents.

11.1.2 Review the policy and procedures and confirm that they are consistent with and comply with the GSP and operational security standards and include the offences referred to in the *Policy on Losses of Money and Offenses and Other Illegal Acts Against the Crown.*

11.1.3 Assess position descriptions for security specialists (DSO, Corporate Security, IT Security, Business Continuity Planning, Occupational Safety and Health, etc.), as well as related policy and procedures for the following attributes:

- clearly defined investigative responsibilities;
- clearly delineated boundaries of investigation;
- clearly written statements on the degree of intervention and authority of investigators;
- accountability of all investigators to the deputy head for the effective and legal conduct of any investigation; and
- clarification of the role of the DSO to comment on all investigations involving security.

Criterion 11.2 A process is in place for reporting possible breaches of security, security violations, and other security incidents.

Audit procedures:

11.2.1 Obtain an overview on reporting practices and procedures on possible security breaches, security violations, and other security incidents.

- Review reports on possible security breaches that were reported since the last internal audit and confirm that possible breaches were reported immediately to the DSO and then to the deputy head.

- Confirm that policy and procedures have been issued regarding reporting incidents listed in the *Policy on Losses of Money and Offenses and Other Illegal Acts Against the Crown*.

11.2.2 Confirm that formal or informal lines of communication with the DSO have been established for the following:

- criminal offences
- compromise of Cabinet confidences
- threats to national interests
- availability of critical assets and services
- hazardous occurrences and injury
- amendments to security standards
- law enforcement agencies
- Privy Council Office
- Canadian Security Intelligence Service
- Critical Infrastructure Protection and Emergency Preparedness
- Health and Safety Officer
- the Secretariat

11.2.3 Review reports on possible security breaches that were reported and determine whether breaches were reported to the above agencies as required. Additionally, determine whether the following cases are applicable and require additional reporting:

- The department from which the information involved in the breach of security originated was informed of the incident, if applicable; and
- other departments that had information or assets involved in the breach of security were informed of the circumstances and findings that affected them, if applicable.

11.2.4 Confirm that the DSO conducts monitoring for security violations and other security incidents. Assess the adequacy of monitoring by the DSO in order to be fully responsible and accountable to the deputy head for the department's security program.

11.2.5 Review the records maintained on security incidents for the previous two years. Verify that the required reports were made to the RCMP for statistical purposes. If the reports were not made, is there a reasonable explanation for this?

Criterion 11.3 A process is in place to minimize loss when there has been a security breach or violation or other security incident.

Audit procedures:

11.3.1 Obtain an overview of practices and procedures in place regarding injury and implementing countermeasures and corrective measures to minimize loss when there has been a security breach or violation or other security incident.

11.3.2 Confirm that reports of security breaches and violations and other security incidents are analyzed to identify common problems that should become issues in the DSO's security awareness strategy.

11.3.3 Assess whether the current practices require security specialists to make recommendations on corrective action to be taken as the result of an investigated security incident.

11.3.4 Assess whether current practices call for a directed TRA to confirm the change in residual risk as the result of an investigated security incident.

Criterion 11.4 An effective response capability is in place for security incidents.

Audit procedures:

11.4.1 Assess whether the current practices require:

- electronic sensors to be monitored at a central location;
- the facility to have a capability to respond to unauthorized access.

11.4.2 Confirm that response personnel are properly equipped.

11.4.3 Confirm that monitoring and response personnel are properly trained. Review position descriptions, training records, post orders, and, if applicable, contracts.

Criterion 11.5 Administrative or disciplinary sanctions are applied for security breaches and violations and other security incidents, when appropriate.

Audit procedures:

11.5.1 Obtain an overview of practices and procedures in place regarding the administrative and disciplinary sanctions that can be applied and the process for doing this, including responsibilities of the DSO.

11.5.2 Confirm criteria for applying rewards and sanctions are clearly stated. Confirm managers at all levels are aware of the possibility of recommending rewards and sanctions. Confirm it is clearly identified what constitutes misconduct or negligence.

11.5.3 Review cases where rewards and sanctions were deserved and determine whether the action taken was according to policy and procedures.

ACCESS LIMITATIONS

Objective 12

Access to sensitive information and assets is limited to those individuals with formal access approval, requisite security clearance, and the need to know (GSP Art. 10.8).

Criterion 12.1 A knowledgeable and responsible manager has given formal access approval to the individual requiring access to sensitive information or assets under the "least privilege principle."

Audit procedures:

12.1.1 Obtain an overview of the process used to grant access and test by sampling that the process ensures that employees have been granted formal access approval (typically in writing or through a briefing) by their manager for access to sensitive information.

12.1.2 Confirm that the least privilege principle[7] is adequately applied, explained in security policy, and is understood by personnel.

12.1.3 Interview a sample of personnel to confirm that they understand how to apply the least privilege principle.

Criterion 12.2 Sensitive information is released only to individuals who have the appropriate reliability status or security clearance and who are authorized to have the information.

Audit procedures:

12.2.1 Confirm that appropriate procedures have been issued regarding employees transferring sensitive information to other employees and individuals.

12.2.2 Confirm that procedures have been issued regarding the controls that are to be in place in Records Management facilities covering:

- the release of files containing sensitive information;
- the records to be maintained on the release and return of such files; and
- periodic verification by the DSO.

[7] Personnel are granted access only to the information and assets necessary to do their job.

12.2.3 Confirm that monitoring is conducted to ensure that Records Management facilities comply with the policy and procedures on the safeguarding, control, release, and return of files containing sensitive information.

12.2.4 Review a Records Management facility and:

- observe the process followed when files containing sensitive information are released;
- examine the records kept on the release of files containing sensitive information and verify that they are being maintained properly;
- select files containing sensitive information that have been charged out for an abnormally long period and confirm that there is an explanation for this; and
- select files containing sensitive information[8] that are charged out and verify that the employees to whom the files have been charged out have the files and have the appropriate enhanced reliability status or security clearance and that the files are secured in the appropriate security container when not used.

12.2.5 Confirm through sampling that employees are aware that they should check a recipient's clearance and need to know before releasing sensitive information.

[8] Select only files marked **TOP SECRET**, **SECRET**, and those designated extremely sensitive (i.e. **PROTECTED C**).

Objective 13

No one individual can independently control all aspects of a process or system (especially a security safeguard) (GSP Art. 10.8).

Audit procedures:

13.1.1 Confirm that the "separation-of-duties" principle, i.e. no one person can independently control all aspects of a process or system or bypass security safeguards, is embodied by the policies and procedures related to access to classified and protected information, including information, systems, and other assets.

13.1.2 Determine practices used by the DSO to confirm that the separation-of-duties principle is explained to personnel.

13.1.3 Determine practices used by the DSO to review and monitor implementation of the principle.

13.1.4 When separation of duties is not possible, determine how the DSO is made aware of such situations and whether adequate compensating controls or arrangements are in place.[9]

[9] Examples of compensatory control include the presence of two people when opening a vault and the requirement for two signatures on a cheque.

SHARING OF INFORMATION AND OTHER ASSETS

Objective 14

Appropriate safeguards are applied to sensitive information shared with or received from official sources outside the department. These official sources include foreign, provincial, territorial, and municipal governments, as well as international, educational, and private-sector organizations (GSP Art. 10.2).

