Government of Manitoba
Enterprise Architecture

Principles, Strategies and Directions

Manitoba Information & Communications Technologies
Department of Energy, Science & Technology
March 2005

Manitoba
Building for the Future

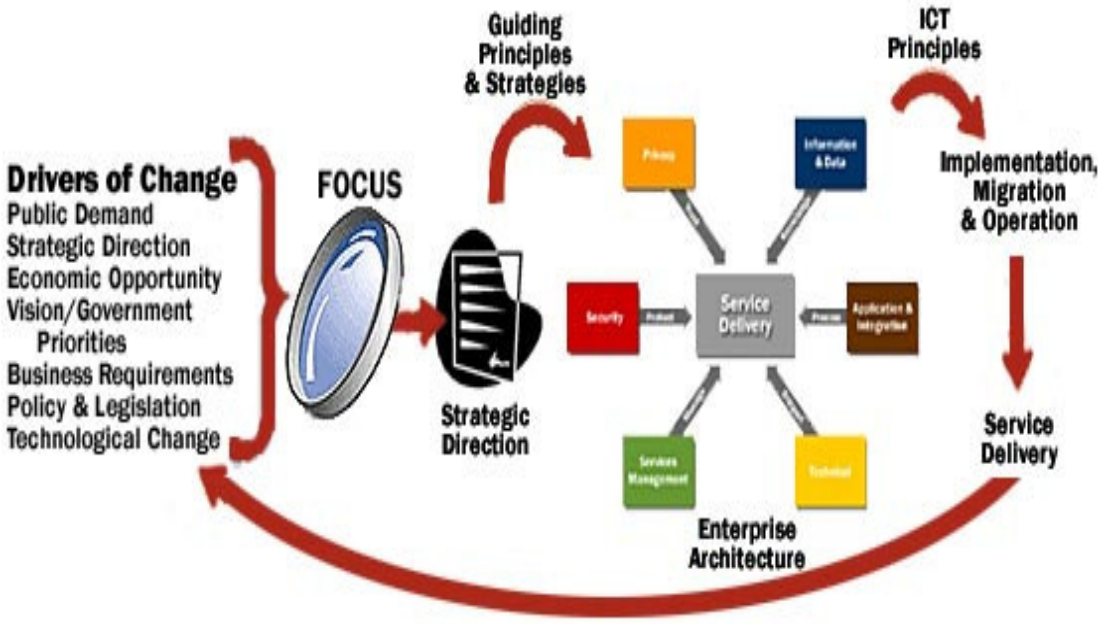
Manitoba's Enterprise Architecture

Manitoba's Enterprise Architecture guides the development, deployment and operations of Information Communication Technology (ICT) systems for the Government of Manitoba. It contains a number of ICT principles, strategies and directions that support the goals of the government, program delivery, while aligning ICT across government.

Manitoba is broadening its service direction toward an overall "citizen first" orientation to meet citizen need. Information and communication Technologies (ICT) are a strategic component of the government's overall vision for service improvements and access to public information.

The Government of Manitoba must have an ICT environment that is flexible and responsive to change leaving a window open for new ideas and innovations that support the government's commitment to improve services and program delivery for the direct benefit of Manitobans.

The Enterprise Architecture reflects the influence of a number of external and internal drivers and service delivery requirements as pictured below. By understanding the impacts of these drivers government can direct the selection, use and operation of technologies needed to support government business requirements.



ICT Guiding Principles

The ICT Guiding Principles guide the provisioning of ICT systems and services focusing on improving government's ability to deliver services to Manitobans. The principles that guide the development and provision of ICT services in the government are:

GP1: ICT systems and services must be designed to accommodate rapid change to government programs and services.

Strategies

1.1 Build applications using open, portable, web-enabling technology that facilitate interfaces and linkages among applications, databases and legacy systems.
1.2 Re-use already developed components in application development.
1.3 Develop enterprise-wide standards and processes based on industry generic standards and products where practical and possible.

GP2: ICT systems and services must facilitate legitimate access to information while providing strict control over the collection, management, and security of this information in accordance with freedom of information and privacy (FIPPA & PHIA) legislation.

Strategies

2.1 Implement content and knowledge management frameworks that address the creation, capture, maintenance, accessibility, dissemination, and use of information.
2.2 Promote a librarian function for these frameworks.
2.3 Review and update existing systems to meet the requirements of freedom of information and privacy legislation.
2.4 Leverage inter-jurisdictional efforts in user authentication.

