

Management Guide to Custodianship (S35)

This guide complements the ministry's [Corporate Information Custodianship policy](#) (Policy 7.3).

Purpose of S35

This guide complements Ministry of Forests and Range Policy #7.3, [Corporate Information Custodianship](#), and explains the concepts presented in the policy. This guide is intended to be used by ministry management or other staff to assist them in dealing with information management concerns that arise out of the ministry's pressing need for computer applications that access integrated, shared data.

The rationale for custodianship is twofold:

1. Information is **critical** to the ministry and is often **shared** across government.
2. Applications that affect corporate information must be **planned** and **managed** at the highest quality assurance level, and **coordinated** across each program area.

Custodians are responsible for deciding what information and/or applications are important for the ministry to use in a particular subject area, and are responsible for validating that the ministry's business interests are served by the investment in that information or application(s). The next section gives a general [introduction to custodianship](#), with an overview of the responsibilities of a Custodian for corporate information and corporate applications. Detailed responsibilities follow, for both a [Data Custodian](#) and an [Application Custodian](#).

Overview

Information management and application delivery are **corporate** (ministry-wide) concerns. The scope of responsibility of a *Custodian* for an information item or an application is the entire ministry, not only their own organizational area. It should be unambiguously clear to the rest of the ministry that the Custodian is ultimately responsible. Custodians provide a leadership role in enabling ministry staff to derive the best possible benefit from the investment made in the gathering of information and/or the development and implementation of an application.

It is **business** information that is important to the ministry, and the intent of the custodianship policy is to clarify that those responsible for the business are responsible for the information that concerns that business. Information Management Group's (IMG's) mandate as it relates to information and application custodianship is to ensure the appropriate infrastructure is built within the ministry to gain the most effective use from information systems over time (see the section titled [IMG Role](#)). IMG cannot dictate the business use of information or what business procedures are implemented; that responsibility lies purely within the business area.

For these reasons, IMG cannot act as the Data Custodian of business information. IMG *does* act as the Data Custodian in areas integral to the ministry's information

management infrastructure, such as security, technology assets, and the corporate data dictionary. IMG also is the Application Custodian where there is large scale utilization in Operations Division, or where there is a large degree of integration between applications, including the common ministry infrastructure.

Stewards have a subset of Data Custodian responsibilities, acting at the request of and on behalf of the Data Custodian. A Steward in this context must already be a Data Custodian (i.e., Branch Director). Stewards ensure that a set of the Custodian's information is available if the Custodian does not have the appropriate operational resources to provide the necessary functions. The *Custodian* therefore specifies the business use of the information and is still responsible for it, defining its structure, format, content, and how the information relates to other business information, but might delegate technical or operational matters to the *Steward*, such as the decision as to how the information is stored and retrieved across the province. The Steward then ensures that the integrity of the information meets the published standards.

Throughout this document, references to *corporate information* or *corporate data* will be made frequently. Corporate information is simply information that is of a permanent or lasting nature and is essential to the ministry's operation. Defining information as *corporate* implies that rigorous standards for definition, entry, update, and use are in place and actively followed by those who access the information. These standards add significant cost to the management of such information. Defining information as being *essential to the ministry's operation* is a management decision, and that decision is the responsibility of the Custodian. For more information see the section titled [Corporate vs. Non-Corporate Data](#), or [related web documents](#).

Data vs. Information

There is a difference between the terms **data** and **information**. **Data** is an individual fact or multiple facts, or a value, or a set of values, but is not significant to a business in and of itself. For example, the following are values with structure but they aren't useful to anyone until given context:

February 15, 2005
D13193
\$609,000
12%
47,000

Data values without business context

Giving data context, or meaning, turns it into **information**. Without this context the data is useless to the business. We store data on paper forms (with headings) to give data meaning. We also store data in computer databases and use the defined data structures and applications or application screens to give that data meaning.

For example, the above numbers are more useful with the added context:

Business context	Data value
------------------	------------

<i>What is the date of the meeting about the fee increases?</i>	February 15, 2005
<i>What was the licence plate number of the car that hit you?</i>	D13193
<i>What did Project 06-073 cost for 2005/06?</i>	\$609,000
<i>What is the estimated profit figure for next year?</i>	12%
<i>How many widgets did we sell last month?</i>	47,000
Information is data at work - data provided in response to a need or question.	

Within this document, any references to **information** mean **data imbued with a business meaning**. The term **data** will be used in the context of collecting raw facts for later use.