Criterion 14.1 Written agreements or understandings are in place to provide for the safeguarding of sensitive information shared with other departments and other governments and organizations.

Audit procedures:

14.1.1 Obtain an overview of practices, policy, and procedures in place regarding the requirements for and the elements to be included in written agreements and understandings with:

- other governments and organizations about how they are to protect classified information being shared with them; and
- other departments about how they are to protect information designated as particularly sensitive[10] or extremely sensitive[11] that is shared with them on a regular basis.

14.1.2 Confirm that the DSO reviews the written agreements and understandings before they are signed to ensure that they are complete and comprehensive.

Criterion 14.2 An inventory exists of information shared with other government departments.

Audit procedures:

14.2.1 Confirm that the department can identify which Canadian and foreign federal, provincial, territorial, and municipal governments provide and receive sensitive information. This may be centralized under the DSO or may be decentralized to each functional group. The departmental *Information Classification Guide* and the Information Management or Information Holdings groups may provide guidance.

[10] The information might be marked **PROTECTED B** to indicate that it is particularly sensitive.

[11] The information might be marked **PROTECTED C** to indicate that it is extremely sensitive.

14.2.2 Confirm that there is a process for the DSO to comment on the continuing requirements and risks of sharing information with outside entities.

Criterion 14.3 Appropriate safeguards are applied to sensitive information shared with or received from official sources outside the department.

Audit procedures:

14.3.1 Confirm that the security standards and *Information Classification Guide* include instructions on how to protect sensitive information shared with or received from official sources outside the department and that they are being followed.

14.3.2 Confirm that security guidance states that sensitive information received from sources outside the department is not to be declassified or downgraded without the prior approval of the owners or originators of the information.

Objective 15

Processes and agreements are in place to confirm that information received from other official sources is protected, in accordance with the security policies and standards of the parties concerned (GSP Art. 10.2).

Audit procedures:

15.1.1 Confirm that periodic tests occur to ensure that individuals process information received from other official sources in accordance with instructions provided by those official sources.

15.1.2 Confirm that those individuals processing information received from other official sources are in possession of the instructions provided.

15.1.3 Confirm that any special handling instructions are the subject of security awareness briefings and/or correspondence.

PHYSICAL SECURITY

Objective 16

An appropriate security assessment is conducted prior to locating and designing facilities to reduce or eliminate the threats and risks to sensitive information, assets, and employees in the facilities (GSP Art. 10.11).

Criterion 16.1 Security requirements are considered when selecting sites and acquiring or constructing new facilities.

Audit procedures:

16.1.1 Obtain an overview of practices, policy, and procedures in place regarding the process to be followed in assessing the security requirements for:

- sites being selected for new facilities; and
- new facilities being acquired or constructed.

16.1.2 Review the policy and procedures and confirm that they are comprehensive and complete. Confirm that physical security safeguards meet security baselines at the planning stage, as outlined in supporting documentation.

16.1.3 Where proposed physical security safeguards are expected to exceed baselines, confirm that their implementation is justified by a TRA. Considerations include:

- whether the security implications of adjacent occupants have been considered in a TRA and security safeguards enhanced if necessary;
- whether control over easements has been confirmed during site selection and lease negotiation; and
- whether the risks and employee safety issues associated with parking areas have been considered in a TRA and security safeguards enhanced if necessary.

16.1.4 Confirm that judicious use is made of electronic intrusion detection, closed circuit video equipment and other technical access control devices (specify). Do not simply rely on employees or a guard force.

16.1.5 Confirm that the physical security specialists take the following approach:

- “protection” (barriers are in place to delay or deter unauthorized access)
- “detection” (unauthorized access is signalled)
- “response” (security incidents are reported to security specialists and corrective action is taken).

16.1.6 Confirm that custodian and tenant security responsibilities have been delineated and reconciled according to the physical security standard so that there are no gaps in protection. Confirm that there is a process whereby the custodian advises the tenant (typically the DSO) of all changes to facility operations so that a security assessment may be made.

Criterion 16.2 Briefs are prepared that identify the security requirements for site selection and facility design.

Audit procedures:

16.2.1 Confirm that a process is in place to inform the DSO of plans to acquire or construct new facilities.

16.2.2 Confirm that there is formal or informal security representation in the layout, design, selection, and modification of facilities.

16.2.3 Confirm that the DSO has a process in place to:

- have briefs prepared that identify the security requirements for site selection and facility design; and
- confirm that physical security measures comply with the relevant regulations and codes.

16.2.4 Confirm that the DSO approves all security specifications in planning documentation, requests for proposal, and tender documentation.

Criterion 16.3 Security requirements are considered at each design stage from concept drawings to completion.

Audit procedures:

16.3.1 Obtain an overview of the process in place that is used to:

- confirm that security site briefs and security design briefs are included in the architectural briefing documents;
- resolve differences between architectural design proposals and the security design briefs;
- review the continued application of security design briefs from the concept drawing stage through to the completion of new facilities and sign-off on the plans at each stage; and
- confirm that security inspections are carried out at facilities before they are occupied.

16.3.2 Select a sample of site plans to confirm they are reviewed and signed off by the DSO at critical stages of implementation.

16.3.3 Confirm whether security costs are captured separately from other facility design, selection, and construction. Confirm if the DSO has discretion in allocating security funds and resources to facility projects. In an interview with the DSO, determine any security implications of the allocation of security funding.

Objective 17

Appropriate physical safeguards are in place at facilities to provide for the safeguarding of sensitive information and assets, and the safety and security of employees (GSP Art. 10.11).

Criterion 17.1 A Treasury Board-approved site access clearance program is in place.

Audit procedures:

17.1.1 Confirm access to key facilities and restricted areas is controlled in accordance with a Treasury Board-approved site access clearance program implemented by the DSO.

17.1.2 Conduct sampling of sites to confirm that they are included in the site access clearance program.

Criterion 17.2 Employees and visitors are identified and their entry into a facility or zone is controlled and monitored by appropriate access control and monitoring systems, if necessary.

Audit procedures:

17.2.1 Obtain an overview of practices, policy, and procedures in place concerning identification procedures for employees and visitors at access control points. Review the policy and procedures with the DSO and confirm that the systems being used at different facilities meet the needs of the department.

17.2.2 Through sampling, confirm that:

- procedures have been issued regarding the control and use of identification cards, proximity cards, keys, or tokens at all facilities and action to be taken when cards are lost or stolen;
- personnel are individually accountable for these security items, including sanctions and charges for lost items, depending on the results of an investigation;
- all employees possess an employee identification card that, as a minimum, includes the name of the department, the bearer's photo, a unique card number, signature, and an expiry date;
- vendors and visitors are required to sign in before entering the facility and wear identification badges in the facility area;
- all visitors, vendors, and service personnel must be escorted;
- employees challenge persons in the facility if they are not properly badged; and

- the access pass system includes a method of issuing a temporary card to visitors and contractors that clearly identifies them as non-employees.

17.2.3 Confirm that policy and procedures have been issued regarding the use of access control and monitoring systems at facilities and restricted zones. Review the policy and procedures and discuss them with the DSO and confirm that the systems meet the needs of the department.

