Information Management Technology (IMT) Assessment Tools for Systems and Applications

Purpose

The purpose of this document is to:

- highlight assessment tools for systems and applications within the Government of Alberta;
- explain when and how each assessment tool is used; and
- outline the obligations, requirements and precursors for each assessment tool.

Background

Information is what the Government of Alberta (GoA) relies on to make decisions that impact Albertans in meaningful ways. Information management (IM) is the way in which an organization plans, identifies, creates, collects, organizes, uses, secures, stores, shares, manages and disposes of its information. A key GoA IM requirement is ensuring the authenticity, reliability, trustworthiness, and usability of all information under the custody and/or control of the GoA—a requirement that extends not only to business processes and governance, but also to the systems and applications used to create, collect, and maintain information.

To support effective IM, all systems and applications in the GoA are subject to mandatory business prerequisites that ensure:

- compliance with policy instruments (e.g., Records Management Regulation, IMT Policy); and
- employees follow standard practices for the creation, use, management and disposition of information.

Information Management Assessment Tool for Systems and Applications

Use:	When: • procuring, developing or enhancing a system or application for the GoA.

Overview:	• The IM Assessment Tool for Systems and Applications allows business areas to evaluate and audit IM capabilities of existing or potential GoA systems and applications.
	• Actions are prescribed based on Yes or No responses during this high-level analysis.
	• There are three phases to the framework:
	  ○ Risk Assessment;
	  ○ System or Application Functionality; and
	  ○ Risk Mitigation.

Link(s):	• Information Management Assessment Tool for Systems and Applications
Contact:	SA.InformationManagement@gov.ab.ca

NOTE: Sections 2.4 and 7.4 of the Information Security Management Directives (ISMDs) require that a risk assessment (i.e., Security Threat and Risk Assessment **AND/OR** Information Security Statement of Sensitivity) **MUST** be performed for all Information Assets and IT Systems.

Security Threat and Risk Assessment (STRA)

Use:	• It is recommended that business areas consult with their Sector Information Security Officer when an STRA needs to be performed. • May be completed concurrently with a Privacy Impact Assessment (PIA).

Overview:	• Intended to assist program managers in assessing:
	  ○ security threats to information and information technology systems;
	  ○ vulnerabilities that may be exploited by identified security threats (and the safeguards in place to protect said vulnerabilities);
	  ○ the risk of vulnerabilities being exploited (based on existing safeguards); and
	  ○ compliance with security requirements described legislation, regulations, contracts and other applicable policy instruments.
	• Identified risks become part of the GoA's Information and Technology Risk Register, which ensures that the risks are monitored and managed while the related system or application is in use.
	• Can assist in deciding whether or not a system or application should be implemented, based on assessed risks and their potential treatment/mitigation.
	• There are three phases to the guide:
	  ○ Business Impact Assessment;
	  ○ Threat and Vulnerability Assessment; and
	  ○ Control Selection.

Link(s):	• STRA Background • STRAs – General Steps • ServiceLink Security Templates
Contact:	Sector Information Security Officer Contact List

Information Security Statement of Sensitivity (SoS)

Use:	When: • procuring, developing or enhancing a system or application handling ministry information; • there is a change in the handling, use or delivery of a system or application that has already had an SoS.
Overview:	• Allows business areas to evaluate and audit the confidentiality, integrity, availability and value properties of the information assets for a system or application.

	• Acts as a Memorandum of Understanding between the Sector Information Security Officer and a business area. • Precursor to the Security Threat Risk and Assessment and the Privacy Impact Assessment.
Link(s):	• GoA IT Security Templates • SoS Process Map
Contact:	Sector Information Security Officer Contact List

Corporate Privacy Impact Assessment (PIA)

Use:	**NOTE: A PIA should not be conducted without first completing an SoS**
	
	• It is recommended that business areas collaborate with their FOIP Office to determine if a PIA needs to be performed. A PIA may need to be completed when:
	  ○ procuring, developing or updating/enhancing a system or application that collects, manages or maintains any personally identifying information (as defined in section 1(n) of the *Freedom of Information and Protection of Privacy (FOIP) Act*);
	  ○ entering into an agreement with a new business partner or vendor who will have access to personally identifying information under the custody or control of a business area (e.g., cloud services); and
	  ○ a change occurs in the range and/or depth of personally identifying information collected, managed, or otherwise maintained by a system or application.
	• May be completed concurrently with a Security Threat and Risk Assessment (STRA).

Overview:	• A process of analysis and risk mitigation that helps to identify, review and address the impact of a new or updated system or application on individual privacy.
	• Designed to ensure that business areas assess system or application compliance with relevant privacy legislation (specifically, section 38 of the *Freedom of Information and Protection of Privacy (FOIP) Act*).
	• Meant for proposed policy instruments, administrative practices and/or information systems and applications that relate to the collection, use, protection, disclosure and retention of individually identifying personal information.
	• Requires close collaboration between a business area and the appropriate FOIP office.
	• Requires periodic review to:
	  ○ ensure compliance to applicable policy instruments; and
	  ○ assess changes in the range and/or depth of personally identifying information collected, managed, or otherwise maintained by a system or application (i.e., “scope creep”).

Link(s):	• FOIP Guidelines and Practices

	• Privacy Impact Assessment Templates
Contact:	Corporate FOIP Office, Service Alberta

Information Technology (IT) System/Application Impact Assessment Tool

Originates From:	Business Continuity Office of Alberta Emergency Management Agency (AEMA)
Use:	• It is recommended that business areas have appropriate business continuity plans in place as part of emergency preparations.
Overview:	• Used to: ○ determine the criticality of a system or application; ○ identify any gaps or misalignments between IT disaster recovery solutions and business continuity requirements; ○ recommend a disaster recovery solution that is cost appropriate, while still meeting the needs of the business area; and ○ rationalize the cost of proposed IT disaster recovery solutions to a business area.
Link(s):	
Contact:	Alberta Emergency Management Agency (AEMA): 780-644-5425 Sector Information Security Officer Contact List Senior Records Officer Contact List

Resources

- Enterprise Information Management
- Data and Information Security Classification IMT Standard

Contact

Enterprise Information Management
sa.informationmanagement@gov.ab.ca