CyberSecurity

THE AMITA. APPROACH

SECURITY AND PRIVACY OFFERING

The Government of Canada (GoC) depends on their personnel and assets to deliver services that ensure the health, safety, security and economic well-being of Canadians. It must manage these resources with due diligence and take appropriate measures to safeguard them from injury.

Federal departments and agencies must design and implement security programs that will protect their employees; preserve the confidentiality, integrity, availability and value of their assets; and ensure the continued delivery of services.

To achieve this, **AMITA** can assist organizations to develop and implement comprehensive security and privacy program frameworks to address their security and privacy requirements and accountabilities. One of the key required elements of the framework is a **security & privacy governance structure**, to support the delivery and oversight of their security and privacy programs.

AMITA Capability and Services

AMITA can both assess and assist with the identification and development of governance and accountability requirements for security and privacy contained in the federal PGS and its related operational security standard for the Management of Information Technology Security (MITS) and TBS Privacy Policy and Guidelines.

AMITA will also take into consideration the best practices as followed in the security industry. Although the PGS and MITS standard provide central guidance on the organization and structure needed for departmental security programs, each department must ensure through its own internal structures, policies, standards and procedures that its security requirements are addressed and delivered effectively.

In order to provide a balanced and effective security and privacy program, the following governance and program requirements need to be addressed. AMITA has the experience and the expertise, both technical and management consulting capability, to evaluate and recommend governance options supported by process and framework coverage that would address overall accountability, senior management oversight and the roles and responsibilities to properly discharge expectations of central GoC bodies such as TBS and Lead Agencies such as CSEC and PWGSC.

Governance & Accountability Overview

Organizations are responsible for the organization and management of an effective security and privacy program that meets the requirements of the Policy on Government Security (PGS) and the GoC Privacy Policy and Guidelines, the Treasury Board *Standard on the Management of IT Security*, departmental operational needs and is consistent with industry best practices.

A fundamental principle of the PGS is the accountability for security within departments or agencies. The accountability rests with the Deputy Head or their equivalent. *Deputy heads* are accountable for safeguarding employees and assets under their area of responsibility and for implementing federal government policies, including the PGS.

If organizations are to implement 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 PGS recognizes these facts by defining broad requirements to ensure a certain level of security within a department or federal agency or the government as a whole, while allowing the discretion required to respond to unique (or specialized) financial and business needs, as well as operational conditions.

Overall Accountability – Within the federal government, overall accountability for security and privacy rests with departmental *Deputy Heads*. They are accountable for safeguarding employees and assets under their area of responsibility and for implementing the government privacy and security policy and related standards.

Senior Management - One of the roles of senior management is to foster a "culture of privacy and security" across the department. They do so by ensuring that privacy and security requirements are addressed when defining the department's priorities, strategic directions, program objectives, budget and personnel allocations. They ensure adequate funding for privacy and security in Information Technology (IT) and other projects, and they approve departmental privacy and security policies, standards and directives.

Departmental Privacy and Security Officer (DPSO) - The PGS requires departments to appoint a Departmental Privacy and Security Officers (DPSOs) to establish and direct a privacy and security program (s) that ensures co-ordination of all policy functions and the implementation of policy requirements. In addition, the PGS suggests that, given the importance of this role, consideration should be given to appointing a Departmental Privacy and Security Officers with sufficient privacy and security experience who is strategically positioned within the organization so as to provide department-wide strategic advice and guidance to senior management.

Chief Information Officer (CIO) - The PGS and MITS require that departments designate an individual to perform the functions of a Chief Information Officer. This individual is responsible for ensuring the effective and efficient management of the department's information and IT assets. Given the potential impact of service delivery failures due to privacy and security breaches, the *Chief Information Officer, the PSO and DSO and the IT Security Coordinator* must work together to ensure that appropriate security measures are applied to all departmental assets, activities and processes.

Business Continuity Planning Coordinator – Departments must establish a business continuity planning (BCP) program to provide for the continued availability of critical services and assets.

The Chief Information Officer, Departmental Privacy and Security Officer (s), IT Security Coordinator and the Business Continuity Planning Coordinator must work together to ensure a comprehensive approach to continuous service delivery.

Protection of Employees – Departments are responsible for the health and safety of employees at work. This responsibility extends to situations where employees are under threat of violence because of their duties or because of situations to which they are exposed.

Physical Security - Physical security involves the proper layout and design of facilities and the use of measures to delay and prevent unauthorized access to government assets. It includes measures to detect attempted or actual unauthorized access and to activate an appropriate response. Physical security also provides measures to safeguard employees from violence.

Personnel Security Screening – Federal government organisations must ensure that individuals with access to government information and assets are reliable and trustworthy. Special care must be taken to ensure the continued reliability and loyalty of individuals and to prevent malicious activity and unauthorised disclosure of classified and protected information by a disaffected individual in a position of trust. Departments must ensure that, prior to the commencement of duties, individuals who require access to government assets undergo a reliability check and are granted a reliability status; and that those who require access to classified information and assets have a valid reliability status, undergo a security assessment and are granted a security clearance at the appropriate level.

Security Education and Awareness – A robust education program is required to support implementation of the privacy and security program in any organisation. This requires education and awareness for senior management, for business and program officials and for privacy and security practitioners and project staff. Departments must:

- Ensure that individuals who have specific privacy and security duties receive appropriate, up to date training.
- Have a privacy and security awareness program to inform and regularly remind individuals of their responsibilities, issues and concerns.
- Brief individuals on the access privileges and prohibitions attached to their screening level prior to commencement of duties.

