BRITISH
COLUMBIA
The Best Place on Earth

Guidelines for Best Practices in Data Management – Roles and Responsibilities

March 2012

Data Architecture Advisory Committee

A subcommittee of Information Architecture & Standards Branch

Table of Contents

1 INTRODUCTION

This document was created by the Data Architecture Advisory Committee (DAAC), as part of their expert advisor role to the Architecture and Standards Branch. The original version of these guidelines was published by the Data Administration Forum (DAAC forerunner) in April 1999.

The roles and responsibilities described here reflect best practices for data management within the Province of British Columbia. From a business context, these concepts provide foundational support for improving information access and sharing both internally within government and to the public.

1.1 Purpose

The Core Policy and Procedures Manual, Chapter 12 sets expectations for ministries and agencies to implement consistent data management practices. Beyond policy directives, the concept of accountability for a set of data is a critical building block for effective business operations and for fostering partner engagement to integrate information management activities across government. Where there is confusion around business accountability, operational risks are higher and there is little or no successful integration of information resources. Understanding and implementing the roles in these Guidelines will clarify business decision-making and encourage information sharing and integration.

This data management model is based on the existence of *Data Custodians*: senior managers who are accountable and responsible for collecting and maintaining data of interest to government and in an appropriate manner making this data publicly available. The Guidelines provide a reference for building and improving this capability.

1.2 Intended Audience

This document serves as a reference for resources involved in the management of government data or the development or maintenance of systems which act on government data. In particular, these guidelines can be used by ministries as part of the education and communication process for improving information management in their organization.

1.3 Scope

The roles and responsibilities in this document pertain to data and information management roles pertinent to the governance, planning, definition, capture, usage and access to data and/or information. The defined roles cover a broad area – some roles only data management, some roles both data management and information management depending on the context of the specific situation. Where "data" is used, it may also refer to information – i.e. data that has been transformed into information.

1.3.1 In Scope: Roles that deal with

- ✓ data stored in databases
- ✓ data wherever else it may reside and in whatever medium, including paper
- ✓ data with context (data translated into information)
- ✓ technical roles that have direct responsibilities for some aspect of data management, such as those related to database management
- ✓ information management leadership and guidance for appropriately planning for and turning data into useful business information

1.3.2 Out of Scope: Roles that deal specifically with

- ✓ records management (e.g., role provided by the Records Officer)
- ✓ information security (e.g., role provided by the Ministry Information Security Officer)
- ✓ technical or enabling technology roles (e.g. application development or infrastructure delivery)

1.4 "Owner"

Within British Columbia, the Crown is the owner of government information (i.e., the asset owner). For information that the Crown (e.g., a ministry) is holding on behalf of, or from another source (e.g., an individual's health information), the data management roles remain constant but the 'owner' will be different.[1]

Information owners have accountability for information throughout its life cycle, including decision making authority for creating, classifying, restricting, regulating and administering its use or disclosure. The implementation of these decisions can be delegated.

1.5 Data Custodianship Principles

There are many data-related roles, but the Data Custodian role is the single most important for decision-making and leadership.

The *Principles of Data Custodianship* on the following page are defined in the **Data Custodianship Guidelines for the Natural Resource Sector** and are fundamental statements for the governance of government data. These Principles are aligned with industry best practices for data management as defined by The Open Group Architecture Framework (TOGAF).

[1] For external-to-Government owners where government has been granted the legal authority and accountability to capture or hold source data, the appropriate government branch with program accountability is the Data Coustodian, for government purposes. Where government holds a copy of the original source data on behalf of the external owner, the appropriate government branch is the Data Steward.

