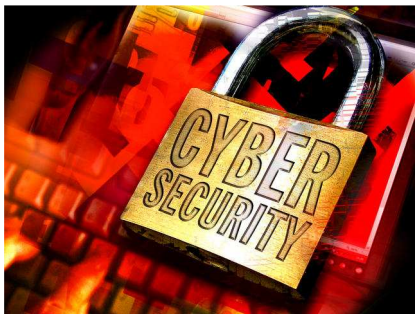
CyberSecurity

THE AMITA. APPROACH

INFORMATION TECHNOLOGY SECURITY RISK MANAGEMENT



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 cyberattack. 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 software 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

AMITA is 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 within the Federal context.

AMITA is also capable of assisting non-federal security practitioners in their efforts to protect information systems that must comply with other 'best practices' such as those published by ISO.

ITSG-33 guidance outlines an approach where IT security risk management activities are orchestrated at two distinct levels in the organization: the departmental level and the information system level. AMITA has access to a range of consulting experts that are familiar with both the departmental and information system level challenges and solutions.

AMITA Services

AMITA can assist *departmental IT Security officials* to carry out on-going work to identify those information systems which are at high risk or critical to business operations using a high-level risk analysis approach (security review). This will permit departmental security officials to categorize its systems into those which require a detailed risk analysis to achieve appropriate protection and those for which baseline protection is sufficient.

If required, AMITA can assist in establishing a 'Threat and Risk Assessment' methodology and can provide the guidance and training so that *business areas and IT system planners, developers, and implementers* can apply the methodology.

AMITA can also assist *security offices* to develop a unique Threat Risk Assessment (TRA) methodology should a client wish to proceed in this manner. The AMITA understanding and expertise in this area will ensure that 'industry best practice' components are included, more specifically Statements of Sensitivity, Threat Analyses, Vulnerability Analyses and Risk Assessments.

Should clients decide to adopt and apply a Federal methodology such as the Harmonized TRA Methodology, AMITA is familiar in its application.

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.

Finally, there is a relationship and/or interdependencies between Information System Security and other business related activities. More precisely, where 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 can provide assistance. AMITA does understand that business needs for security (including privacy requirements) and sensitivity and criticality serve to establish the security category of business activities.

Security Mandate

Organizations, more specifically those within the Government of Canada (GoC) depend 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.

Organizations are responsible for the planning and implementation of activities that constitute an effective IT Security Risk Management program that will be compliant with applicable GC legislation and TBS policies, directives, and standards as they relate to security controls.

More specifically, departments must meet the requirements of the Policy on Government Security (PGS) and the Treasury Board *Standard on the Management of IT Security as well as Lead Agency IT Security Risk Management requirements such as ITSG-33.*

Federal departments may wish to conduct continuous risk management, as defined by TBS's *Framework for the Management of Risk* (FMR) which requires: the establishment of baseline security, the conduct of threat and risk assessments to determine the need for safeguards beyond baseline levels, and the continuous monitoring of the threat environment so that an appropriate balance between operational needs and security can be maintained.

Threat Landscape Overview

Public and private sector organizations are increasingly dependent upon the use of the internet to perform their business, to serve their clients and to exchange sensitive information over this hostile medium. Many of the larger organizations operating in this space are driven by legislative and regulatory requirements that demand requisite due diligence including appropriate safeguards such as: Policy on Government Security and Privacy Impact Assessment Guidelines enunciated by the Treasury Board of Canada, the Government of Canada Privacy Policy and Protection of Information Privacy and Electronic Documents Act (PIPEDA), the Health Protection of Privacy Act (HPPA) and Industry Regulations including the Payment Card Industry (PCI) PIN/DSS and Interact Standards.

AMITA is a service provider who delivers products and services to clients who require privacy and security solutions and due diligence that will assure protection of their sensitive information assets and integrity and availability in information systems that service client's needs.

For the past several years, Governments have been more involved in protecting information resources as part of their critical infrastructure protection efforts. State sponsored hacking and an increase in computer based crimes motivated by monetary gains, largely by criminal organizations in developing nations, have both been drivers for Government strategies in this respect; more precisely, the publication of a Canadian & US Government Cyber Security Strategy.

The increased dependence on partnerships leads to the challenge of maintaining a balance between efficiency and control. Loss of control will lead to increased risk. The increased use of cloud computing and smart technologies is resulting in loss of control and inadequate security provisions, respectively, are now evident on an ever expanding basis. Additionally, the blurring of work and personal assets, in particular, the use of wireless devices is resulting in data leakage and increased risk to sensitive information assets.

Use of social media for corporate objectives and personal work-life is also posing to be a difficult balance to manage. Finally, published in the Information Security Forum (ISF) 2015 Threat Horizon is one new and emerging threat -- cyber breaches don't merely lose data, the associated loss of reputation reduces corporate share value.

Experience illustrates the need for easily accessible and comprehensive lists of emergency assets to improve response during crises. Emergency resource management brings together business methods and procedures that include how to "type" the capability of a resource, how to find, borrow, and return a typed resource belonging to another agency, and how to recognize a target capability gap within a geographic area. The processes and procedures for resource management collaboration such as resource ownership, resource assignment, types of resource capabilities are becoming more critical to support emergency response.