Applications

Applications are designed and constructed (or purchased) for several reasons:

- To capture, store, deliver, and report on data vital to the business.
- To ensure business data is collected, distributed and reported according to policy and standards.
- To increase business efficiency by automating repetitive manual processes and procedures.
- To ensure business policy and rules are implemented consistently and uniformly across the organization.

Hence, applications are the implementation and integration of business policy, business rules, business processes, data, and procedures.

Application Custodianship and related responsibilities have become clouded. Generally, custodianship of applications has been assumed, but not always made explicit. As a result of organizational changes within the ministry over time, Application Custodian identification has led to some confusion and lack of understanding. This document is meant to clarify and simplify the Application Custodian designation and related responsibilities.

[Back to top](#)

Custodianship Defined

Introduction to Custodianship

Managing Information as a Resource

Information is one of the most important resources the ministry has. There is a significant cost to gathering and maintaining good quality information, and the ministry cannot operate without it. Increasingly, information is being combined or updated by staff from many different areas, using different applications. Information from one program area is often relevant to many other program areas, and information from different program areas can and should be combined or integrated

to be of maximum use. The Custodian is responsible and accountable for managing corporate information or a corporate application as a vital resource on behalf of the ministry.

The integrity of this information is threatened unless proper care is taken. The ministry has therefore defined three roles with separate but teamed responsibilities to ensure a continuing focus on managing information as a vital resource:

1. **Data Custodian - Branch Director.** The branch director who establishes province-wide policy, definitions, and rules for business information within their mandate, to enable the ministry to gain maximum value out of the information.
2. **Application Custodian - Branch Director.** The branch director who sponsors projects to develop information systems, and provides ongoing support for those systems, to enable staff to meet business needs.
3. **Data Resource Manager - District Manager, Regional Executive Director** (also a Branch Director). A generic title for someone who is responsible for collecting and/or managing corporate data (to the standards set by the Data Custodian). The most senior manager in each office (e.g. district manager, regional executive director, or branch director) is ultimately accountable for ensuring corporate data collection and management is done properly (e.g. in the district) to enable effective business decisions.

In summary, the *Data Custodian* has the lead role in encouraging and enforcing data use and sharing throughout the ministry. The *Application Custodian* provides development and process support, to ensure data is in the hands of those who need it. The *Data Resource Manager* is accountable for ensuring high quality corporate data collection, entry, and management, to the relevant Data Custodian's standards. For more information about statements for insertion into job descriptions, see [Job Description Inserts](#).

The integrity and sharing of information across the ministry, and the exploiting of information to the ministry's advantage via applications are the key focal points of Data and Application Custodians. Custodians provide leadership, and treat their scope of responsibility as the entire ministry, not only their own organizational area. A Custodian enables cooperation, appropriate allocation of resources, and partnership throughout the ministry, and is accountable for determining the business information required by the ministry. This may involve influencing other program areas and stakeholders to convince them that proposed definitions and/or policies will meet the ministry's goals, and ensuring that conflicts between ministry business needs are successfully resolved.

Each discrete information subject (e.g. "Opening"; "Employee"; "Asset") and each application (e.g. "Timber Tenure Administration"; "Client Management") that is the responsibility of the ministry is assigned a single Data Custodian.

Overview of General Responsibilities

Data Custodianship involves two main areas of responsibility:

- *Information management*: establishing what business information is of interest to the ministry within the custodian's program area, and establishing definitions, policy, standards, and rules for that information; and,
- *Information sharing*: ensuring the information is available to the widest possible audience so that the ministry gains maximum value out of the investment made in that information.

Application Custodianship involves two main areas of responsibility:

- *Application development*: sponsoring projects to develop information systems that enable staff to meet business needs, including the provision of training on those systems; and,
- *Application management*: periodically enhancing applications where necessary, managing the change process where an application enhancement affects other ministry program areas, and providing application support to ensure the ministry's business needs are being met.

Data Custodian

In the past, applications were developed on a departmental basis, but the increasing use of shared database technology has changed the nature of these systems. Today, ministry information is well integrated. Because of this increased sharing, ways must be found to encourage the joint funding, sponsorship, and cooperation of information management across departmental, application, and program area boundaries.

A Data Custodian's responsibilities pertain to the creation and use of data for the purpose of enabling decision-making and providing information. At a detailed level the Data Custodian is accountable for information structures called *entities* and *databases* (see [Definitions](#)). These structures usually require some maintenance, improvements or enhancements, and updates over time.

Principles

- A single, explicit Data Custodian shall be identified for each set of corporate information (each "entity").
- Corporate Information must meet each of the following characteristics:
 - has a permanent or lasting nature
 - is essential to ministry operation
 - falls within the ministry's mandate
- Data Custodians plan and act in the best interest of the ministry (within their mandate), not only for the good of their own program.
- Data is a corporate (ministry-wide) asset, best exploited when shared extensively.

