Content Management Requirements Assessment and Risk Acceptance Guideline

Technology and Innovation, Data and Content Management Division, Enterprise Content Management Branch

Version: 1.0

Approved by: Executive Director, Enterprise Content Management Branch	**Owner:** Enterprise Content Management Branch	
Approval date: September 25, 2023	**Last reviewed:** September 25, 2023	**Review date:** September 25, 2024
Contact: SA.IMPrograms@gov.ab.ca	**Policy Instrument type:** Guideline	

Contents

Guideline Statement

This guideline outlines recommendations for the assessment of content management requirements and documentation of potential content management risks by information controllers and custodians in the Government of Alberta (GoA). This guideline supports the implementation of the requirements detailed in the Content Management Policy.

NOTE: There are legislated, mandatory requirements for information that are part of Freedom of Information and Protection of Privacy (FOIP) requests and/or information that is subject to the *Health Information Act* (HIA); these requirements are paramount to this guideline.

Authority

This guideline is issued under the authority of the *Government Organization Act* and the Records Management Regulation.

Under the Records Management Regulation, Technology and Innovation has the authority to establish, maintain, and promote the enterprise policies, standards, and procedures for the creation, handling, control, organization, retention, maintenance, security, preservation, disposition, alienation, and destruction of records in the custody and/or under the control of a Government of Alberta department or departments.

Application

This guideline applies to all departments defined under section 14 of Schedule 11 of the *Government Organization Act* and agencies, boards, and commissions as defined in Schedule 1 of the Freedom of Information and Protection of Privacy Regulation.

Agencies, boards, and commissions that are not contained within Schedule 1 of the Freedom of Information and Protection of Privacy Regulation are encouraged to align with this guideline.

Definitions

Information Controllers: Information controllers have the responsibility and decision-making authority for assigned collections of information, including (but not limited to) regulating and administering use, disclosure, and/or disposition of information.

Information Custodians: Information custodians have the responsibility for maintaining and/or administering the systems and/or applications in which content is managed without having responsibility for the information itself.

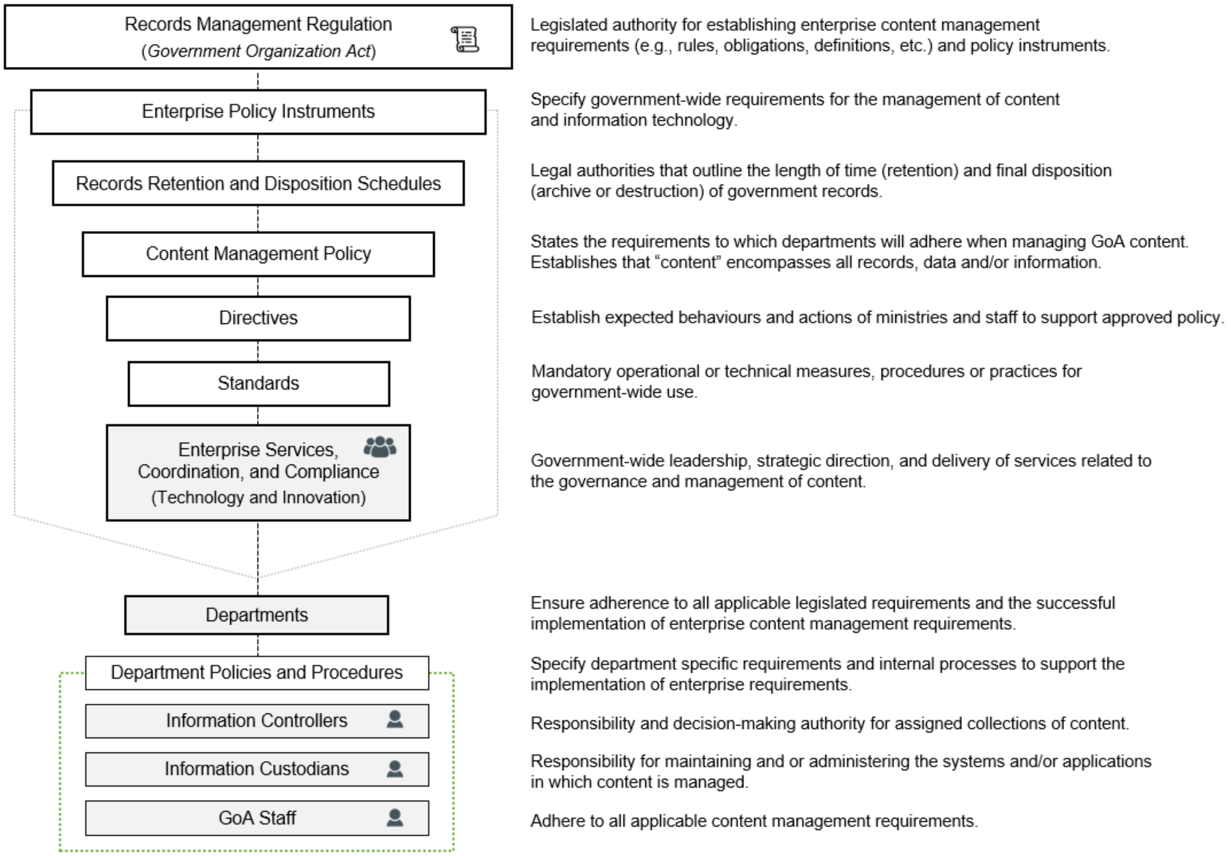
NOTE: The GoA Content Management Policy (Appendix A) includes definitions of key concepts to support a common understanding of enterprise content management requirements.