GP3: ICT systems and services must support and encourage interaction between constituents and the government.

Strategies

3.1 Use technologies such as the Internet, electronic information repositories, online transaction processing, telephone, and facsimile to facilitate multi-channel access to services and encourage open communications.
3.2 Investigate opportunities to better serve the public through meaningful partnerships with other levels of government.
3.3 Establish a reliable, end-to-end financial infrastructure to allow on-line transactions, payments, and procurement for information and services.

GP4: ICT systems and services must promote the accessibility and integration of government services by providing a standards-based enterprise view of services that cross organizational boundaries.

Strategies

4.1 Provide a single, consistent and accurate source of information.

4.2 Integrate applications and implement data standards to achieve information consistency across all access channels.

4.3 Manage projects as an inter-related group of activities (i.e., not in isolation of each other). Opportunities for reuse of infrastructure components such as shared servers, networks, databases, information, and software, will be identified.

4.4 Provide an easy-to-navigate interface, allowing citizens and businesses to interact with government, and civil servants with access to the information and systems they need to deliver services.

4.5 Maintain an ICT infrastructure that is based on standards.

GP5: ICT systems and services must align with the program planning and delivery requirements of the government and its stakeholders.

Strategies

5.1 ICT investment decisions will be based on the established priorities of the government's program planning and delivery requirements.

5.2 An investment management framework will be followed to develop ICT business cases.

5.3 Provide staff with the appropriate technology and training needed to meet increasing expectations from a technically well-informed citizenry.

GP6: ICT systems and services must facilitate access to government services with a goal of "anywhere at anytime" where practical.

Strategies

6.1 Develop applications in a manner that minimizes dependence on the channel used to access the service.

6.2 Make information systems available to all users 7x24 where the demand for a particular service warrants it.

6.3 Develop a Business Resumption Plan to ensure that continuous service is maintained

Architecture Domain Applied Principles

Architecture Domain Applied Principles are statements of preferred direction or practice. Principles form the basis of the rules, constraints, and behaviours with which an organization complies in its daily activities. Principles may change over a period of time, as the organization's mission, delivery requirements, business, or operational environment changes

Manitoba's Enterprise Architecture contains six domain architectures, each with a number of applied principles that have been developed specifically to guide decision making related to areas contained in the domain.

1. Privacy Architecture Principles (PAP)

PAP1: Accountability

Direction

1.1 All systems must be capable of being auditable.

1.2 Program Managers are accountable for ensuring system compliance with privacy legislation and policies. A privacy impact assessment may be advisable.

1.3 All contracts for electronic information systems and services must include terms and conditions requiring contractors to comply with all relevant privacy and retention requirements and policies. Legal counsel should be consulted when developing requests for proposals, contracts, etc. to ensure all legal requirements, including privacy requirements, are met.

PAP2 : Limits On Collection

Direction

2.1 It is the responsibility of the program manager (or designate) to verify the authority for the collection of personal and personal health information as part of the system development process.

PAP3: Collection From The Individual

Direction

3.1 Systems must include reasonable provisions to verify the identity of the individual personal information is about.

NOTE: Examples might include error checking for external facing systems to the provision of information collection guidelines accessible by agents for internal facing systems.

PAP4: Identifying The Purpose Of Collection

Direction

4.1 When collecting personal and personal health information systems must reveal the following at the time of collection.

- Purpose
- Authority
- Contact information

NOTE: External facing systems (i.e. where information is collected *by* the system) must reveal the above at the time of collection. Internal facing systems (i.e. where information is input by an agent) must reveal the same information to the agent to enable them to provide it to the individual.

PAP5: Access To One's Own Information

Direction

5.1 Systems must be designed in a manner that enables the retrieval of personal information and personal health information as needed.

5.2 Systems must be capable of producing records of personal and personal health information in a form usable by an individual who makes a request for access.

5.3 Systems must be designed so that personal information and personal health information (when in identifiable form) can be unequivocally attached to an identity, thereby reducing the risk that information regarding the wrong individual is provided in response to a request for access.

PAP6: Correcting One's Own Information

Direction

6.1 Systems must be capable of effecting changes to personal and personal health information.

6.2 Systems must provide a mechanism for tracking refusals to correct information and for indicating the presence of statements of disagreement.