Responsibilities

Data Custodians are responsible for the structure and content of information the ministry needs to conduct its business, within the context of the Data Custodian's business area. The Data Custodian's obligations include:

1. Information management:

1. determining the business information required by the ministry: deciding what information is important for the ministry to record, and validating that the ministry's business interests are served by the investment in that information.
2. ensuring that core information requirements for all ministry interests are addressed: consulting with any program areas and Operations Division representatives that have a business interest in the information being collected.
3. establishing policies, procedures, definitions, standards, and guidelines: ensuring that definitions for ministry information structures (*entities, attributes, and spatial data structures*; see *Definitions*) are complete, correct, and understandable, from a ministry-wide perspective.
4. making decisions about public access, creation of records, and fee estimates as per the requirements of the *Freedom of Information and Protection of Privacy Act*.
5. taking steps to continually improve the integrity, accuracy, precision, timeliness, consistency, standardization, and value of information.
6. defining codes and edit rules to ensure completeness and integrity of ministry information.
7. deciding on appropriate levels of access to business information, providing authorization for security access rights and privileges to information for designated individuals or groups, and deciding on investigative and corrective controls to prevent the addition of unauthorized or inaccurate information to databases.
8. providing appropriate training to staff and others to ensure data is captured accurately and completely.
9. ensuring recovery of information by authorizing information retention rules, physical security programs, information disposal plans, and disaster and other recovery plans.
10. checking to ensure retention rules and other recovery plans are met.
11. acting upon requests for changes to ministry information requirements from other program areas, and soliciting cooperation from different program areas in realizing changes to ministry information requirements.
12. providing resources for the building of bridges or links to ensure access to common ministry information on different computer systems, where necessary. For example, there should be a single primary source for information, however, when additional related information resides on technology different from that of the primary source, then conversion, alteration, or transfer of existing information may be necessary. Two-way bridges may be required for loading, maintaining, and using common ministry data.

2. Information sharing:

1. ensuring the ministry obtains maximum value out of the investment in information by making the information known and available to the widest possible audience: information should be collected with the intent that it will be shared with any other program areas that may gain benefit out of its use.
2. marketing the decisions made about what the supported ministry information requirements will be: when decisions are made about what

data will be collected, other program areas will need to know about those decisions and understand the reasons for them.

3. influencing other program areas where necessary to convince those involved that the definitions and policies will meet the ministry's goals.
4. functioning as negotiator and arbitrator to achieve the best compromise in preventing or resolving conflicts in information use, interpretation, or meaning.
5. knowing how their information is affected by other business areas (conversely, knowing how *others* are affected by *their* information).

How to Identify

A Data Custodian is a Branch Director. District Managers and Regional Executive Directors cannot be Data Custodians because they do not have the mandate to act in a province-wide context. The Data Custodian for a particular set of information will be the Director whose branch has the corresponding business and policy mandate within the ministry. If this is not obvious, the Data Custodian can be identified through consensus at the Director level, or by using the Information Governance Council as a resource. Where necessary, the Executive will make a formal assignment.

If the information in question is within the mandate of another ministry, then by definition there is no Data Custodian within the Ministry of Forests and Range (see Steward - External).

Data Standards Manager

The Data Custodian will normally delegate the day-to-day responsibilities of custodianship (e.g. issue resolution) to one of their staff members -- this role is formally called the Data Standards Manager (DSM). This staff person does not necessarily have a management classification -- it is the person who takes care of the day-to-day management of the data standards, for the Data Custodian. See [MoFR list of DSMs](#).

Application Custodian

An Application Custodian's responsibilities pertain to the building of automated applications for the purpose of processing routine transactions, and enabling information retrieval and the resultant decision-making by ministry staff. Applications often access information from many different subject areas, and at a programming level access data from *databases*. It is essential for Application Custodians to work with any Data Custodians who control information in databases to which their application requires access.

Principles

- A single, explicit Application Custodian shall be identified for each corporate application.
- All application processes maintain the integrity of the data they act upon.
- By definition, applications reflect current business rules and processes.

Responsibilities

Application Custodians are responsible for ensuring that, within the scope of their application boundaries, the ministry's processing requirements are met through the accepted practice of multiple releases of an application over time. Applications that are built should ensure that data is collected and reported according to documented ministry standards. The Custodian's obligations include:

1. Application development:

1. determining the business information and application requirements that will be supported; providing leadership and including in any discussions staff from areas of the ministry most affected (e.g., policy or business rule experts, Operations Division representatives, etc.).
2. determining the relative priorities of business information requirements that are to be provided in each new application release (i.e. determining the scope of the project).
3. sponsoring projects to ensure the business needs of the ministry are satisfied, through applications that are developed from a corporate perspective.
4. coordinating implementation of the new application, including development of material for courses and providing initial training.