17.2.4 If access cards or access keys are used to control entry to facilities or security zones, confirm that policy and procedures have been issued regarding the "need to access" principle and the issue, retrieval, and cancellation of cards and keys.

17.2.5 Visit facilities and, through observation and interviews with employees, confirm that monitoring of the restricted zones is carried out according to procedures.

17.2.6 If security guards are used at facilities, determine the direction provided and training received. Confirm that they have been issued written post orders that have been approved by the DSO.

17.2.7 If electronic equipment is used for access control and/or monitoring at facilities or restricted zones, interview employees who operate the equipment to confirm that they are knowledgeable about it.

17.2.8 Confirm that procedures have been issued regarding the action to be taken when an access control system has been compromised.

17.2.9 Confirm that the DSO has oversight processes in place to ensure compliance with access control procedures.

Criterion 17.3 Sensitive information is stored in the appropriate containers listed in the *Security Equipment Guide*. (Exception: When the volume of information and assets is such that it is necessary to use an appropriate restricted zone.)

Audit procedures:

17.3.1 Obtain an overview of practices and procedures in place regarding the storage of sensitive information when it is not in use. Assess whether these procedures are readily accessible by all employees. Confirm that a process is in place to ensure that employees are made aware of the highest level of sensitive information that can be stored in the security containers to which they have access.

17.3.2 Confirm that the DSO has a process in place to ensure that sensitive information and assets are stored according to policy and procedures or that exceptions have been adequately assessed.

17.3.3 Review a Records Management facility and other facilities and, through interviews and observation, confirm that:

- sensitive information is stored in security containers appropriate for the types of zone in which the containers are located; and
- managers and employees are aware of the highest level of sensitive information that can be stored in the security containers used in their facility.

Criterion 17.4 Sensitive information and assets are transported and transmitted properly.

Audit procedures:

17.4.1 Obtain an overview of practices, policy, and procedures in place for the transportation and transmission of sensitive information. This is typically covered in the *Information Classification Guide*; if a departmental guide does not exist, there is guidance in the Secretariat's operational security standards.

17.4.2 Conduct a sampling of Records Management facilities to confirm that they are following the departmental or Secretariat standards.

Criterion 17.5 Sensitive information is destroyed using equipment listed in the *Security Equipment Guide*. (Exception: Low-sensitive designated information may be shredded by hand.)

Audit procedures:

17.5.1 Obtain an overview of the practices and procedures in place regarding the destruction of sensitive information. Review and assess whether these practices and procedures are reasonably comprehensive and complete.

17.5.2 Interview employees to determine their knowledge of and compliance with required practice for the destruction of sensitive information.

17.5.3 Confirm that all destruction equipment is included in the *Security Equipment Guide*. Where this is not the case, confirm that the DSO has authorized the use of other equipment.

17.5.4 Confirm that procedures have been issued regarding the maintenance of equipment used to destroy sensitive information and valued assets. Select equipment and verify that the process is being followed.

Criterion 17.6 Sensitive assets are controlled and safeguarded throughout their life cycle.

Audit procedures:

17.6.1 Obtain an overview of the practices and procedures in place regarding how sensitive assets are to be controlled and safeguarded from the time they are acquired until they are disposed of.

17.6.2 Obtain listings of different types of sensitive assets, such as laptop computers, electronic notebooks, personal digital assistants, Blackberries, and cellular telephones and review the specific controls and safeguards in place for these assets from the time they are acquired until they are disposed of. Select a sample of items to confirm their existence and ensure the integrity of lists.

17.6.3 Confirm that there is a process to review the safeguards and controls in place when sensitive assets are lost, stolen, or vandalized and to conduct an impact assessment.

17.6.4 Identify incidents where sensitive assets were lost, stolen, or vandalized and review the safeguards and controls in place when the incidents occurred and what action was taken to reduce the risks in the future.

Criterion 17.7 Appropriate physical security safeguards are implemented.

Audit procedures:

17.7.1 Confirm what access point protection is used in the facility, and that these safeguards are included in security baselines or are the result of a TRA, e.g.:

- physical barriers;
- acoustic baffles;
- break wire;
- infrared/photoelectric break beams;
- magnetic detectors;
- heat detectors;
- capacitance; and
- other (specify).

17.7.2 Confirm that there are monitors (e.g. closed circuit television, guards, etc.) and alarms for all key facility access points.

17.7.3 Confirm that electronic access logs are reviewed periodically for unusual activity. Confirm who conducts the review and whether the DSO is apprised of results.

17.7.4 Confirm that there is adequate control of keys and tokens. Are all keys, swipe cards, and proximity cards accounted for? Are all spare keys, swipe cards, and proximity cards secured, with limited access? Are all keys, swipe cards, and proximity cards logged in and out from the key press? Confirm the process and how it is audited for compliance.

17.7.5 Confirm that combinations to secure rooms and cabinets are kept confidential. Confirm there is a standard to this effect. Are combinations changed:

- when someone knowing the combination leaves;
- every six months;
- upon suspected compromise?

17.7.6 Confirm that logical and physical authorization lists and control mechanisms allowing facility entry are updated when a person's entry authority is revoked.

17.7.7 Confirm whether the following physical security measures are in place and justified by security baselines or a TRA:

- There is adequate perimeter lighting for observation and employee safety. Confirm that there is backup power for perimeter and key point lighting.
- All windows at ground level are either fixed or lockable with heavy-duty commercial hardware.
- All perimeter openings are protected against unauthorized entry.
- Warning signs are positioned at intervals of approximately 100 feet, are properly displayed, and are legible from a moderate distance.
- There is adequate emergency power to ensure safe evacuation (e.g. partial elevator service and emergency lighting).

Objective 18

A series of increasingly restrictive physical security zones is established and maintained with appropriate access control mechanisms to protect sensitive information and assets (GSP Art. 10.11).

Audit procedures:

18.1.1 Obtain an overview of practices and procedures in place regarding security zones and access control measures and procedures in establishing public, reception, operations, security, and high-security zones in facilities. Confirm that these measures are based on the results of a TRA. Confirm how the DSO monitors that the appropriate zones are established and maintained at facilities and assess the reasonableness of current practices.

18.1.2 Confirm that security boundaries are delineated and that current drawings, sketches, plans, or schematics of facilities are current and readily available, including:

- facility perimeter;
- topography;
- perimeter barriers;
- neighbouring facilities;
- entrance/exit points;
- facility and exterior roadways;
- facility locations;
- storage locations;
- emergency equipment locations and evacuation rendezvous;
- locations of doors, windows, and similar openings; and
- alarm placement and diagrams (schematics).

18.1.3 Assess the location of support and amenity areas (daycares, cafeterias, recreational areas, meeting areas, etc.) to ensure they are situated away from operational or sensitive areas.

Objective 19

A continuous review of physical security safeguards is conducted to reflect changes in the threat environment and to take advantage of new cost-effective technologies (GSP Art. 10.11).

Audit procedures:

19.1.1 Confirm who is responsible for conducting the continuous review. How are the results communicated to the DSO? What discretion does the DSO have in taking action to amend physical security safeguards to reflect changes in the threat environment and emerging technologies?