6.3 Systems that have external (beyond the department or agency) relationships must have the ability to propagate changes to the data and track changes for audit.

PAP7: Accuracy

Direction

7.1 Systems must record the source and date of collection of personal and personal health information to enable the assessment of data accuracy and integrity.

7.2 Further steps to ensure reliability and integrity of information are covered in the Information Architecture.

PAP8: Consent To Use And Disclose

Direction

8.1 Where consent to use or disclose person or personal health information is required, systems must be capable of recording consent.

8.2 Where consent is refused, systems must be able to accommodate refusal.

PAP9: Limits On Use

Direction

9.1 Systems must have the ability to limit access to personal and personal health information based on differing levels of authorization.

9.2 Systems must have the ability to manage access to personal and personal health information by verified individual authentication.

See also the Security Architecture.

PAP10: Limits On Disclosure

Direction

10.1 Systems must have the ability to limit access to personal and personal health information based on differing levels of authorization.

10.2 Systems must have the ability to manage access to personal and personal health information by verified individual authentication.

10.3 Systems must have the ability to indicate an individual's instructions not to disclose information retained in the system.

10.4 Systems must be able to accommodate entries based on consent and refusal of consent.

PAP11: Safeguarding Personal Information And Personal Health Information

Direction

11.1 Systems that collect or maintain personal health information must be capable of logging successful and unsuccessful attempts to view, add to, delete, modify, or transmit information.

11.2 Systems must have safeguards to prevent personal information and personal health information from being intercepted by unauthorized persons when transmitted by electronic or other means.

11.3 Systems must have safeguards to prevent unauthorized access to repositories of personal information and personal health information.

PAP12: Openness

Direction

12.1 Systems must be capable of publishing practices and policies regarding personal and personal health information.

PAP13: Records Retention And Destruction

Direction

13.1 Record retention schedules must be established by departments and agencies before records are created.

13.2 All systems that contain personal information and personal health information must support the ability to retain the information for the period of time designated in the approved record retention schedule.

13.3 All systems should be capable of creating and maintaining a record of destruction of personal and personal health information.

13.4 Destruction of electronic information must include permanent erasure.

PAP14: Challenging Compliance

Direction

14.1 Systems must be designed to support investigation of complaints related to the collection and handling of personal and personal health information.

2. Security Architecture Principles (SAP)

SAP1: Information Protection policies, standards, procedures and systems must be implemented in accordance with Government of Manitoba policy to ensure alignment with service delivery requirements.

Direction

1.1 Use security mechanisms to isolate public access systems from mission critical resources.

1.2 Ensure no single point of failure for critical information systems.

1.3 Utilize simple, security mechanisms that can be leveraged.

1.4 Documented analysis will be conducted at an appropriate (not excessive) level to arrive at a reasonable solution prior to implementation to ensure protection of information while using resources responsibly.

1.5 Solutions will be developed interactively with an emphasis on simplification and standards with repeatable solutions for common function.

SAP2: Information protection must permeate the Government of Manitoba and its ICT infrastructure and must be monitored and maintained on an ongoing basis.

Direction

2.1 Technology solutions that use resource (i.e. application-level) security will be implemented before network solutions to provide appropriate security for service delivery function while maintaining network function.

2.2 End users will by default have the least amount of access to resources (applications, files, etc.) required to perform their delivery functions, while internal networks will seldom be restricted with the exception of high security zones.

2.3 Connections to external networks will be heavily restricted.

2.4 The principle of least privilege will be applied to electronic information resources and external network connections in order to protect information resources.

2.5 The principle of most access will be applied to internal networks to maintain internal network access and the flexibility to change.

2.6 Resource and network security will be actively monitored to protect information resources.

2.7 Integrity, confidentiality, and availability of information should be

maintained in transit as well as in storage and when being processed.

2.8 Security services and mechanisms should be re-evaluated periodically to keep pace with requirement changes and technical refresh.

SAP3: Information Protection issues must be regularly communicated at all levels of Government to ensure awareness, appropriate behaviour and reduced risk.

Direction

3.1 A comprehensive plan for communicating the Government of Manitoba security policy must be developed and sustained on an ongoing basis.

3. Data & Information Architecture Principles (DIAP)

DIAP1: Information is a Government of Manitoba asset and will be accessible and reliable, while preserving the integrity of the information, to support government decision making and program delivery.