2. Application management:

1. accepting complete responsibility for any change process that affects the information resources of the ministry (i.e. affecting any program area's *information definitions*, and/or any program area's *applications*).
2. using scheduled releases to implement enhancements to applications.
3. providing ongoing application training for new users and making periodic refresher training available.
4. providing support to application users, assisting them in properly using the application within the context of their business functions. This includes investigation of application problems as well as providing assistance to users to show how the application can be used to support the business functions that staff are performing.
5. providing solutions to problems of a business nature that may arise. When an application release is implemented, there can be major effects on the business and on staff who use the applications. These effects often reach beyond the scope of the actual systems development project. For example, the development of application releases that enforce business rules must be timed properly so the releases coincide with changes to ministry policy or relevant BC Government Acts. The Custodian must deal with the issues that arise, and coordinate efforts to ensure the right decisions are made and appropriate action is taken.
6. negotiating or arbitrating to achieve the best compromise where there are conflicting interests.

Related Data Responsibilities for Application Custodians

- Data related to operational delivery / business design (process specific data)
 - responsibility of application custodian

- collected due to the manner in which the business is implemented - - relates to the processing of data, operational workflow or factors that include ministry resources required or technology options. (If the process or technology was different, then this particular type of data would not be captured or required.) e.g. work events
- Data related to the physical or technical implementation
 - responsibility of application custodian
 - e.g. control tables such as next skey number, update or create userid, security requirements

How to Identify

A) The Application Custodian is the ministry's Chief Information Officer (Director, Information Management Group) where there is a large degree of integration between applications, or applications share and utilize common ministry infrastructure. For example,

- RESULTS and Forest Tenure Administration (FTA) are widely used.
- Electronic Submission Framework (ESF) standards and services is the common ministry infrastructure for data collection.

B) The ministry's Data Custodian (the business or policy branch owning the mandate) retains Application Custodian title for applications implemented on a narrow (single-program or limited number of sites) or small-scale (only 1 or 2 users in each office) basis. For example,

- The Protection program applications are examples of narrow scale implementation (program confined to a limited number of sites).
- CAS (Financial Management Branch) and CHIPS (Human Resources Branch) are applications implemented on a small-scale - only 1 or 2 users in each ministry office.

C) Application Custodian title moves to the ministry's Chief Information Officer (Director, Information Management Group) where branches have *service delivery responsibility* and *large-scale utilization* in Operations Division (i.e. more than five users per district). For example,

- Forest Tenure Administration (FTA) is an example of an application with a large-scale implementation in Operations Division.

Applications that fall outside this defined model, or fall within several boundaries, will be reviewed by Branch Directors to avoid confusion. The Information Governance Council can be used as a resource to identify the single Application Custodian.

Data Resource Manager

District Manager, Regional Executive Director (sometimes a Branch Director). A generic title (capitalized) denoting the management or leadership responsibility within an office for collecting and/or managing corporate data (to the standards set

by the Data Custodian). The most senior manager in each office (e.g. district manager, regional executive director, or branch director) is ultimately accountable for ensuring corporate data collection and management is resourced and completed properly (e.g. in the district) to enable effective business decisions.

In addition, anyone who uses or updates information in any form is acting in the role of a data resource manager (note lack of capitals, in this case it is not a "title").

Steward

A sub-classification of the Data Custodian is a **Steward**, who at the request of and on behalf of a Data Custodian, can ensure that a set of the Data Custodian's information is available, if that Data Custodian does not have the appropriate operational resources available to provide the necessary functions. The Steward chosen must already be a Data Custodian for other program information (since by definition the Steward must have access to operational resources relating to managing data standards province-wide).

The Data Custodian remains fully responsible for the information with respect to the business, but can delegate technical or operational portions that may be better dealt with by other experts. In other words, the Data Custodian is responsible for specifying *what* information is recorded but might delegate the decision of *how* it is stored and retrieved province-wide to a Steward. The Data Custodian specifies the business use of the information including structure, format, content, and how the information relates to other business information. The Steward might then ensure that, for a particular operational platform, the integrity of the information meets the published standards. The Steward will have only limited responsibility for information content.