Custodian Principle	Description
Data Custodian is Corporate Trustee	*Data Custodians operate as a trustee on behalf of the Information Owner.*
Data Custodian is Standards Bearer	*Data Custodians ensure the development and enforcement of standards for data within their care.*
Data Custodian is the Authoritative Source for the Province	*Data Custodians are the authoritative source for data within their care, and are responsible for all aspects of the data including distribution. In some cases, where data management practices are in place, the Data Custodian may delegate distribution of the data to a Data Steward under an agreement that ensures data integrity, authorized access, and adherence to conditions of use.*
Data Custodian is Accountable	*Data Custodians are accountable for managing the data within their care*
Data Custodian Ensures Availability	*Data Custodians will ensure that data is available to authorized users and, where possible, make this data accessible to the public*
One and Only One Data Custodian	*Each set of data[2] has a single, designated Data Custodian, without exception*

1.6 Other Related References

The scope of this document includes the roles required for data management which may include some information management functions. Information management depends on data planning and management activities to optimize the use of information as a vital business resource.

1.6.1 Data Administration Standards

The *Data Administration Standards* define minimum criteria for data management that apply to data within the BC government, and are for use by ministries when developing a data architecture function. The intent is to make a minimum set of data standards mandatory, while encouraging all ministries to follow best practices in all information management.

[2] *Set of data* has a specific meaning in this document. It is defined as data holdings (collected data) for a discrete corporate information subject. The set of data must be of a lasting nature, collected, managed, and used to serve an essential defined business purpose for government. One may also use the term “corporate data” for similar meaning in the context of a ministry’s business (i.e. ministry corporate data) or in the context of government-wide standards (i.e. government corporate data). It does not equate to a “dataset”, which is popularly used for anything from a single spreadsheet to massive multiple databases, and is therefore a term which is difficult to scope.

2 DATA MANAGEMENT ROLES AND RESPONSIBILITIES

The responsibilities outlined here are meant to introduce basic concepts and roles, and are not intended to be used as the full set of functions for a specific staff position.

To consistently manage data, and by extension, information, ministries should ensure they understand and use the three ***Critical* Data Roles** defined below. Core and Additional roles supplement the Critical Data Roles and will help support business operations and integration. Smaller ministries, or those with fewer data holdings, may be able to combine multiple roles into single jobs – where this happens, the role descriptions will help Ministries understand and differentiate activities.

The Data Custodian role needs to be positioned at a senior management level within ministries to be effective, e.g. Director in larger ministries or Executive Director in smaller ministries.

Typically, ministries will already have staff performing some or all of the activities described in these role descriptions. The best practices described here will guide improvement.

To effectively implement data management responsibilities they must be assigned to a specific set, or collection, of data (refer to Definitions). The word “Manager” describes the function of the role and does not necessarily imply it is at a management level.

2.1 Critical, Core, Additional and Existing Roles

2.1.1 Critical Data Roles

The following roles are critical for successful data management, and should be the first data management roles implemented or assigned within any ministry.

- ✓ Data Custodian
- ✓ Data Standards Manager
- ✓ Data Steward (where support to the Data Custodian is required)

2.1.2 Core Data Roles

The following core roles are important to help guide and implement successful data management. Larger ministries or those with larger data holdings will find these roles indispensible.

- ✓ Data Resource Manager
- ✓ Application Custodian
- ✓ Data Architect or Data Administrator
- ✓ Database Administrator
- ✓ Discipline Authority

2.1.3 Additional Roles for Best Practices

- ✓ Data Usage Contact
- ✓ Data Analyst
- ✓ Data User
- ✓ Data Product Provider

2.1.4 Existing BC Government Roles

The following three roles are defined within the normal government organizational structure and are included to provide context in supporting the data management roles.