19.1.2 Determine what process is in place to have security consultations and inspections carried out at facilities. Confirm that the DSO receives the results of all security inspections.

19.1.3 Determine what security consultations and inspections were carried out in the department during the previous two years and confirm that recommendations were actioned by the DSO (either implemented or the reasons for not doing so are recorded). Confirm that the justification not to take action was approved by senior management.

19.1.4 Determine what process the DSO has in place for carrying out internal reviews of physical safeguards at facilities in addition to any formal consultations and inspections.

PERSONNEL SECURITY

Objective 20

All individuals with access to government assets (except for Governor in Council appointees) must have at least a reliability status (GSP Art. 10.9).

Criterion 20.1 Required checks are authorized, consented to, and completed before individuals occupy positions.

Audit procedures:

20.1.1 Review personnel screening files for different types and levels of screening and confirm that:

- the Personnel Screening Request and Authorization forms were completed and the required and optional checks were appropriately included;
- the checks were consented to by the individuals or their parents or guardians if they had not reached the age of majority;
- the checks were completed and the required type and level of screening was authorized before the individuals took up their positions; and
- the individuals signed the Security Screening Certificate and Briefing form.

20.1.2 Review the files for positions that require a security clearance and verify that the prerequisite screening requirements were completed before the security assessment was carried out.

20.1.3 Verify that a clearance level is assigned for each position in the department and that a process is in effect to confirm that no employees are granted access to sensitive information or valued assets unless they meet the access limitation requirements.

Criterion 20.2 Personnel doing business with the department possess the requisite security screening status.

Audit procedures:

20.2.1 Confirm that government employees accessing facilities have undergone at least a Basic Reliability Check.

20.2.2 Confirm that personnel accessing classified information have been granted a security clearance and that personnel accessing PROTECTED information have undergone an Enhanced Reliability Check.

20.2.3 Through sampling, confirm that employees are aware of their security screening status and that their status is current.

Objective 21

The security screening of individuals is carried out according to the GSP and Personnel Security Standard (GSP Art. 10.9).

Criterion 21.1 A security screening program is in place that complies with the GSP and the Personnel Security Standard.

Audit procedures:

21.1.1 Obtain an overview of practices and procedures in place regarding the security screening process and the required checks for each type and level of screening. Confirm they have been reviewed and approved by the DSO.

21.1.2 Review the policy and procedures and confirm that they are consistent with and comply with the GSP and Personnel Security Standard.

21.1.3 Interview managers and staffing personnel and confirm that they are familiar with the security screening process, including the requirement for employees to be clearable as a condition of employment with the government and the clearance requirements for specific positions within the department.

Criterion 21.2 The screening required to fill positions is identified and documented.

Audit procedures:

21.2.1 Review a percentage breakdown of the security screening types and levels authorized for employees and confirm that the percentages appear reasonable considering the department's mandate, as well as the types and quantities of sensitive information and valued assets held. If these quantities and types appear unusual, discuss the matter with the DSO and determine whether there is a reasonable explanation for this.

21.1.2 Interview managers and confirm how they decide the type and level of screening required for positions.

21.1.3 Review completed Classification Action forms, or similar forms in use and verify that the screening type and level were noted on them.

21.1.4 Interview the incumbents of positions and confirm the highest level of sensitive information that they handle and how frequently they handle it. Confirm that this is consistent with the type and level of screening that has been authorized for them. Confirm through interviews whether they understand their responsibilities for the protection of sensitive information under their control.

Criterion 21.3 A process is in place to upgrade and update the enhanced reliability status and security clearance of individuals when required.

Audit procedures:

21.3.1 Confirm that a centralized record is maintained of the screening types and levels authorized for employees and other individuals working in the department and the date that these were authorized. Confirm that the DSO has access to this record.

21.3.2 Confirm that procedures cover the process for the upgrading and updating of reliability status and security clearances and that they are consistent with and comply with the GSP and Personnel Security Standard.

21.3.3 Review the files for positions where the type and level of screening was upgraded and verify that the required checks were completed.

Criterion 21.4 Individuals are informed in writing of their right of access to review or redress processes when it has been decided to deny or revoke their reliability status or a security clearance.

Audit procedures:

21.4.1 Confirm that procedures have been issued requiring that individuals be informed in writing of their right to have a security decision reviewed when they are denied reliability status or a security clearance or when these are revoked and how the process can be initiated.

21.4.2 Review the files on denials and revocations of reliability status and security clearances during the previous two years and verify that individuals were informed in writing of their rights of access to review and redress processes.

Criterion 21.5 Records in a personnel security file are transferred or destroyed according to the GSP and the *National Archives of Canada Act.*

Audit procedures:

21.5.1 Obtain an overview of practices and procedures in place regarding the handling of records in a personnel security file, as it relates to an employee's transfer to a new department or an employee's retirement or separation. Consider the specific requirements for criminal records or other adverse information.

21.5.2 Compare and assess current practice with the GSP and the *National Archives of Canada Act* and determine whether:

- adverse information is removed from files and destroyed if the files are transferred to another department, except when the information is still valid and relevant;
- the DSO provides advice to senior management regarding removal of information from personnel files;
- the security screening records received by a department covering an employee on assignment or secondment are destroyed if the move does not take place or when the assignment or secondment is finished;
- the security screening records of retired or separated employees are destroyed according to the retention and disposal schedule of the *National Archives of Canada Act*.

Objective 22

Termination of an individual's employment is undertaken in a way that reduces or eliminates any risk to the department's sensitive information, systems, assets, or personnel (GSP Art. 10.9).

Audit procedures:

22.1.1 Obtain an overview of practices and procedures in place regarding the process that is to be followed when it has been decided to terminate the employment of an individual. Confirm that the process covers the following:

- recovering all physical security items, such as identification cards, access badges, tokens, keys, and locks;
- changing combinations known by the individual and removing authorizations on electronic systems; and
- completing a written record that these actions have been taken and forwarding this record to the DSO.

22.1.2 Review the files of individuals whose employment has been terminated and verify that the practices and procedures were followed.

22.1.3 Determine whether the procedures require that, when individuals are being terminated for cause, all electronic and physical accesses are terminated and individuals are immediately removed from any area where they may be a threat to any of the department's sensitive information and assets or essential systems. Confirm that a departmental employee arranges subsequent access to personal effects under escort.

PROTECTION OF EMPLOYEES

Objective 23

A threat and risk assessment (TRA) has been conducted to identify situations where employees are under threat of violence because of their duties or because of situations to which they are exposed (GSP Art. 10.10).

Audit procedures:

23.1.1 Confirm that threat scenarios involving employee safety have been developed and assessed as part of the ongoing TRA process within the department.

23.1.2 Confirm the security oversight process that the DSO has in place to monitor incidents involving the safety and security of employees and to review the adequacy of the safeguards at facilities where incidents occurred.

23.1.3 Review reports on incidents involving the safety and security of employees in the previous two years. Determine what safeguards were in place when the incidents occurred, recommendations made to address risk of future incidents, and the changes made in response. If recommendations were not acted on, assess the reasonableness of the justification provided and confirm the DSO's or senior management's approval.