Responsibilities

The scope of each Steward's responsibilities depends on the particular arrangements made between the Steward and Data Custodian, however, Steward responsibilities will always be a *subset* of Data Custodian responsibilities. The primary purpose and responsibility of a Steward is:

- to provide adequate resources to sustain the essential quality of the information in question; to manage the standards for the information in its physical environment (province-wide) and ensure that its integrity is intact relative to its business meaning, as specified by the Data Custodian.

The following list contains suggestions where identifying a Steward may assist custodians in managing their information resources. A Steward might assume some or all of the following obligations, depending on the needs, resources, and decisions of the Data Custodian:

- providing access to corporate information identified by the Data Custodian and based on access authorization developed by the Data Custodian. No responsibility for the capture, content, or accuracy of the information is assumed.

- authorizing physical security, disaster recovery plans and procedures, retention plans, and disposal plans for information, to ensure physical recovery of information in disaster situations.
- providing resources for the building of links to ensure access to common ministry information on different computer systems, where necessary. For example, there should be a single primary source for information; when additional related information resides on technology different from that of the primary source, then information conversion, information transfer, or alteration of existing information may be necessary. Two-way links may be required for loading, maintaining, and using common ministry data, however where possible should be avoided.
- notifying the Data Custodian when requests for changes to ministry information requirements are made. Assisting the Data Custodian by soliciting cooperation from different program areas in realizing changes to ministry information requirements.

The following table may help to describe the differing levels of responsibility between the Data Custodian and the Steward.

Data Custodian	Steward
Defines data requirements to a standard specific level (information content) - retains responsibility for <i>what</i> business data is recorded.	Processes data into the physical platform and manages the data thereafter from a technical perspective - might be responsible for <i>how</i> data is recorded.
Defines and publishes business specifications for spatial data requirements.	Ensures the data entering the physical platform meets the published standards in terms of format (representational and positional), and <i>limited</i> content.
Defines and publishes business specifications for spatial data requirements.	Assists in defining physical specifications for spatial data requirements where technical expertise is scarce and the Data Custodian does not have access to such expertise (e.g. where spatial/GIS data management is pushing the boundaries of available technology).

Principal Data Areas

The [Principal Data Areas](#) list shows the Data Custodians in the ministry, and lists the major data holdings they are each responsible for.

[Back to top](#)

Corporate vs. Non-Corporate Data

The quality of any data that is essential to the ministry's operation must not be eroded; it must be continually improved. To ensure this, the ministry expends significant resources ensuring its data remains accurate. To assist custodians in

making a decision about which types of data really are *essential to the ministry*, the terms **Corporate** and **Non-Corporate** are used.

Full Corporate Data

In general, corporate data is defined to be data that is

- of a permanent or lasting nature;
- critical to the operation of the ministry;

and, it is implied that usually corporate data is potentially used by many staff or by different program areas.

Because of its importance, full corporate data is

- managed rigorously:
 1. a Custodian is identified who is responsible for ensuring it meets ministry needs;
 2. standards for definition, collection, accuracy, entry, use, update, disposal are developed so the information is used consistently across the ministry;
 3. a primary physical source is identified so all staff know how to get the latest information.
- relied on to be accurate, meaningful, and available.

This stringent management of data has a significant cost. This cost must be weighed against the value of the data in terms of making business decisions. When the decision is made by the custodian that the cost is too much relative to the data's value, one can infer that the data is *not* critical to the operation of the ministry.

Full Corporate data can be further designated into two distinct sets: **Shared** and **Program-Specific**.

Shared - Full Corporate

Corporate data is generally, though not always, shared across one or more programs or between several offices. The distinction **shared** means the information must be treated with the highest standards of care and cooperation between ministry programs. Shared data generally affects several different program areas, and any change to such data invariably affects multiple computer applications, policies/procedures, and/or ministry business itself.

Program-Specific - Full Corporate

There is also vital data that requires careful management, but is not shared at all with other program areas, or is only minimally shared (e.g. Lightning Location). This data must still be designated corporate since it is so vital to the ministry, however, since the effect on other areas as the result of a decision about changing the data is slight, it may not need to be managed with quite so much rigor. All users of the data

are within the program's accountability line, so the custodian will be cognizant of all relevant factors and be better able to consciously manage the risk involved. In a management sense, the custodian is the user for program-specific corporate data.

Extended Corporate and Local Corporate Data

Extended Corporate data is data whose structures (i.e. how the data is stored) have been published across the ministry (contact [Data Administration staff](#) for more information), and when data is stored, it is stored on a ministry corporate platform (e.g. an office LAN where there is professional management -- NOT on a personal computer).

Local Corporate data is that data defined and collected within an office, and not usually shared.