- ✓ Government Chief Information Officer
- ✓ Ministry Executive
- ✓ Ministry Chief Information Officer

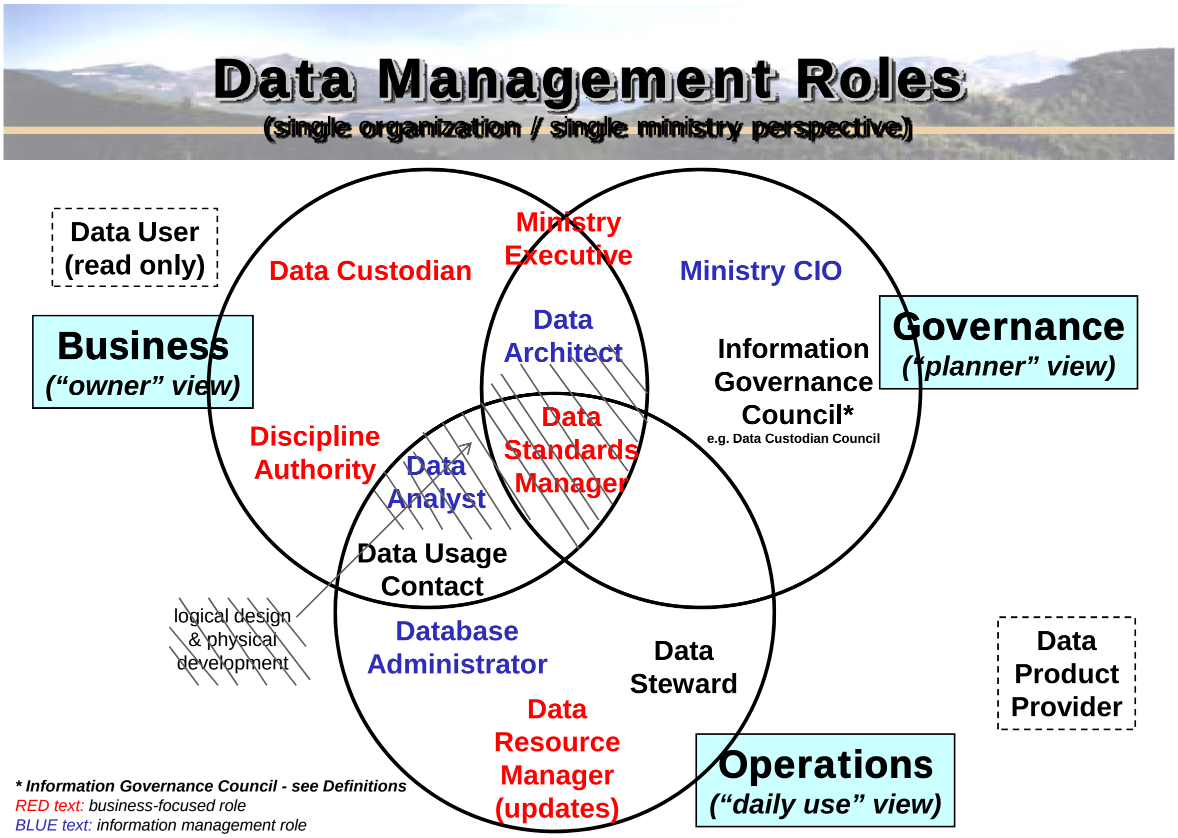
2.2 Data Management Roles and Interactions

The following diagram depicts the three viewpoints of data management:

- **Business**, or business context for the data;
- **Governance** or overall planning for the data; and
- **Operations**, or the implementation and daily management of data.

The interactions of the roles are depicted in the diagram below. The intersection of the circles depicts the areas of commonality and interaction between subject matter experts from different perspectives.

Note: All roles may interact at times. Key interactions are depicted as specific roles (Data Standards Manager, Data Usage Contact).



** Information Governance Council - see Definitions*
RED text: business-focused role
BLUE text: information management role
Inside the circles = roles related to standards and decisions
Outside the circles = data use and maintenance

2.2.1 Data Management Roles

The following sections include a description of each role and its responsibilities. In addition to the viewpoints above (Business, Governance, Operations), we included an *Organizational* (overseer) viewpoint. Thus, *Ministry Executive* and *Ministry Chief Information Officer* both have overall organizational responsibility for the effective management of data within the organization.