Understanding Content Management Requirements

Content management requirements are informed by business, legal and regulatory context. Under the Content Management Policy, content must be managed in accordance with the government's content management policy instruments (e.g., records retention and disposition schedules, Official and Transitory Records Directive, etc.) and applicable legislation. The GoA's foundational content management principles are specified in the Records Management Program Standard.

The diagram below outlines the relationship between enterprise content management requirements and department policies and procedures in the GoA.

NOTE: The diagram focuses on the GoA content management program and as such it does not include other key information management and technology (IMT) related legislation (including but not limited to FOIP Act, and *Health Information Act*.)


Records Management Regulation
(*Government Organization Act*)
Enterprise Policy Instruments
Records Retention and Disposition Schedules
Content Management Policy
Directives
Standards
Enterprise Services, Coordination, and Compliance
(Technology and Innovation)
Departments
Department Policies and Procedures
Information Controllers
Information Custodians
GoA Staff

Legislated authority for establishing enterprise content management requirements (e.g., rules, obligations, definitions, etc.) and policy instruments.

Specify government-wide requirements for the management of content and information technology.

Legal authorities that outline the length of time (retention) and final disposition (archive or destruction) of government records.

States the requirements to which departments will adhere when managing GoA content. Establishes that "content" encompasses all records, data and/or information.

Establish expected behaviours and actions of ministries and staff to support approved policy.

Mandatory operational or technical measures, procedures or practices for government-wide use.

Government-wide leadership, strategic direction, and delivery of services related to the governance and management of content.

Ensure adherence to all applicable legislated requirements and the successful implementation of enterprise content management requirements.

Specify department specific requirements and internal processes to support the implementation of enterprise requirements.

Responsibility and decision-making authority for assigned collections of content.

Responsibility for maintaining and or administering the systems and/or applications in which content is managed.

Adhere to all applicable content management requirements.

Figure 1: Content Management Requirements in the GoA

In addition to the policy instruments identified in Figure 1, enterprise procedures and guidelines are available to assist departments in the implementation of enterprise policy and requirements.

In practice, the assessment of content management requirements and risks occurs at multiple levels including (but not limited to): business unit, business process, projects, applications, and storage locations.

NOTE: For the purposes of this guideline 'application' refers to an application, system, solution, platform, product, software and/or database.