Objective 24

Mechanisms are in effect to identify, protect, and support employees (and their families, as appropriate) under threat of violence or working in high-risk areas (GSP Art. 10.10).

Criterion 24.1 Policy and procedures have been issued and standards developed governing the safety and security of employees working in high-risk areas.

Audit procedures:

24.1.1 Review the policy, procedures, and standards and confirm that they are comprehensive and complete with respect to the protection of employees.

24.1.2 Confirm that the responsibilities of managers at all levels for the health and safety of employees at work is written and accessible.

24.1.3 Confirm that procedures have been issued and standards developed governing the safety and security of employees working in high-risk areas.

Criterion 24.2 Dangerous or potentially violent situations have been identified and measures taken to mitigate risks.

Audit procedures:

24.2.1 Confirm that an inventory has been drafted of job classifications and specific positions with the potential for danger to the health and safety of employees and/or that the types of danger are specified in job descriptions.

24.2.2 Confirm whether there is an executive protection program currently in place and, if so, who is protected under the program (list names and positions). Confirm whether the program is extended to family members.

24.2.3 Confirm who performs executive protection functions (list names and duties). Confirm the size of the executive protection staff. Confirm criteria are established for hiring executive protection personnel, e.g. background investigation, level of training, experience, etc.

24.2.4 Confirm that initial and periodic Occupational Safety and Health (OSH) briefings are provided to employees whose positions have been identified as being potentially dangerous. Confirm whether briefings are provided separately or as part of the departmental security program. Confirm whether the DSO is involved in either oversight or provision of OSH training.

24.2.5 Confirm that employees are encouraged to report all incidents of violence that they experience or witness. Determine if there is a "zero-tolerance" policy for workplace violence.

24.2.6 Confirm that all reported incidents are investigated promptly and that management, Human Resources, the DSO, and police authorities are advised, as appropriate.

24.2.7 Is there a formal or informal process for deciding to involve police authorities? Who is involved in the decision-making process (senior management, DSO, Human Resources, union representatives, etc.)?

24.2.8 Through sampling of selected incidents, confirm that thorough records are maintained of all investigated incidents. Who holds the records (Human Resources, DSO, etc.)? Confirm that an annual report to senior management is required and produced.

Criterion 24.3 Counselling and support is provided to victims of occupational or workplace violence.

Audit procedures:

24.3.1 Confirm that there is a program in place for the provision of counselling and support to employees and their families who have been victims of violence.

24.3.2 Determine how counselling arrangements are made. Is counselling provided automatically as part of an administrative process or must it be requested? Confirm that current practices ensure that counselling is provided in a timely fashion subsequent to an incident.

SECURITY AND CONTINGENCY MANAGEMENT

The BCP Program complements emergency preparedness that is mandated by legislation or government policy (*Operational Security Standard—Business Continuity Planning (BCP) Program*, Preamble).

Objective 25

Managers of facilities throughout the department have developed plans to protect sensitive information, assets, and employees during all types of emergencies and increased threat situations (GSP Art. 10.14).

Criterion 25.1 Managers of facilities have developed and documented plans to respond to different emergency situations.

Audit procedures:

25.1.1 Confirm that directives have been issued concerning the development of managers' plans to deliver critical services and protect associated assets during disruptive situations.[12]

25.1.2 Confirm that emergency and response plans have been developed for each facility and that there is a point of contact for each. Determine the means used to ensure that plans are harmonized and kept current.

25.1.3 Determine the process used by the DSO to confirm plans are current, logical, comprehensive, and complete.

25.1.4 Review a sample of the plans from facilities and confirm that they are reasonable, comprehensive, and complete.

Criterion 25.2 Emergency plans are maintained and tested.

Audit procedures:

25.2.1 Confirm that directives are issued regarding the regular update of emergency plans, the suggested frequency of testing of plans, and the nature of tests to be conducted (e.g. live or desk tests or both). What process does the DSO have in place to monitor the conduct of the tests?

25.2.2 Confirm that there are procedures permitting facility access to emergency personnel in case of fire, major power outage, or other emergency or disaster.

[12] Examples of such situations include fires, bomb threats, environmental disasters, attacks on employees, and demonstrations but are not restricted to only these.

25.2.3 Confirm that a process is in place to ensure that, as the security readiness levels increase, the degree of attention to detail also increases through more frequent checks of areas and stricter controls being applied to visitors and contractors. Confirm results of tests.

25.2.4 Confirm if there are plans and procedures for constituting and operating an Emergency Operations Centre (EOC). Confirm how the decision is made to open the EOC (who are the decision makers), and if the DSO is consulted.

25.2.5 Confirm that EOC members are adequately trained. Review the nature of training provided.

25.2.6 Test through sampling that the EOC call-out membership lists are current.

Criterion 25.3 A co-ordination process exists for all principal security staff (Corporate Security, IT Security, Business Continuity Planning (BCP), OSH, etc.) to move to heightened security levels under the direction of the DSO.

Audit procedures:

25.3.1 Confirm the existence of lines of communication between senior management and the DSO to order heightened security levels. Confirm whether they are formal or informal. Confirm whether the DSO is on the senior emergency management committee.

25.3.2 Confirm the existence of lines of communication between the DSO and the principal security staff to move to heightened security levels. Is there a security planning committee for emergency situations? Does the DSO chair this committee?

25.3.3 Confirm that plans allow for partial movement to heightened security levels. If the DSO is not the primary co-ordinator, then identify who is.

25.3.4 Identify the central point of contact for acting on direction from the government to implement heightened security levels.

Objective 26

Department-wide plans are developed to provide for the continuity of critical business operations, services, and assets following an unplanned interruption (GSP Art. 10.4).

Criterion 26.1 An effective business continuity program (BCP) is in place.

Audit procedures:

26.1.1 Obtain an overview of the BCP, as well as planning and monitoring activities.

26.1.2 Review policy and functional direction provided to confirm that the program:

- emphasizes overall responsibility and accountability for the BCP, including approval of priorities for business continuity, and recovery;
- identifies the BCP co-ordinator as program champion for the BCP;
- explains the functional relationship between the BCP co-ordinator and the DSO;
- describes intra-departmental structure to oversee, co-ordinate, and monitor the development and update of BCP;
- provides sufficient and appropriate direction by issuing related policy, procedures, and directives.

26.1.3 Interview the BCP co-ordinator and selected members of related senior management committees to confirm that different perspectives are taken into account. Consider the representation of the following functions in the program structure:

- audit;
- environment;
- finance;
- occupational safety and health;
- informatics;
- departmental business operations;
- corporate planning;
- materiel management;
- property and facilities management; and
- security.

Criterion 26.2 Appropriate business continuity plans have been developed and adequately documented to mitigate the risk of disruption of critical business functions.

Audit procedures:

26.2.1 Confirm that policies and procedures have been issued regarding the development of BCPs by managers to ensure continuity of critical business operations.

26.2.2 Obtain a corporate-level summary, if available, and other documentation and assess the adequacy of the department's challenges and readiness to address business continuity and recovery priorities. Confirm that a Business Impact Analysis (BIA) has been conducted to verify and prioritize the department's critical services and assets.