2.3 Critical Roles

2.3.1 Data Custodian

Establishes province-wide standards, definitions, and rules for business information within their mandate, to enable the Province to gain maximum value from the information.

Viewpoint: Business

Responsibility

- ✓ accountable for implementing operational policy, business value, scope, definitions, rules, standards, structure, content, use and disposal for data under their responsibility
- ✓ responsible for the collection, storage, protection, promotion and delivery of their data, ensuring it meets the business needs of the organization
- ✓ fulfilling the legislated responsibility or program mandate of ensuring data quality, completeness, and integrity through the management of its creation and maintenance
- ✓ allocating resources in order to meet data needs
- ✓ ensuring the value of data is maximized through sharing
- ✓ serving on an Information Governance Council or equivalent where the scope of their information resources is substantial within their Ministry.

Contact when

- ✓ a major business need for data is identified
- ✓ issues arise concerning data policy, business value, scope, security

2.3.2 Data Standards Manager

Business expert with detailed knowledge of the data structure, content, and appropriate use of the business information for their program area(s), who develops and sets the data management standards approved by their Data Custodian. Responsible for the day-to-day management of the data and business issues, according to the defined data standards and data management plan.

Viewpoint: Business & Operations

Responsibility

- ✓ acting as the primary contact for business data within the program area, on behalf of the Data Custodian
- ✓ authoring data management plan(s) (see Definitions), defining and managing the standards for acquisition, maintenance, and disposition of data to ensure data quality, resolving issues, and advising other roles
- ✓ ensuring designed data structures meet business needs
- ✓ ensuring the delivery of defined services at an operational level
- ✓ ensuring the protection of data is commensurate with its value and Information security classification

Contact when

- ✓ data access is required, within the scope of the program area
- ✓ operational, business, or data definition issues arise or cannot be resolved, or data errors are perceived
- ✓ further detailed information about their program area's data is required
- ✓ further data services are required to meet new business needs
- ✓ data management planning is required, or additional data may be encompassed within their business scope

2.3.3 Data Steward

An inclusive role that accepts one or more negotiated data stewardship activities on behalf of the Data Custodian. Data Stewards have the operational or technical ability to assist a Data Custodian in the collection, delivery, or maintenance of the set of data.

Note that the Data Custodian cannot transfer <u>accountability</u> to the Data Steward although the Data Steward may be responsible for specific activities.

Viewpoint: Operations

Responsibility

- ✓ supports the Data Custodian with expertise, or resources, to carry out one or more of their responsibilities
- ✓ as a peer of the Data Custodian, the Data Steward is bound by signed agreement which details the responsibilities with respect to both parties
- ✓ specific identified responsibility(s) are transferred from the Data Custodian to the Data Steward (<u>accountability</u> remains with the Data Custodian)
- ✓ where an agreement is in place with the authoritative source (see Definitions), delivers (or provides access to) authoritative data, ensuring data management practices are in place to maintain integrity, authorized access, and conditions of use

Contact when

- ✓ Per the stewardship agreement, when operational needs arise

2.4 Core Roles

2.4.1 Data Resource Manager

Any employee who has responsibility for the collection and/or management of government data. The use or update of information must be consistent with standards set by the Data Custodian.

Operational accountability resides with the most senior person in each office to verify that data collection and management is conducted to the defined standard.

Viewpoint: Operations

Responsibility

- ✓ providing leadership for data collection, update, and management to the Data Custodian's defined standards
- ✓ providing operational input into the business design decision-making process
- ✓ assessing the quality of data collection efforts to ensure that the data is collected to the standards defined by the Data Custodian
- ✓ retaining a focus on overall program needs while collecting information, to optimize the use of that data and ensure business decisions are based on the best information available

Contact when

- ✓ business-related queries are required

2.4.2 Data Architect (a.k.a. Data Administrator)

Senior technical data management expert with a corporate role (i.e. an overall organizational point of view), providing leadership on information systems theory and practice, data architecture and modeling expertise, and custodianship of the corporate data models. Provides and promotes the framework for consistency in scope, meaning, and handling of data across the entire organization (e.g. ministry).

