CyberSecurity

THE AMITA. APPROACH

PROJECT & SYSTEM SECURITY ASSESSMENT & IMPLEMENTATION OFFERING

Canada's Cyber Security Strategy spells out the increasing dependency that government, industry, and individuals have on using cyberspace to exchange digital information, resulting in vulnerability and economic collapse if faced with a disruption to this medium through cyber-attack. The Canadian Cyber Security Strategy is built on three pillars; AMITA directly addresses the pillar of securing Government systems.

With over 25 years of experience in IT services and developing business solutions that are IT-enabled, with security top of mind, AMITA has been supporting the securing of information as a partner of the Canadian government intelligence, public safety and defence agencies since 2002.

AMITA Capability

Departments and agencies are responsible for organizing and managing an effective security and privacy program. Departments must meet 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 (MITS),* departmental operational needs and be consistent with industry best practices. ITSG-33 guidance, provided by CSEC, outlines an approach where IT security activities are orchestrated at two distinct levels in the organization: the departmental level and the information system level. It has full System Development Life Cycle (SDLC) integration and better support of IT-enables projects. ITSG-33 was published in November 2012 and replaces the current guidance MG-2 and MG-4.

Project Management Offices (PMO) and Enterprise-wide PMO's (e-PMO) are accountable to ensure that Project Management Frameworks and SDLCs incorporate the necessary tasks, deliverables and reviews required by these security and privacy policies and guidelines. Project Managers (PM) ensure that these frameworks and SDLC's are adhered to in the conduct of a project. A best practice for IT-enabled projects includes gate reviews incorporating privacy and security issues that must be considered by the project team. Treasury Board Secretariat CIOB provides guidance for project gating for IT-enabled projects.

AMITA has access to a range of consulting experts that are familiar with both the departmental and information system level challenges and solutions. AMITA provides experts with the top level of security clearances as required. AMITA can assist *PMO's, EPMO's and PM's* to ensure that best practices defined in PM frameworks and SDLC's incorporate necessary security and privacy frameworks.

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, implementing federal government policies, including the PGS and ensuring continued delivery of services. The *PMO and EPMO* are accountable on management's

behalf, to ensure that security and privacy are incorporated in departmental best practices for project management and software engineering methodologies.

The risks associated with operating an IT system can never be totally eliminated, but can be minimized using a risk management approach in developing new or updating existing systems. The *department head/deputy head* is accountable for safeguarding sensitive assets including information under his/her control and ultimately accepts the risk of operating information technology systems within the organization.

AMITA is also capable of undertaking the IT security risk management activities that are performed by an IT security function as part of a departmental security program, more specifically, those enunciated in Annex 2 of ITSG-33 to be performed by IT projects and IT operations groups.

AMITA Services

AMITA can assist *Program and Service Delivery Managers* who work on behalf of the department's Deputy Head to ensure appropriate levels 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 such as ITSG-33) have been identified and addressed, and accepting the associated residual risk. With its experience in Project/Program Management, AMITA can also assist *departmental managers* in meeting budget and scheduling requirements of their programs and projects.

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, PMO/ePMO, PSO, DSO and the IT Security Coordinator* must work together to ensure that appropriate security measures are applied to all departmental assets, activities and processes. AMITA, as an ISO 9001 company, can assist this team in the review, implementation and communication of necessary processes and procedures.

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. AMITA will work with ePMO/PMO to integrate the necessary security and privacy tasks.

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.

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.

At the organizational or department level, lead agency guidance sets out the need to continuously monitor and assess the performance of deployed security controls. AMITA's professionals are experienced in conducting a variety of audits that place them well to conduct this activity. AMITA's experience in developing software products and solutions and in applying SDLC methodologies makes it routine for AMITA professionals to apply security where definition of controls, their integration and testing and finally, their monitoring and maintenance throughout the information system operational life occurs. The SDLC process also produces artefacts that are needed as **evidence in the Certification** of information systems. Some of this evidence includes documents such as: business security requirements, Statement of Security Requirements, Security Systems Design Specifications, Security Test and Acceptance Plans etc.

Finally, there is a relationship and/or interdependencies between Information System Security and other business related activities. More precisely business impact analyses that program and service delivery managers may conduct in support of their business activities may contain useful input to determine the business needs for security and the sensitivity and criticality of departmental business activities. AMITA does understand that business needs for security, including privacy requirements, and sensitivity and criticality serve to establish the security category of business activities.