26.2.3 Confirm that there is an inventory of the department's essential services, programs, and operations. Who maintains the inventory and is there a formal or informal method for updates? Is the DSO made aware of all changes and updates? Interview the official responsible for business continuity planning and confirm that he or she is satisfied that all the essential business activities were identified.

26.2.4 Confirm that BCPs have been developed for all mission-critical systems and operations. Review a sample of them to ensure they are complete, comprehensive, and logical.

Criterion 26.3 BCPs are reviewed, tested, and subject to validation by the DSO.

Audit procedures:

26.3.1 Confirm that a process is in place to monitor the implementation of the BCP program, including the development and update of site-specific plans.

26.3.2 Confirm directives are issued on the update of BCPs and recommended frequency of tests and approach to testing (e.g. live or desk tests or both).

26.3.3 Select a sample of BCPs to confirm that they are subject to periodic update and testing.

26.3.4 Obtain a copy of a recent status report as prepared for senior management. Test the accuracy and completeness of the information provided by comparing the report contents to the sample previously tested.

SECURITY AND CONTRACTING MANAGEMENT

Objective 27

Security requirements for the protection of information, assets, and personnel are addressed as part of the contracting process (GSP Art. 10.4).

Criterion 27.1 Security requirements are considered when entering into contracts and are described in documents provided to contractors throughout the contracting process.

Audit procedures:

27.1.1 Obtain an overview of how security requirements are addressed throughout the contracting process.

27.1.2 Review the policy and procedures regarding security requirements in contracts involving sensitive information and assets and confirm that they are comprehensive in their coverage and address requests for contracts, bidding, negotiating, awarding, performance evaluation, and termination of contracts.

27.1.3 Confirm that the policy indicates that contracts involving foreign contractors having access to sensitive Canadian government information and assets or contracts involving sensitive foreign government information must be processed through Public Works and Government Services Canada (PWGSC).

27.1.4 Review a sample of contract files involving sensitive information and assets and confirm that the necessary security requirements were included in all applicable documents.

Criterion 27.2 Monitoring activities are in place to ensure that security requirements are met throughout all phases of the contracting process.

Audit procedures:

When PWGSC is the contracting authority

27.2.1 Confirm that the policy and procedures require the use of the Security Requirements Checklist (SRCL) for all contracts involving sensitive information and assets where PWGSC is the contracting authority.

27.2.2 Test a sample of files handled by PWGSC and confirm that the SRCL is on file and duly completed.

When the department is the contracting authority

27.2.3 Obtain an overview explaining what is done to confirm that contractors have met the security requirements.

27.2.4 Confirm that the policy explains the circumstances under which the department requests that PWGSC ensures that the security requirements have been met.

27.2.5 Review a sample of contract files where the department accepted full responsibility for ensuring that the contractors met the security requirements and confirm that:

- the contractors' status was checked with PWGSC at the start of the process;
- the contractors did not start the contracts before the security requirements were met;
- PWGSC was informed when the contractors had met all security requirements; and
- adequate documentation to confirm that the contractors met the security requirements is on file.

27.2.6 Confirm that processes are in place for carrying out scheduled inspections of contractors' work sites, when this is applicable. Confirm that there is a process for the DSO to co-ordinate inspections and be informed of the results.

Criterion 27.3 All contractors are subject to the departmental security policy.

Audit procedures:

27.3.1 Confirm that a current list is maintained of contractors working for the department. Confirm that the DSO has access to this list and the security screening level of each contractor (required and actual).

27.3.2 Confirm that there is a process in effect to inform the DSO that contractors have received the necessary security briefings and have access to departmental security policy and supporting documentation.

27.3.3 Confirm that there is a process in effect for the DSO to ensure that the necessary security requirements are included in terms and conditions in any contractual documentation.

APPENDIX A—AUTHORITIES AND REFERENCES

The authority for the GSP derives from a government decision and section 7 of the *Financial Administration Act*.

http://laws.justice.gc.ca/en/F-11/index.html

Relevant legislation is referenced in section 13 of the GSP.

Policy and standards

Government security—first-tier policy and second-tier operational security standards
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_12a/siglist_e.asp

Government policies and guidelines relevant to the GSP

Access to Information
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_121/siglist_e.asp

Policy on Electronic Authorization and Authentication
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/tbm_142/2-2_e.asp

Policy on Losses of Money and Offenses and Other Illegal Acts Against the Crown
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/tbm_142/4-7_e.asp

Privacy and Data Protection
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_128/siglist_e.asp

Risk Management Policy
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/riskmanagement/siglist_e.asp

Contracting Policy
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/contracting/siglist_e.asp

Government security—third-tier technical documentation and guidelines for physical security

Construction of a Special Discussion Area (SSB/SG-21), August 1988

Construction Specification for Secure Room C (SSB/SG-23), March 1991

Construction Specification for Secure Room D (SSB/SG-22), March 1991

Cross-Stairwell Barriers (SSB/SG-13), November 1987

Doors and Frames (SSB/SG-16), March 1985

Entry Controls for Overhead Doors (SSB/SG-9), December 1981

Exterior Fixed-Ladder Barrier Specification (SSB/SG-8), August 1987

Glazing (SSB/SG-11), February 1988

Guide to Managing Guard Services (SSB/SG-29), May 1993

Guide to Preparation of Physical Security Briefs (SSB/SG-25), October 1992

Hardware (SSB/SG-15), February 1985

Identification Cards / Access Badges (SSB/SG-27), June 1992

Master Key Systems (SSB/SG-10), December 1981

New Construction to Provide Speech Privacy (SSB/SG-12), December 1986

Overhead Door Specifications (SSB/SG-4), August 1987

Security Connotations of the 1980 National Building Code (SSB/SG-14), September 1983

Security Connotations of the 1985 National Building Code (SSB/SG-26), March 1990

Sound Control (SSB/SG-3), January 1981

Security Control Room Space Requirements (SSB/SG-7), July 1987

Security Design Brief for RCMP Buildings (SSB/SG-18), August 1988

Security Design Brief: General Purpose Office Buildings (SSB/SG-19), November 1987

Security Equipment Guide (SSB/SG-20), October 1992 (distribution restricted to federal government departments and not available electronically)

Security Lighting (SSB/SG-2), August 1987

Security Sealing of Building Emergency/Master Keys or Cypher Lock Codes (SSB/SG-28), March 1991

Standard for the Transport and Transmittal of Sensitive Information and Assets (SSR/SG-30), June 1994

Suspended Ceiling Systems (SSB/SG-6), August 1987

Vaults (SSB/SG-17), March 1985

Common-use and operational signs, Appendix A, Standard Signs, *Federal Identity Program Manual*, Treasury Board of Canada Secretariat, March 1990

Guidelines for Dealing with Security Incidents and Securing HRD Premises (Security Bulletin No. 92-1), Human Resources Development Canada, 1992

Personal Security and Service to the Public, Human Resources Development Canada, 1994

Stocked Items Supply (SIS) catalogue, Public Works and Government Services Canada, no date

APPENDIX B—GLOSSARY

Access badge *(insigne d'accès)*—document issued by a department to indicate the zone or facility to which the bearer has authorized access