Viewpoint: Governance and Business

Responsibility

- ✓ Ministry-wide leadership role promoting data/information resource management: the concept that data/information is a major corporate resource and must be managed using the same basic principles used to manage other major assets
- ✓ promoting information management principles, practices, guidelines and standards within the organization, while adhering to published government standards and guidelines for data management

- ✓ providing a framework for defining and interpreting the ministry’s corporate data and its structure (information architecture, including metadata) to support the organization’s data related goals and objectives, and ensuring the corporate value of data is maximized through sharing across diverse program areas
- ✓ creating or validating data models produced in the organization, and storing and maintaining the data models and definitions (e.g. a metadata repository)
- ✓ providing expertise to the ministry in improving data quality across all business areas
- ✓ defining compelling business arguments for senior management to elicit change on future or existing data issues
- ✓ cooperating with the Database Administrator in database design efforts
- ✓ liaise across-government (e.g., Data Architecture Advisory Committee (DAAC)) to develop and promote sound and consistent data management practices

Contact when

- ✓ analysis of the organization’s data inter-relationships is required
- ✓ access to data repositories is required
- ✓ standards for defining, storing, and delivering data are required
- ✓ responsibilities for data need to be determined
- ✓ data models require validating and quality assurance, prior to incorporating as corporate models and transposing them into physical models
- ✓ deviations from defined logical data structures are required

2.4.3 Database Administrator

Senior database management expert with a ministry-wide focus responsible for the analysis, design, and creation of new databases, the physical design and implementation of new database tables and applications on existing databases, and for database administration and backup. Typically, this role also plans, co-ordinates and implements security measures and improves the performance and efficiency of data storage.

Viewpoint: Operations

Responsibility

- ✓ building databases to support developing, maintaining, and implementing of physical data structures
- ✓ defining ministry-wide standards for physical data management
- ✓ ensuring that efficient data structure design and disaster recovery/backup procedures are effectively tested and implemented
- ✓ developing (and reviewing) physical data structures in consultation with Data Administration and system development and maintenance staff

- ✓ ensuring security administration through monitoring and administering DBMS security constraints, such as removing users, administering quotas, auditing, and checking for security problems.
- ✓ analyzing data stored in the database and making recommendations relating to performance and efficiency of that data storage. This includes the effective use of indexes, enabling "Parallel Query" execution, or other DBMS specific features

Contact when

- ✓ logical data models are ready for implementation
- ✓ expertise is required to resolve issues related to:
  - ◦ database management anomalies occurring in the operation of a database
  - ◦ physical data security
  - ◦ disaster recovery or database back-up
  - ◦ system migration or database platform standards
  - ◦ data performance degradation

2.4.4 Application Custodian

Sponsors projects to develop information systems, and provides ongoing support for those systems to meet business needs.

Viewpoint: Business

Responsibility

- ✓ accountable for applications that enable information entry, retrieval, and updating , and derive the best possible business benefit from the use of the application
- ✓ ensuring that, within their application mandate, they provide local leadership in support of the Data Custodian(s)
- ✓ conducting impact analysis and coordinating application changes to avoid adverse impacts on other applications or data

Contact when

- ✓ a need for a new business function(s) or new application(s) is identified
- ✓ there are major problems with existing applications

2.4.5 Discipline Authority

Business expert or specialist who understands the business relevance of the data standards within their scope of work. Interprets the meaning of detailed data standards to ensure the appropriate use of data and information needed to meet organizational needs. A primary resource for the **Data Standards Manager**.

The **Discipline Authority** is usually at the senior scientific, analytical, or research level.