For more information on the above two categories, see the [Corporate Data Categories](#) document.

Non-Corporate Data ("Personal" Data)

Because the cost of managing corporate data is so high, a definition is needed for data that is still useful, but not relied on nearly so much for making critical decisions or providing specific information. This data can be termed Non-Corporate data. Care must be taken in the use of such data: since there is little investment in ensuring non-corporate data is accurate (no standardization in collection procedures, etc.), it should not be relied on without extremely well-informed judgment.

Non-corporate data could be data that is personally created and does not need to be shared. This may include scraps of paper, temporary files, some word processing files or spreadsheets, output files, or input files that are not shared for business purposes. Non-corporate data might be created to help answer tactical questions that operational-level corporate data is not quite in the best format for.

Non-corporate data could also be a copy of corporate data, taken at some point in time and manipulated outside of the corporate infrastructure (i.e. without regard for the defined standards for use and update of corporate information). *As soon as the copy of corporate data is taken, it becomes non-corporate data.*

Proportionally few resources are expended on the gathering and maintenance of non-corporate data. This makes non-corporate data easier to obtain but more dangerous to use, because to use the data properly the user must know more about where that data has come from, how it was gathered, and what transformations it has gone through. If the use of non-corporate data might lead to erroneous or inaccurate assumptions, then it should not be used.

[Back to top](#)

Information Management Group Role

The Information Management Group's (IMG's) mandate as it relates to custodianship is to build the appropriate infrastructure so the ministry can effectively put

information to use. To complete this mandate, IMG ensures the infrastructure (that is, the communications networks, databases, systems development procedures, quality assurance standards, technological vision, etc.) can be used to sustain the integrity of ministry business information. It is then up to each Data and Application Custodian to use that infrastructure appropriately according to their business needs.

IMG's specific responsibilities with respect to the Custodianship policy revolve around assisting ministry program areas to recognize and deal with their corporate and integrated/shared data responsibilities, building and maintaining the corporate database, and providing assistance and coordination in the systems development process. IMG is responsible for the integrity of the physical corporate database, that is, ensuring that the shared on-line computer platform (machine, network links, development standards, development methodology, development software and languages, development procedures) and application development environments are robust and stable, and can be trusted to perform as expected.

For *shared corporate data*, these responsibilities require IMG to ensure that Data and Application Custodians do not implement changes to the shared corporate database that would directly affect data from other program areas, unless each relevant Data Custodian has approved of the change.

For *program-specific corporate data*, the Data Custodian assumes more of the responsibility for determining risk when planning modifications.

IMG's mandate and responsibilities do not extend into the business arena. IMG staff cannot dictate to Data or Application Custodians how they should run their business. Changes to the business, and all business-related decisions, must be actively prepared for and dealt with by the Custodian.

Policy changes on IMG's role

A Custodian will actively manage the implementation of changes for their area, and where their actions affect others' information resources. This includes assessing potential Ministry-wide impacts to policy, procedures, systems, and resourcing whenever there is a proposed change in one or more of those areas.

As a systems specialists, IMG is jointly responsible, along with business specialists (e.g., Resource Tenures & Engineering Branch, Forest Practices Branch, Financial Management Branch, etc.) and representative Data Resource Managers (districts and/or regions), for impact assessments such as to investigate and analyze potential impacts on corporate information and applications system before drafting changes

IMG as Ministry's Application Custodian

IMG is the ministry's application custodian and is responsible for building automated applications for processing routine transactions and aid ministry staff with information retrieval and decision-making based on the information retrieved. IMG also develops most of the applications in the ministry and manages them, from the application side, for business areas. However, IMG is not the custodian for applications implemented on a narrow (single-program or limited number of sites) or

small-scale (only 1 or 2 users in each office) basis. Those applications are managed by the ministry's Data Custodians instead.

[Back to top](#)

Integration Process and Issue Management

The process of building and maintaining a corporate database is complicated and takes a lot of cooperation and coordination between the areas of the ministry that are custodians of information and applications. This section will describe the process that is required to develop and maintain the corporate database while developing and maintaining the applications that work on the corporate database. Any change to or deletion of a data structure in the corporate database needs agreement and planning by all the custodians of applications that access that data.

Identification And Resolution Of Data Changes

1. The triggers that will bring the data issues to light are:
 1. Business Area Analyses
 2. New Applications
 3. Releases of Applications (which include changes in business rules, new legislation, user requested enhancements, etc.)
 4. Information Access (ISB program to deliver copies of corporate data to office LANs)

Note: What is likely to happen in the Information Access scenario is that a user may discover that some data they require is not available or is not defined as they require it. The process for resolving issues triggered by Information Access will be the same as described below except that since the issue will not have come to light during a project, the issue will be referred to the Data Custodian to initiate discussions.