Direction

1.1 Standard interface components will be used to permit the authorized flow of information among disparate systems.

1.2 Security systems will be put in place to authenticate access to information.

1.3 Appropriate protection mechanisms will be implemented based on the value of the information and the guidelines identified in the ICT Security Architecture.

)IAP2: Information will originate from a single reliable information source with a clearly defined steward.

Direction

2.1 A steward will be defined as the owner for each information source within the government.

2.2 A single originating source will be identified for each type of information across the enterprise.

2.3 An inventory of information and associated stewards will be developed and maintained.

DIAP3: Common information and data elements will be consistently defined and used across the enterprise.

Direction

3.1 A repository of shared schemas will be developed and maintained.

3.2 Common information and data elements will be used when designing systems, reducing inconsistent and overlapping information and data elements.

3.3 A common data dictionary and data standard will be established.

3.4 A governance mechanism will be established to assist in mediating between stewards with conflicting data and information requirements.

4. Application & Integration Architecture Principles (AIAP)

AIAP1: Consistent application development, integration and maintenance processes will be used across government.

Direction

1.1 Develop a Governance model to ensure that necessary administrative and decision-making structures are in place to support Application Development. Roles and responsibilities of the various organizations and committees will be established. Resources in these roles will plan, approve, develop, document, champion, and enforce compliance to standards for application and integration development, maintenance, and technologies.

1.2 The Governance model, once developed, will pilot the process with an actual development project, receiving supporting resources (i.e. expertise, funding) to ensure the processes are efficient and to transfer knowledge to development and development personnel.

1.3 The Governance model will provide guidance and resources (i.e. expertise, funding) as initiatives are proposed and planned. This will ensure that the processes for application development and integration are followed.

1.4 Establish the application development and maintenance processes, as well as integration standards to be used across the government.

1.5 Establish the capturing of integration requirements as part of the requirements gathering process.

1.6 The processes and standards will include guidance on:

- Business process transformation
- Requirements gathering and management
- Architecture and alignment
- Planning and design
- Components and Integration

- Development and test environments
- Testing (e.g. functional, stress/load, regression testing)
- Security
- Resilience and Manageability
- Documentation (e.g. breadth, depth, format, style)
- Acceptable integration protocols and standards
- Appropriate integration models (e.g. publish/subscribe; push; request/response; broadcast)

1.7 Use International standards (e.g. IEEE/EIA 12207 and SEI CMM) as the basis for Manitoba standards although no actual certification will be required.

1.8 Identify a champion who will establish buy-in from all development organizations through the demonstration of effectiveness of the process.

AIAP2: Application development will encourage the reuse of existing components, and will identify and communicate opportunities for developing standard, shareable, and reusable components, processes, and services.

Direction

2.1 Establish a repository for the collection and storage of components for reuse.

2.2 Establish a librarian function to harvest and manage the catalogue of sharable assets.

2.3 Establish guidelines, practices, and funding to ensure that shareable and reusable components are developed.

2.4 Establish acceptable protocols, transports, and other integration standards.

2.5 Establish an enterprise event model that can be used to facilitate better integration.

AIAP3: Applications must be developed to minimize barriers to delivery across multiple access channels.

Direction

3.1 Decouple the application presentation layer from business logic to provide greater flexibility of adding new access channels without changing the business logic.

3.2 Focus on delivering services across the most common channels (e.g. web-based services).

3.3 Establish and adopt best practices and patterns for application development and integration.

AIAP4: A standardized set of tools must be adopted for use in all application development.

Direction

4.1 Establish a standard set of tools that meets the requirements of Class 1, 2, and 3 technologies.

4.2 Establish a process to ensure that this toolset is maintained, up to date, and adhered to by developers across the government.

4.3 Harmonize tool set use practices across the enterprise.

AIAP5: Application and information access components should be abstracted, catalogued, and packaged as services to integrate applications across the government.

Direction

5.1 Establish a common catalogue of services that will define services and interfaces to the services.

5.2 Abstract integration services into a series of layers to allow integration to be performed at the most appropriate layer.

5.3 Services will not be tied to a particular transport or delivery mechanism.

5.4 Abstract integration strategies from the implementation using a Published Service Model.

5.5 Establish a directory that represents the catalogue of assets to hold service metadata and facilitate service lookup and connection.

AIAP6: Application and integration components should be bought vs. built where they adhere to the Enterprise Architecture and Standards.

Direction

6.1 Establish a common catalogue of standards, standard components, frameworks, and service that will define standard application environments.