Viewpoint: Business

Responsibility

- ✓ interpreting and defining data within the scope of their expertise and according to the business need
- ✓ providing expert understanding of the subject area and business definitions
- ✓ providing guidance and subject matter expertise on the business use of the data

Contact when

- ✓ understanding of data is not clear from definitions and specifications
- ✓ interpretation of data, outside of existing specifications, is required

2.5 Additional Roles

2.5.1 Data Usage Contact

Business data expert that commonly provides technical services for decision making support for data managers, data custodians, business managers and operational users.

A primary resource for the Data Resource Manager.

Viewpoint: Business and Operations

Responsibility

- ✓ querying data content and using data effectively according to standards
- ✓ performing statistical analysis of business data
- ✓ analyzing business and system data

Contact when

- ✓ business-related database queries are required
- ✓ data mining or data reporting is needed to solve system or business related questions

2.5.2 Data Analyst

Information management analysis and design role that focuses on providing business or IT system decision support through analysis, and problem solving data related topics including data design, integration, data relationships, data quality, data transformation, data replication and data modeling. This role varies widely across government.

Viewpoint: Business and Operations

Responsibility

- ✓ Performing systems analysis and design, documenting the structure, relationships and types of business data through logical modeling, or validating logical models from other sources
- ✓ mapping the data dependencies from system to system to identify cross-program impact issues or answer business-related technical questions
- ✓ Providing business intelligence support by performing business data analysis and reporting to enable better business decision-making

Contact when

- ✓ analysis and problem solving of business or system data-related issues is required

2.5.3 Data User

Anyone who uses data to conduct analyses, make decisions or otherwise carry out work.

Viewpoint: Business

Responsibility

- ✓ obligated to abide by the Data Custodian's governing policies and standards
- ✓ understands the context in which the data can be used.

Contact when

- ✓ business-related queries are required

2.5.4 Data Product Provider

Any party responsible for the creation or publication of a set of data that is derived from one or more sources of primary government data, i.e., data for which there is an assigned Data Custodian.

(NOTE: must have written permission from the Data Custodian for proper acknowledgement of copyright. With future emphasis on government moving to open data, this may become less important.)

A Data Product is created by combining or manipulating one or more sets of data in order to address a particular business need. Data Products may also be called resultants, derivative products, analytical products, value-added sets of data, integrated sets of data, etc.

Viewpoint: Business and Operations

Responsibility

- ✓ recognizing that accountability for the original data remains with the originating Data Custodian
- ✓ ensuring that all aspects of the data lifecycle are followed for the Data Product
- ✓ ensuring that the Data Product is managed as a set of data, and that any interpretation, modification or aggregation with other sets of data is consistent with the original data; i.e., accountable for the data product standard
- ✓ ensuring acknowledgement of the primary data source(s), from which the Data Product is derived

Contact when

- ✓ business-related queries into the Data Product are required

2.6 Existing Related Roles

2.6.1 Government Chief Information Officer (GCIO)

Ensures government-wide policy for data creation, maintenance, and use is compliant with legislation, policy and standards. Operationalizes strategic directions for the management of IM/IT within government. The policy direction provided applies to all Ministries and sector groupings.

Viewpoint: Governance

Responsibility

- ✓ leads the structure for IM/IT management and decision making, in concert with senior executives from all BC Government ministries
- ✓ manages the OCIO and for the Ministry Chief Information Officers (MCIOs), as described in detail in the Province's Core Policy and Procedures Manual
- ✓ is accountable for the creation of government-wide data management policy, frameworks, standards and infrastructures
- ✓ strengthens the IM/IT governance processes of the province through strategic planning and discussion with all ministries on priorities and possibilities to leverage best practices and industry standards

Contact when

- ✓ Ministries are established or changed and this involves the definition of data management mandates or roles
- ✓ new/changed information management policy or standards are proposed that affect multiple ministries, or entire sectors
- ✓ IM/IT issues arise that require corporate consideration
- ✓ compliance issues arise between Ministries

2.6.2 Ministry Executive

Responsible for developing the policy framework within specific line(s) of business within a Ministry. Collectively define the strategic scope of the organization and overall business services.