Access key *(clé d'accès)*—method used by a department to authorize a person to pass through an access control point at a facility or a security zone, for example, physical characteristics, personal knowledge and/or a device

Accreditation *(accréditation)*—approval by the responsible manager for an information technology system to operate using a particular set of safeguards

Availability *(disponibilité)*—the condition of being usable on demand to support business functions

Basic reliability check *(vérification de base de la fiabilité)*—an assessment to confirm the trustworthiness of individuals; condition for being granted basic reliability status

Basic reliability status *(cote de fiabilité de base)*—the minimum type of personnel screening; allows access to non-sensitive information and assets only

Breach of security *(infraction à la sécurité)*—any compromise, including probable compromise, of sensitive information, and/or assets

Business continuity planning *(planification de la continuité opérationnelle*)—an all-encompassing term that includes the development and timely execution of plans, measures, procedures, and arrangements to ensure minimal or no interruption to the availability of critical services and assets

Business hours *(heures d'ouverture)*—posted hours when reception zones are open to the public and when an authorized person or visitor may access the controlled area

Classification and designation guide *(guide de classification et désignation)*—a corporate document, approved by the deputy head of a department or head of an agency, that shows the various types of information that must be either classified or designated

Classified assets *(biens classifiés)*—assets, other than information, that are important to the national interest and therefore warrant safeguarding

Classified information *(renseignements classifiés)*—information related to the national interest that may qualify for an exemption or exclusion under the *Access to Information Act* or the *Privacy Act*, the compromise of which would reasonably be expected to cause injury to the national interest

Compromise *(atteinte à l'intégrité)*—unauthorized disclosure, destruction, removal, modification, or interruption of sensitive information and assets

COMSEC *(COMSEC)*—protection resulting from applying cryptographic, transmission, and emission security measures to telecommunication emissions and information handling equipment and from applying other measures appropriate to COMSEC information and material

Confidential *(confidentiel)*—level of classification that applies to information and assets when compromise could reasonably be expected to cause injury to the national interest; in capital letters, a mark to indicate level of sensitivity

Confidentiality *(confidentialité)*—the sensitivity of information or assets to unauthorized disclosure, recorded as classification or designation, each of which implies a degree of injury should unauthorized disclosure occur

Consequence *(conséquence)*—outcome, effect; used synonymously with impact

Container *(coffre)*—any enclosure, including a cabinet or a room, for the storage of information and assets

Contingency planning *(planification des cas d'urgence)*—the process of developing a plan to restore information technology operations in the event of a disruption

Contracting process *(Processus de passation des marchés)*—includes bidding, negotiating, awarding, performance, and termination of contracts

Controlled area *(lieu contrôlé)*—an area comprised of any combination of the three restricted zones

Custodian departments *(ministères gardiens)*—departments having responsibility for the administration of a facility assigned to other departments for the conduct of government programs

Data *(données)*—a representation of facts, concepts, or instructions arranged in a formalized manner suitable for telecommunications, interpretation, or processing by people or by automated means

Declassification *(déclassification)*—the decision, recorded in writing, of the originator of classified information or another officer authorized by the deputy head or head of a department or agency, to remove the classified status of information

Defence of Canada or any state allied or associated with Canada *(défense du Canada ou de tout État allié ou associé)*—includes the efforts of Canada and of foreign states to detect, prevent, or suppress activities of any foreign state directed toward actual or potential attack or other acts of aggression against Canada or any state allied or associated with Canada

Department *(ministère)*—any federal institution subject to the *Government Security Policy* (GSP)

Departmental security officer *(agent de sécurité du ministère)*—the individual responsible for developing, implementing, maintaining, co-ordinating, and monitoring a departmental security program consistent with the GSP and operational security standards

Designated assets *(biens désignés)*—assets, other than information, that have been identified by the department as being important to operations by virtue of the function performed or as being valuable and therefore warranting safeguarding; for example, cash and other negotiables, as well as information technology systems that require protection to ensure the confidentiality, integrity, and availability of the information stored in them

Designated information *(renseignements désignés)*—information related to anything other than the national interest that is of low sensitivity, particularly sensitive, or extremely sensitive and that may qualify for an exemption or exclusion under the *Access to Information Act* or the *Privacy Act*

Designation guide *(guide de désignation)*—See ***Classification and designation guide***.

Downgrading *(déclassement)*—the decision, recorded in writing, of the originator of sensitive information or another officer authorized by the deputy head or head of a department or agency, to lower the classification level of information or remove the designated status

Effectiveness *(efficacité)*—a term used in value-for-money auditing, referring to the achievement of the objectives or other intended effects of programs, operations, or activities

Efficiency *(efficience)*—a term used in value-for-money auditing, referring to the use of financial human and physical resources in a manner that maximizes resources inputs for any given quantity of output ***Enhanced reliability check*** *(vérification approfondie de la fiabilité)*—

an assessment to confirm an individual's trustworthiness; condition for enhanced reliability status

Enhanced reliability status *(cote de fiabilité approfondie)*—the type of personnel screening that, with a need to know, is required for access to designated information and assets

Extremely sensitive, designated information *(renseignements désignés de nature extrêmement délicate)*—a subset of designated information that could reasonably be presumed to cause extremely serious injury, such as loss of life, if compromised; may be marked PROTECTED C

Facility *(installation)*—This refers to a physical setting used to serve a specific purpose. A facility may be part of a building, a whole building, or a building plus its site or it may be a construction that is not a building. The term encompasses both the physical object and its use.

For cause *(avec motif)*—This is a determination based on available information that a greater degree of screening is required. This may be confirmed by the department or the investigative agency in individual cases or jointly for a particular group or category.

Functional reporting relationship *(rapport hiérarchique fonctionnel)* —This is a reporting relationship between individuals such that the subordinate individual is *not* in the organization of the manager but has been assigned specific duties to the manager of another organization, due to the subordinate's unique expertise. These duties are limited in scope and typically feature attendance at meetings and working groups, participation in committees, and routine reporting of statistics. The subordinate in a functional reporting relationship may be put under a line relationship to the manager of another organization during emergency and increased threat situations.

High-security Zone *(zone de haute sécurité)*—This is an area to which access is controlled through an entry point and limited to authorized, appropriately screened personnel and authorized and properly escorted visitors. The zone should be accessible only from security zones and separated from security zones and operations zones by a perimeter built to the specifications recommended in the TRA. Monitoring is 24 hours a day and 7 days a week by security staff, other personnel, or electronic means.

Identification card *(carte d'identité)*—document issued by a department to identify the bearer as an employee of that department

Information holdings *(renseignements détenus)*—This refers to all information under the control of a department, regardless of physical mode or medium in which the information is stored.

Materials held by federal libraries that were not prepared or produced by or for the government are excluded from this definition.

Information technology security *(sécurité des technologies de l'information)*—the protection resulting from an integrated set of safeguards designed to ensure the confidentiality of information electronically stored, processed, or transmitted; the integrity of the information and related processes; and the availability of systems and services

Integrity *(intégrité)*—the accuracy and completeness of information and assets and the authenticity of transactions

Interruption *(interruption)*—the non-availability of information, assets, systems, or services; interruption can be accidental or deliberate

Lead agency *(organisme-conseil)*—an agency with government-wide responsibilities related to the GSP, as defined in the GSP

Line reporting relationship *(rapport hiérarchique)*—This is a reporting relationship between individuals such that the subordinate individual is in the organization of the manager. Typically, the manager is responsible for assigning work to the subordinate individual, looking after the subordinate's well-being and professional development, and assessing the subordinate individual.