2. Issues will be identified through data modelling done in the projects. Data issues may also be recognized before the data modelling process identifies them; they should be dealt with *when identified* by the Data Standards Manager(s) involved (see [Definitions](#)).
3. The Data Administrator (Information Systems Branch) and the Data Standards Manager(s) involved in the projects are responsible for identifying the issues.
4. The Data Standards Managers for all the branches affected by the data issue and the Data Administrator will meet to clarify the requirements, define the issues, assess the impacts, define the alternatives, and finally to produce a recommendation to proceed. The recommendation to proceed goes to the Project Sponsor.
5. If the issue cannot be resolved at the Data Standards Manager level, the issue must be referred to the next level of authority: the Project Sponsor. A *Data Issue Bulletin* should be developed that describes the issue, the effect to ministry business, and alternatives. The Data Issue Bulletin could be initiated by a Data Standards Manager or the Data Administrator. The bulletin will be distributed to the relevant Data Standards Manager(s), Data Custodian(s), Application Custodian(s), and the Project Sponsor. The Project Sponsor and

the Data Custodians will resolve the issue with input from the Data Administrator as required. The Project Sponsor will be supported by the Project Manager and the Data Custodians will be supported by the Data Standards Managers.

6. If the issue cannot be resolved at the Project Sponsor/Data Custodian level it will be escalated to the Executive by the Project Sponsor.

Project Responsibility For Changes

1. The Project Sponsor is responsible for ensuring the planning is done for the changes being scheduled. This means it is their responsibility to ensure that all Application Custodians who have to modify their applications because of the change to the database, plan and schedule their projects to coincide with the database change.
2. The Project Manager responsible for the project that initiates the database change(s) is responsible for documenting the application dependencies in the project plan so the DataBase Administrator (DBA) can ensure the changes made to the database have been approved by all the Application Custodians affected. The method the DBAs have to ensure that all approvals have been received is by comparing the signatures on the migration requests to the dependency list in the project plan. The DBA will refuse to make changes to the corporate database when they have not received approval for the changes from all application areas affected. The DBA has the ability to check that all the applications that could be affected have been listed in the project plan.

Characteristics Of Integration Issues

All changes to data stem from ministry policy/procedures, which means that a change in one policy/procedure that causes a data change in the corporate data model may also require change(s) to other policy/procedures.

Any addition, deletion, change in size, or change in definition to a piece of data in the corporate data model has the potential to affect every application that uses the corporate data model, whether the applications use that particular piece of data or not.

Depending on what the change is to the piece of data in the corporate data model, the scope of change(s) required to applications and policy/procedures may be small, very large, or somewhere in between. The only way to understand the scope is for the Data Custodians and Application Custodians to have the policy/procedures and the applications analyzed. The effect of the changes must be analyzed with regard to the ministry as a whole on the basis of cost, timeframe, effort required, and the effects on people and the business.

Funding for maintenance of and enhancement to the ministry's applications comes out of STOB 25 (program Branch or Operations Division responsibility centres). The Application Custodian is responsible for funding maintenance and enhancements for their applications; in addition, an Application Custodian who creates a change must ensure other affected Custodians are able to fund any changes they would then require. If not, it is the creator who must either escalate the funding problem or fully support its escalation, including informing the Director, Information Systems.

Roles Matrix

Roles matrix not available in HTML format at present

Process Flow

The [process flow diagram](#) [12kb] shows a general procedure for implementing change within a modelling or systems development project. (Note: in May 1997 the definition for "Data Resource Manager" changed to mean staff who collect and manage data, and the term "Data Standards Manager" began to be used for the Data Custodian's staff help. This diagram has not yet been updated with "DSM" wherever "DRM" is displayed, **so when you see DRM, it really means DSM!**)

[Back to top](#)