Viewpoint: Business and Governance

Responsibility

- ✓ identifying and communicating Custodianship responsibilities within their organization
- ✓ ensuring ministry Data Custodians liaise between their organizations and others
- ✓ establishing and resourcing the areas of data responsibility
- ✓ approving ministry policies
- ✓ ensuring compliance with legislation, policies and standards
- ✓ formally recognizing and communicating the importance of information to the business

Contact when

- ✓ lines of business are established or changed that require definition of data management roles
- ✓ new/changed policy or legislation is proposed
- ✓ compliance issues arise
- ✓ need resourcing for data responsibilities

2.6.3 Ministry Chief Information Officer

Ensures the organization uses information management and information technology (IM/IT) efficiently, in alignment with OCIO policy, standards and directions.

Viewpoint: Governance

Responsibility

- ✓ ensuring compliance with the strategic direction of government
- ✓ ensuring strategic and operational plans for IM/IT are developed
- ✓ establishing and promoting the organization's information management policies, in alignment with OCIO policies and standards
- ✓ providing IM/IT leadership and facilitating data management within the organization
- ✓ advising the OCIO on information management and information technology issues and opportunities

Contact when

- ✓ compliance issues arise
- ✓ strategic direction of the ministry changes
- ✓ information management policy amendments or new policy is required

3 DEFINITIONS

Authoritative Data: Officially recognized data that can be certified and is provided by the authoritative source, or by a Data Steward via specific formal agreement.

Authoritative Proxy Agreement: A formal agreement (e.g., Memorandum of Understanding; Information Sharing Agreement) between a Data Custodian and Data Steward for delivery (or providing access) to a copy of a Data Custodian's source data and implementing data management practices to guarantee the same integrity. The agreement must include conditions of use and control of access.

Authoritative Source: an entity (by definition, the Data Custodian) that is officially authorized by a legal authority to develop or manage a set of data for a specific business purpose – the authoritative source of the data.

Corporate information: information that is of a permanent or lasting nature, is essential to the Government's operation.

Data Architecture: describes the structure of an organization's logical and physical data assets and data management resources (see TOGAF).

Data Management Plan: describes the strategic use and future plans for a major set of data within a program area. The management of a set of data goes beyond where is it stored, what format and when was it last updated – potential issues such as whether the data will meet future business and user needs, adequacy of data collection standards, level of data quality, adequacy of resourcing, etc. See the Natural Resource Sector's Data Management Plan Template.

Information Governance Council: A strategy group made up of those Data Custodians responsible for the more substantial Ministry information resources. This core group concentrates on major issues, and chooses Ministry-wide options, thus influencing the choices that other Data Custodians will have available. The Council is also a forum for contemplating impacts of legislative or policy changes.

Ministry Client (from a Data Custodian's perspective): any agency, company, office, or individual for whom services are rendered (e.g., a Ministry employee or Ministry office; another government Ministry or agency; an external private sector industry company or company employee; a member of the public).

Set of Data: "*Set of data*" has a specific meaning in this document. It is defined as data holdings (collected data) for a discrete corporate information subject. The set of data must be of a lasting nature, collected, managed, and used to serve an essential defined business purpose for government. One may also use the term "corporate data" for similar meaning in the context of a ministry's business (i.e. ministry corporate data) or in the context of government-wide standards (i.e. government corporate data). It does not equate to a "dataset", which is popularly used for anything from a single spreadsheet to massive multiple databases, and is therefore a term difficult to scope.