6.2 Ensure the business need is adhered to first before applying technology solutions.

6.3 Establish a mechanism for addressing deviations from the Standard Application Architecture, and governance for decision making when a potential purchase can be made and it doesn't fully meet standards or adhere to the Enterprise Architecture.

IAP7: A common language and business model (vocabulary, syntax, and semantics) will be adopted within the Government of Manitoba.

Direction

7.1 Adopt Extensible Markup Language (XML) as the language for Business Integration.

7.2 Identify and catalogue all the Government of Manitoba's business information domains and opportunities for business process integration.

7.3 Develop criterion, such as Return on Investment (ROI) for establishing document adoption and integration opportunities.

7.4 In consultations with business sponsors and data stewards, prioritize the list of information domains and integration opportunities:

- In priority order, each information domain must be analysed,
- Perform a prior art search in similar domains
- Make an adopt vs. build decision
  - For adopt, analyze the delta
  - For build, consider deferring till a public schema has been identified
- catalogue and publish the resulting document schema

7.5 The identified schemas and formats should receive first consideration as native data formats for new application development.

7.6 Identify subsequent integration opportunities.

5. Technical Architecture Principles (TAP)

TAP1: Technology standards and solutions are driven by business requirements gathered from stakeholders to encourage the development of shareable services that can be leveraged.

Direction

1.1 Gather Business requirements as part of the design of all technical solutions.

1.2 Leveraged and shared solutions across the government will be preferred to point solutions.

1.3 Track emerging technologies to identify opportunities to improve government service delivery through technology.

˙AP2: Technology standards will be maintained and extended into new areas to make better use of government resources and to promote integration within government and with business partners.

Direction

2.1 Set Technology standards for the purpose of guiding technology deployments and ensuring integration of services as delivered by Service Providers and business partners who support the Government of Manitoba program delivery.

2.2 Technology standards maintained and kept current for all technologies deemed strategic in support of Government of Manitoba program delivery.

2.3 Government of Manitoba employees will be involved in both the selection of strategic technology standards as well as establishing the technology training requirements.

TAP3: A life cycle management plan is required for all infrastructures.

Direction

3.1 Develop a life cycle management plan template to ensure consistent planning of systems.

3.2 Create Life cycle management plans for all new and upgraded systems based on the life cycle management plan template.

3.3 Establish strategic technology roadmaps, including infrastructure related initiatives to deliver infrastructure enhancements in an appropriate timeframe to support business objectives.

TAP4: Consolidate infrastructure services to take advantage of opportunities for maintaining or improving service delivery and reducing total cost of ownership.

Direction

4.1 Review all major infrastructure services to identify opportunities for consolidation of services.

4.2 Act upon consolidation opportunities that are identified and are cost effective without degrading performance levels.

4.3 Design new systems to take advantage of existing infrastructure services.

TAP5: Technology standards must be reviewed to identify opportunities to take advantage of new and emerging technologies.

Direction

5.1 Review Technology standards on a regular basis to identify opportunities to take advantage of new and emerging technologies.

5.2 Update Technology standards only after a careful evaluation is performed.

6. ICT Service Management Architecture Principles (SMAP)

SMAP1: Employ consistent direction to ICT services management to align processes across organizational boundaries.

Direction

1.1 Define Service management processes at the enterprise level.

1.2 Use Enterprise service management processes throughout the government ICT service organizations.

SMAP2: Government of Manitoba ICT service management practices will be based on the IT Infrastructure Library (ITIL).

Direction

2.1 Prioritize and develop Enterprise level service management processes based on ITIL.

2.2 ICT service organizations must align their existing service management processes with enterprise-level processes.

SMAP3: ICT service management processes will define the performance indicators used to measure and improve the effectiveness of the process.

Direction

3.1 Publish all ICT services and associated measurable performance indicators.

3.2 Consistently use Performance indicators across the enterprise to allow them to be summarized at the enterprise level.

3.3 Track and monitor Performance indicators to evaluate effectiveness as well as to provide a basis for negotiating service levels.

3.4 Government ICT organizations will publish the services they provide to their customers along with the performance indicators used to evaluate the service.

SMAP4: ICT service management processes will be implemented and sustainable.

Direction

4.1 Develop a comprehensive awareness and training program for the implementation of service management processes.

4.2 The executive level of government must fully support this awareness and training program and sustain it over the long-term.