Any assessment of content management requirements must consider:

- applicable records retention and disposition schedules;
- the classification of content as either transitory or official;
- format (e.g., documents, emails, data, images, audio, and video recordings, etc.);
- authenticity, reliability, integrity and useability of records;

- sensitivity (e.g., security classification, privacy, and confidentiality, etc.); and
- flow of information into, through, and out of GoA business areas, processes, and/or applications.

Assessing Content Management Risk

The assessment of content management risk is necessary to safeguard GoA content (inclusive of all records, data and information) against unauthorized access, collection, use, disclosure, and/or destruction.

As information controllers are responsible for assigned collections of information, they are also responsible for ensuring all applicable content management requirements are met and that any risks have been identified, mitigated, and accepted.

Assessing content management risk is a collaborative process that involves multiple stakeholders. While risk acceptance is ultimately the responsibility of the information controller, identifying and managing content management risk should involve the following stakeholders:

- information controllers;
- information custodians;
- content management service areas (i.e., Enterprise Content Management branch);
- business areas;
- IT, privacy, cybersecurity, legal, procurement and/or other service areas as required.

Over time, risk may need to be re-assessed (e.g., when substantive changes are made to a system and/or application in which GoA content is managed). Substantive changes to a system and/or application may also require reassessment of privacy and security risks.

Considerations when assessing content management risks may include but are not limited to content being:

- retained for less or more time than is required by applicable records retention and disposition schedules;
- dispositioned but not in compliance with mandatory procedures;
- subject to a FOIP or legal hold and not preserved;
- unreliable, unusable, or authenticity and integrity is not preserved; and
- captured and/or stored without the required metadata.

The assessment of content management risk should occur in conjunction with other approved/required risk assessments (e.g., Security Threats and Risks Assessment). Based on a review of the documented risk assessment, content management service area staff can advise whether sign-off (i.e., documented risk acceptance) by the information controller(s) is required. Content management requirements can be assessed by completing the Content Management Requirements in Applications Checklist (PDF).

Documenting Risk Mitigation and Acceptance

The results of a content management risk assessment and any proposed mitigation should be fully documented, reviewed, and validated with the appropriate stakeholders and subject matter experts. Content management service area staff can advise whether sign-off (i.e., documented risk acceptance) by the information controller(s) is required.

An editable template is available to support the documentation of accepted risk when necessary: Risk Acceptance Documentation (PDF).

Roles and Responsibilities

NOTE: The responsibilities identified in this guideline are not comprehensive and may be expanded in other policy instruments.

Information Controllers are responsible for assessing and, as necessary, signing off on any identified content management risks, provided satisfactory and appropriate mitigation is established.

Information Custodians are responsible for understanding and adhering to all approved department and enterprise content management requirements and ensuring GoA systems and/or applications support compliance with all applicable content management requirements.

Content management service areas are responsible for advising information controllers, information custodians and business areas to ensure GoA content is managed in accordance with established enterprise and department policy instruments.

GoA staff (including contracted system and application developers) are responsible for understanding their content management obligations.

Compliance

Consequences of non-compliance with this guideline could result in: the loss of content; breach of confidentiality; breach of privileged information; significant impact to GoA's proprietary rights; damage to GoA's reputation; exposure of Albertans to harm; and/or incurrence of unnecessary costs (including, but not limited to, inability to respond appropriately to a claim in court).

Depending on the severity of non-compliance:

- either informal or formal requests and/or follow-ups may be made by Innovation, Privacy and Policy Division, Corporate Internal Audit Services, Cybersecurity, Office of the Information and Privacy Commissioner, Office of the Auditor General and/or Public Service Commission; and
- legislated disciplinary action (i.e., *Public Service Act*) may be taken.

References and Supporting Resources

- Records Management Regulation
- Content Management Policy
- Records Management Program Standard
- Data and Information Security Classification Standard
- Information Security Management Directives
- Template: Risk Acceptance Documentation
- Checklist: Content Management Requirements in Applications

Contact

Types of Questions	Contact
Content Management – GoA Departments	Information Management Advice and Consultation Service (BERNIE)
Content Management - GoA Agencies, Boards and Commissions	SA.IMPrograms@gov.ab.ca