Limited-access hours *(heures d'accès limité)*—periods outside business hours when access to the reception zones and controlled area is limited to authorized persons, usually employees, and by exception to authorized visitors

Low-sensitive, designated information *(renseignements désignés de nature peu délicate)*—a subset of designated information that could reasonably be presumed to cause injury if compromised and that may be marked PROTECTED A

Modification *(modification)*—the alteration of information, data, software, or IT equipment, whether accidental or deliberate

Monitor *(surveiller)*—to ensure that information and assets or the safeguards protecting them are checked by the personnel in control of the information or assets, security staff, or electronic means with sufficient regularity to satisfy the TRA

National interest *(intérêt national)*—concerns the defence and maintenance of the social, political, and economic stability of Canada

Need-to-access principle *(principe d'accès sélectif)*—limiting access to a specific area to those who need to work there

Need-to-know principle *(principe de connaissance sélective)*—limiting access to information to those whose duties require such access

Open-office area *(bureau à aires ouvertes)*—an office comprised of many work stations not separated by doors and walls

Operations zone *(zone de travail)*—an area where access is limited to personnel who work there and to properly escorted visitors and that should be monitored periodically, based on a TRA, and should preferably be accessible from a reception zone

Organizations *(organisations)*—organizations not subject to the GSP, including international organizations, such as the North Atlantic Treaty Organization

Other governments *(autres gouvernements)*—includes municipal, regional, and provincial governments, as well as those of other nations

Particularly sensitive, designated information *(renseignements désignés de nature particulièrement délicate)*—This is a subset of designated information that could reasonably be expected to cause serious injury if compromised; it may be marked PROTECTED B.

Personal information *(renseignements personnels)*—This refers to any form of recorded information about an identifiable individual. See section 3 of the *Privacy Act* for examples. The Act also includes some exceptions to the definition. Personal information, a subset of other sensitive information, deserves enhanced protection and may carry the marking "PROTECTED—personal information."

Physical security *(sécurité matérielle)*—protection, detection, and response mechanisms used in the physical environment to control access to sensitive information and assets

PROTECTED *(PROTÉGÉ)*—the marking that shows that the information qualifies as designated information and requires more than basic protection

Public zone *(zone publique)*—This generally surrounds or forms part of a department facility. Examples include the grounds surrounding a facility, public corridors, and elevator lobbies in a multi-occupancy facility.

Reception zone *(zone d'accueil)*—This is the area located at the entry to the facility where the initial contact between the public and the department occurs, where services are provided,

information is exchanged, and access to restricted zones is controlled. Access by the public may be limited to specific times of day or for specific reasons. Monitoring is, to varying degrees, done by personnel who work there, by other personnel, or by security staff.

Removal *(suppression)*—This refers to loss of information or assets. Loss can be accidental, as when information is discarded with waste, or deliberate, as in the case of theft.

Restricted zones *(zones restreintes)*—operations, security, and high-security zones

Risk *(risque)*—(i) chance of vulnerabilities being exploited; (ii) uncertainty

Risk assessment *(évaluation des risques)*—an evaluation, based on the effectiveness of existing or proposed security safeguards, of the chance of vulnerabilities being exploited

Secret *(secret)*—level of classification that applies to information or assets when compromise could reasonably be expected to cause serious injury to the national interest

Secure perimeter *(périmètre de sécurité)*—continuous physical barriers that can reasonably be expected to counter identified threats

Security assessment *(évaluation sécuritaire)*—an appraisal of loyalty to Canada and, so far as it is related thereto, the reliability of an individual; condition for a security clearance

Security clearance *(cote de sécurité)*—the type of personnel screening that, with a need to know, is required for access to classified information and assets

Security design brief *(énoncé de la conception de la sécurité)*—describes the physical security concept and the layout of restricted zones developed in response to a TRA

Security equipment *(équipement de sécurité)*—This is equipment that has been evaluated or tested against standards developed by the lead agency. The *Security Equipment Guide* lists security equipment for use in the Government of Canada.

Security guard *(garde de sécurité)*—person whose primary duties involve the protection of information and assets

Security incident *(incident de sécurité)*—includes a breach and violation of security and any other occurrence reflecting on the safeguards or measures in place to protect sensitive information and assets

Security inspection *(inspection de sécurié)*—routine checks of sites where sensitive information is processed or stored by personnel or security guards (where employed) at the end of normal working hours

Security site brief *(énoncé de sécurité du site)*—a document that lists the site attributes to be considered when determining the location of a facility

Security standard *(norme de sécurité)*—This refers to the level of security regarded as a measure of adequacy, as well as security requirements and guidelines approved for government-wide use. (Operational security standards form part of the *Treasury Board Manual*; technical standards are produced by the lead security agencies.)

Security zone *(zone de sécurité)*—This is an area to which access is limited to authorized personnel and to authorized and properly escorted visitors. The zone should preferably be accessible from an operations zone and through an entry point but not necessarily separated from the operations zone by a secure perimeter. Monitoring is 24 hours a day and 7 days a week by security staff, other personnel, or electronic means.

Sensitive assets *(Biens de nature délicate)*—classified assets and designated assets

Sensitive discussion area (SDA) *(aire insonorisée)*—specially designed and managed area to prevent the overhearing, by electronic or other methods, of discussions on classified and designated information

Sensitive information *(renseignements de nature délicate)*—classified or designated information

Service spaces *(aires de service)*—areas such as cloakrooms, toilets, cafeterias, circulation routes, registries, as well as building service areas, such as telephone, electrical, and janitorial closets

Site-access security clearance *(cote de sécurité donnant accès aux sites)*—type of personnel screening required in limited and specific circumstances when duties of individuals require access only to sensitive government-related sites or facilities, usually for a short time, and not to information

Sponsoring department *(ministère tuteur)*—a department that makes submissions to the Treasury Board for approval of project objectives and expenditure authority and that is responsible for managing the project

Statement of sensitivity *(énoncé de la nature délicate)*—a description of the confidentiality, integrity, or availability requirements associated with the information or assets stored or processed in or transmitted by an information technology system

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

Threat assessment *(évaluation de la menace)*—an evaluation of the nature, likelihood, and consequence of acts or events that could place sensitive information and assets at risk

Top secret *(très secret)*—level of classification that applies to information or assets when compromise could reasonably be expected to cause exceptionally grave injury to the national interest

Value *(valeur)*—estimated worth

Violation of security *(manquement à la sécurité)*—This refers to any act or omission that contravenes any provision of the GSP. Such acts may include failure to classify or designate information in accordance with the policy; classification or designation, or continuation of same, in violation of the GSP; unauthorized modification, retention, destruction, or removal of sensitive information; and unauthorized interruption of the flow of sensitive information.

Vulnerability *(vulnérabilité)*—inadequacy related to security that could permit a threat to cause harm