4 ACKNOWLEDGEMENTS

We would like to acknowledge the work done by the following in establishing these roles and definitions:

- ✓ ANZLIC (Australia and New Zealand Land Information Council)
- ✓ Integrated Land Management Bureau, Province of British Columbia
- ✓ Ministry of Attorney General, Province of British Columbia
- ✓ Ministry of Education, Province of British Columbia
- ✓ Ministry of Environment, Province of British Columbia
- ✓ Ministry of Finance, Province of British Columbia
- ✓ Ministry of Forests and Range, Province of British Columbia
- ✓ Office of the Chief Information Officer, Province of British Columbia
- ✓ John Zachman's Framework for Enterprise Architecture

5 APPENDIX A: OTHER BC GOVERNMENT DISCIPLINE GROUPS

The following diagram shows the relationship between the Data Management, Records Management, and Security Management disciplines' major roles (in green round-cornered rectangles). Ownership flows from the Crown, and legislation, policy and standards define how the custodians can work with the information in their care. These custodians may be internal or external to government, but the Data Custodian is ***always*** within government, exercising the Crown's control over the information. Government can have full custody and control of the information in its care, or it may relinquish full or partial custody of the information to another party. Government always retains decision-making authority on how that information will be stored, managed and protected. For example, where data is in the custody of parties external to government (e.g. personal health information in Health Authorities), the Crown still sets the rules and requirements for how that information must be handled. The Crown retains control of the full information lifecycle for government information.

5.1 Role Definitions: Data, Security, and Records Management

Records Management and Security Management are two other discipline groups in the Province of British Columbia that have defined accountability for managing data and/or information.

The following table shows some of the semantic differences between published roles from the three disciplines (Data Management, Records Management, and Security Management).

Published Role (see definitions below)	**Discipline**	**Normally Assigned To:**
Information Owner[3]	Security Management	Deputy Minister, on behalf of the Crown; may be further delegated by the Deputy Minister
Information Custodian	Security Management	Anyone who maintains or administers information resources on behalf of the Information Owner.
Data Custodian	Data Management	Branch Director, on behalf of the Deputy Minister, who maintains or administers data resources on behalf of the Information Owner.
Office of Primary Responsibility (OPR)	Records Management	Senior manager of any government office

*Information Owners (*Information Security Policy*, see Definitions)* – have the responsibility and decision making authority for information throughout its life cycle, including creating, classifying, restricting, regulating and administering its use or disclosure. Within the Government of British Columbia, information ownership flows from the Crown to government Ministers to Deputy Ministers (or equivalent). Information ownership may be further delegated by the Deputy Minister.

Information Custodians (Information Security Policy, see Glossary) – maintain or administer information resources on behalf of the Information Owner. Custodianship includes responsibility for accessing, managing, maintaining, preserving, disposing and providing security for the information resource. In contrast, information custody means having physical possession of information without necessarily having responsibility for the information.

Data Custodian ***(this document)*** – the branch director or senior manager who establishes province-wide policy, definitions, and rules for business information within their mandate, to enable government to gain maximum value from the information.

[3] HInformation Security PolicyH 2.1.3 (b) states: Within the Government of British Columbia, information ownership flows from the Crown to government Ministers to Deputy Ministers (or equivalent). Information ownership may be further delegated by the Deputy Minister.

Office of Primary Responsibility (Recorded Information Management Manual and external *Glossary)* – The office that has primary responsibility for a category of records or holds the master copy of any record series for that ministry or agency. The OPR maintains the official master copy of the records in order to satisfy operational, financial, legal, audit and other requirements.

5.2 Definitions: Security and Records Disciplines

For the underlying policy framework and standards, see Core Policy chapter 12 (http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm) including section 12.3.3.

Information Security roles are defined in policy and procedures (see gww.cio.gov.bc.ca). In scope of this document are responsibilities for granting access to data and the physical enabling of access to data in databases. Out of scope are other security responsibilities such as monitoring, handling incidents, security awareness and training.

Records Management is the exercise of intellectual and physical control over records to ensure their integrity in support of an organization's accountabilities and actions. Ministries and agencies establish intellectual control over their records by ensuring they are classified, retained and disposed of in accordance with records schedules., and establish physical control by ensuring records are identified, documented, located, retrieved, and protected from loss, physical damage or inappropriate access. There are touch points and overlap with some aspects of data management, but the relationship to records management is not fully defined in this document.

END