Definitions

Word/phrase	Definition
Application	A series of computer programs that are developed primarily to support the business of the ministry in a particular program area; a part of their function is to allow users to use, update, and manipulate information contained within the ministry's databases. An application can also be called an <i>Information System</i> or <i>Application System</i> .
Corporate Application	A computer application that affects corporate information or is designated at the planning stage as a corporate application, thus requiring the highest levels of quality assurance in its development.
Corporate Data or Corporate Information	Data that is of a permanent or lasting nature and is critical to the operation of the ministry, potentially used by many staff or by different program areas. Because corporate data is relied on to be accurate, meaningful, and available, it is managed rigorously according to standards for definition, collection, accuracy, entry, use, update, and disposal. For more information see the Guide S35 section titled Corporate vs. Non-Corporate Data .
Corporate Database	A set of multiple repositories designed for the electronic storage of shared ministry information within a managed environment, and functioning over a long period.
Custodian	A branch director, who is responsible and accountable on behalf of the ministry for an information resource or an application. A custodian provides leadership and treats their scope of responsibility as the entire ministry, not only their own organizational area. For more information see the Guide S35 sections titled Data Custodian and Application Custodian .
Data Administrator	The position responsible for providing leadership to the ministry in information resource management. Information resource management includes development of standards for the use and manipulation of data, promoting

	improved quality, more interest in and better access to corporate information, and orienting systems development towards the use of shared data. The position is in Information Management Group, and its mandate is for the entire ministry (i.e. not just for a branch).
Data Resource Manager (DRM)	The staff responsible for collecting data at the field level (although ultimate accountability rests with the senior manager of the office, e.g. the District Manager). They are accountable for collecting Corporate data <i>to the standards set by the Data Custodian</i> . The DRM is a key role for the ministry: where Full Corporate data does not exist, they will determine what data is important enough to define it Locally or begin moving it into the Extended Corporate category.
Data Standards Manager (DSM)	<p>A position that reports to a Data Custodian, and is accountable for performing the day-to-day operational responsibilities of information management within the Data Custodian's mandate. The Data Standards Manager fully understands the data requirements of their program area and how the program uses data within the corporate ministry context, and is the first point of contact for any access to program area information. The DSM is responsible for resolving any business issues that involve data within the scope of the program area, including data associations to other program areas.</p> <p>In large, complex program areas, a Data Custodian might split the business area up and assign Data Standards Managers as being responsible for one or more portions. For each portion, there may be a single DSM responsible. Specific responsibilities, and the number of DSMs that exist for the entire business area, are decided by the Data Custodian. However, where more than one Data Standards Manager exists in a program area, one of them should be identified as the single point of contact and responsibility for associating with those outside the program area. This will ensure minimum confusion when cross-program issues are being dealt with.</p> <p>A Data Standards Manager's responsibilities go beyond systems development projects (see Project Sponsor and Project Manager), because business issues and ministry information requirements are not constrained by project boundaries.</p>
Database	<p>A place where information is stored within a computer system.</p> <p>A database's contents are determined by its corresponding entity definitions (see Entity). For example, the <i>Client</i> database would contain the name of each client known to the ministry, along with all other information pertaining to Clients. A database is made up of many <i>database views</i>; each database view is built from a single entity definition.</p>
Data vs. Information	<i>Data</i> is an individual fact or multiple facts. <i>Information</i> is data with meaning - data provided in response to a question. For

	<p>more information see the Guide S35 section titled Data vs. Information.</p>
Entity	<p>A person, place, thing, or concept in which the ministry has a business interest, and for which the ministry must record information, including spatial information (e.g., information in terms of geographic location and features). For example, <i>Clients</i> and <i>Tenure Agreements</i> are entities. An entity is defined only once within the context of the ministry's business.</p> <p>The definitions of entities are the fundamental building blocks for determining the ministry's information needs. Each entity is defined with a specific description and common attributes. For example, the attributes for <i>Client</i> would include the client's <i>name, address, and phone number</i>. This information is physically stored in a database to provide automated access.</p> <p>Each entity is governed by a single Data Custodian.</p>
Project	<p>A management undertaking to define and plan for the scope of change to the way the ministry does business.</p> <p>Projects should have a clear statement of objectives. Depending on the scope of the project and the amount of business change required, projects involve most or all of: identification and resolution of business issues, policy changes, application development, implementation planning, and preparing and delivering staff training and education. There may be organizational or staffing implications, or external timing considerations.</p> <p>Usually a project is a major undertaking requiring many months or years, considerable expenditures for contracted assistance, and significant staff involvement and commitment.</p>
Project Manager	<p>The Project Manager reports to the Project Sponsor, and is responsible for directing and tracking the day-to-day activities that ensure the success of the project.</p>
Project Sponsor	<p>The person from the program area that acts as the champion for the project, has overall management responsibility for a project, and provides leadership and direction to the project team.</p> <p>The Project Sponsor ensures adequate funding and staffing are available, and decides what the critical success factors are for the project to meet the ministry's business needs. The sponsor will often be the Application Custodian for the existing or proposed application.</p>

Got a word or phrase from Guide S35 you don't understand? [Let us know](#): we'll get back to you with an answer and probably update the guide as well.

[Back to top](#)
[Back to Data Administration Section](#)