Information Technology Security – Privacy drivers and other aspects require information systems to be secured against rapidly evolving threats that have the potential to impact their confidentiality, integrity, availability, intended use and value. To defend against these threats, an IT security strategy is required that accommodates changes in threat conditions, and supports the continuous delivery of services. This dictates that departments apply baseline security controls, continuously monitor service delivery levels, track and analyse threats to departmental IT systems, and establish effective incident response and IT continuity mechanisms.

IT Security for IT Projects - Departments must ensure that IT security is an integral part of each stage in the system development life cycle. Security requirements and related funding must be identified and included in planning, requests for proposals, and tender documents for IT projects.

AMITA has the necessary experience in applying security design, implementation and test requirements in s/w products and in their implementation into information systems that applying the broader IT Security safeguards at the conceptual, logical and physical stages of projects is well understood and can be provided as a service to clients.

The *PGS* and *MITS* require that the following specific roles be established/addressed as part of an organization's IT security program:

- **IT Security Coordinator** - Departments must appoint an IT Security Coordinator with at least a functional reporting relationship to both the departmental CIO and DSO.
- **IT Operational Personnel** - IT operational personnel includes network or system administrators or managers, help desk personnel, account managers, system security, maintenance and all other IT support personnel. Under the general direction of the IT Security Coordinator and in accordance with departmental priorities, policies and procedures.
- **IT Project Managers** - IT project managers must ensure, with guidance from the IT Security Coordinator and IT operational personnel, which project security requirements are met through the development and implementation of technical security specifications.
- **COMSEC Custodian** - Departments that hold classified cryptographic material, controlled cryptographic items or "accountable" publications require a COMSEC (Communications Security) account. These departments must appoint a COMSEC custodian (and an alternate, if required) to account for this material, items and publications in accordance with Communications Security Establishment instructions.

Information Management – departments must address the following security requirements and controls with regards to the identification and protection of their information:

- **Classification of Information** - In order to protect their information, departments must first identify and classify the information accurately by applying risk impacts. This process is essential to identifying departmental security priorities and helps in determining the graduated application of controls and safeguards.
- **Access to Sensitive Information Assets** – Departments must limit access to classified and protected information and other assets to those individuals who have a need to know the information and who have the appropriate security screening level.
- **Sharing of Information** - Departments must implement and comply with the PGS when sharing GoC information and other assets with other governments (including foreign, provincial, territorial, and municipal), international, educational and private sector organizations. In these cases, departments must develop arrangements that outline security responsibilities, safeguards to be applied, and terms and conditions for continued participation.

Audits & Monitoring – Departments are required to conduct active monitoring and internal audits of their security program. Internal and/or 3rd party audit is a necessary component of any security posture. The purpose of regular audits is to determine the effectiveness of policy and to allow for the correction of any ineffective policies or procedures. AMITA's capability in auditing to requirements such as ISO 17799 and ISO 27001, Scorecard Audits, s5970 and s5025, can assist departments in ensuring their security and privacy programs meet legislative and regulatory requirements and that control objectives and measurements have the proper coverage.

Investigation of Security Incidents – Departments must develop procedures for reporting and investigating security incidents when they occur, to determine impact and take corrective action, and to reduce the risk of future occurrence.

Security Risk Management – Departments must conduct ongoing assessments of threats and risks to determine the necessity of safeguards beyond baseline levels. They must continuously monitor for any change in the threat environment and make any adjustment necessary to maintain an acceptable level of risk and a balance between operational needs and security. AMITA is well versed in the necessary approaches and methodologies in assessing risk and recommending remedial measures to assist departments in continuous risk management.

Security in Emergency and Increased Threat Situations – Organizations must be able to identify and adjust to changing threat situations, recognizing that they are still obliged to meet security requirements during emergency situations. The changing threat environment must be tracked and protective programs must quickly adjust to minimize the exposure of departmental assets, to ensure safe and secure delivery of services and maintain confidence in program capability.

Departmental Security Procedures - apply to a host of activities in the security program area. These procedures detail how things are done. They are required to support both security policy and security standards.

Program and Service Delivery Managers -- On behalf of the department's Deputy Head, *program and service delivery managers* are responsible for ensuring an appropriate level of security for their programs and services. In designing programs and services, managers will work with departmental security specialists to manage the risk associated with their programs or services, by ensuring that security requirements (as per the *PGS*, the *MITS standard* and other related policies, standards and technical documentation) have been identified and addressed, and accepting the associated residual risk. With its experience in traditional Project Management and in operational Project Management, AMITA can assist at the program and delivery stages to assist departmental management in meeting budget and scheduling requirements.

Role of Other Personnel - All personnel must abide by the Government's and the department's IT security policy, procedures and other related documentation. They must report real and suspected security incidents to designated security officials, normally through their immediate supervisor.

Privacy and Security Committee Oversight - Although the *GSP* or *MITS* standard does not specifically identify the need for a committee to deal with the security function, it is clear that a security and privacy steering committee will add significant benefit to an organization's security governance structure. Such a committee made up of representative high-level managers and specifically mandated to provide oversight to the privacy and security function is commonplace in most organizations and is considered an industry best practice. AMITA has experienced consultants that can recommend Terms of reference to address oversight requirements.

Reporting and Support Structure – AMITA, once having assessed current governance and accountability structures, can recommend both a Terms of Reference for the Steering Committee and can make recommendation on the reporting and support structures that will be workable options for the department.