

Government of Alberta's Enterprise Architecture Principles

INTRODUCTION

Enterprise Architecture principles are a set of overarching guidelines and rules that relate to Information Management Technology (IMT) architecture work across all areas of the Government of Alberta (GoA). The principles reflect a level of consensus among the various government organizations of the GoA enterprise, and form the basis for making IT decisions.

All principles have a definition, associated rationale and implication statements to support the understanding and acceptance of the principles, and to help with decision making. Enterprise Architecture principles are used to capture the fundamental truths about how the enterprise will use and deploy IMT assets. The principles are used in a number of different ways:

- To provide a framework within which the enterprise can start to make conscious decisions about enterprise architecture and projects that implement the target enterprise architecture
- As a guide to establishing relevant evaluation criteria, thus exerting strong influence on the selection of products, solutions, or solution architectures in the later stages of managing compliance to the enterprise architecture
- As drivers for defining the functional requirements of the architecture
- As an input to assessing both existing implementations and the strategic portfolio, for compliance with the defined architectures; these assessments will provide valuable insights into the transition activities needed to implement an architecture, in support of business goals and priorities
- The Rationale statements within an Architecture Principle highlight the business value of implementations consistent with the principle and provide guidance for difficult decisions with conflicting drivers or objectives
- The Implications statements within an Architecture Principle provide an outline of the key tasks, resources, and potential costs to the enterprise of following the principle; they also provide valuable inputs to future transition initiative and planning activities

Enterprise Architecture principles are inter-related, and need to be applied as a set. Principles will sometimes compete with each other, so a decision will be required as to which principle will take precedence on a particular issue. The rationale for such decisions must be documented.

Failure to follow these principles may cause operational problems and inhibit the ability of the Government of Alberta to fulfil its mission. As such, adherence to these principles should be followed at all times and the rationale for any exceptions must be documented.

For more information on how to apply these principles, please contact imtstandards@gov.ab.ca.

(Excerpted from TOGAF 9.1, section 23)

PRINCIPLES

1. Life Cycle Management	
Statement	Major IMT assets and services must be managed throughout their life cycle and an up to date Life Cycle Management Plan must be maintained.
Rationale	<ul style="list-style-type: none"> • IMT decisions must be made with the goal of reducing the overall total cost of ownership of the IMT asset as opposed to immediate acquisition/build costs. • Continuous improvement in processes and technology implementations will lead to reduced costs, improved efficiency and effectiveness and increased confidence in public bodies to provide services.
Implications	<ul style="list-style-type: none"> • May require the implementation of a Life Cycle Management Plan within the ministries or the enterprise. • As technologies change and business requirements evolve, the processes and technologies put in place to support them must also change, ensuring appropriate protection and efficiencies. Without continuous review and management of solutions they become unwieldy, interruptive and costly. • Must provide continuous improvement of tools and processes.

2. Standardization	
Statement	Standardization must be used in order to add value and consistency.
Rationale	<ul style="list-style-type: none"> • Ensuring standards are current minimizes any barriers to change. • Standardized assets across the enterprise bring the benefit of economies of scale to the government. • Standard processes are repeatable, predictable, scalable, and more efficient. • It is easier to focus attention, resources, knowledge, and investments in a standardized environment.
Implications	<ul style="list-style-type: none"> • All procurement and development processes involving IMT assets and services must maintain compliance with standards • Exceptions are possible using well defined processes. • Standards will be reviewed regularly and updated before they are obsolete or no longer provide value. • Standardization initiatives must have a clear governance model. • Development of enterprise-wide applications is preferred over the development of similar or duplicate applications which are only intended for a single organization.

3. Accessibility	
Statement	IMT services and processes must enable and encourage customer interaction, and strive for consistency regardless of access method.
Rationale	<ul style="list-style-type: none"> • Provide better, more intuitive, customer service through the use of consistent application interfaces and processes.
Implications	<ul style="list-style-type: none"> • Customer interaction becomes a primary consideration in the development of services and processes. • Access to services must be simplified and consistent processes must be developed, approved, and communicated. • Applications will require a consistent mechanism(s) to discover, search, access, and present information using a “common look and feel”. • Application interfaces must be sufficiently adaptable to meet a wide range of stakeholders (e.g. persons with disabilities) and their corresponding methods of access.

4. Privacy	
Statement	Privacy of all individuals or entities must be maintained and respected in the development, acquisition, and operation of all IMT systems.
Rationale	<ul style="list-style-type: none"> • The GoA is obligated to protect and respect the privacy of citizens they interact with. • Delivery of services to citizens and other entities in line with government strategies is imperative. • Services must be delivered while protecting both the citizen and the GoA by ensuring that statutory obligations are met, and civil or criminal penalties are avoided.
Implications	<ul style="list-style-type: none"> • All IMT systems must allow appropriate access to information for the intended audiences while not allowing data to become available in contravention to legal or contractual obligations. A balance between both these requirements must be maintained. • Government must meet both protection of privacy and access to information requirements established in legislation. • Education must be provided on the relevant laws, regulations, and policies.

5. Business Continuity	
Statement	The technology used by the business must be built to minimize service interruptions.
Rationale	<ul style="list-style-type: none"> • Business is dependent on technology to provide services, therefore reliability must be considered in their design and use. • In order to minimize the effects of any service interruptions, resolutions must be planned before they occur or at the time of system design, based on criticality and sensitivity of the asset.
Implications	<ul style="list-style-type: none"> • Business Assets must be assessed for criticality and impact on the business, in order to determine what level of continuity and protection is required. • Scalability, recoverability and redundancy should be addressed at the time of design in relation to the risk and impact assessment. • Business entities throughout the enterprise will be provided with the capability to continue functioning according to the assessed criticality and corresponding continuity plan. • Defined testing and remediation of continuity plans must be scheduled and conducted on a regular basis.

6. Business driven change	
Statement	Changes to technology are only made in response to business needs and values, or to avoid risk.
Rationale	<ul style="list-style-type: none"> • Technology changes in response to the needs of the business, rather than having the business change in response to technology. • Changes to technology are only implemented based on clear business needs or the need to avoid risk, such as with technology obsolescence. • Business clients include Alberta citizens, ministry units, agencies and Government officials.
Implications	<ul style="list-style-type: none"> • Funding for technology changes only happens when there is a documented business need. • Business and technology groups must be integrated and work closely together. • Technology groups must understand the business they support so they can ensure the changes made benefit the business. • All changes to technology are tracked through a change management system with a defined rationale for the change and well understood impacts to the business systems. • Innovation and research are required to ensure that business needs are proactively addressed.

7. Enterprise Reusability	
Statement	The delivery and use of enterprise-wide systems is preferred over business-unit specific systems.
Rationale	<ul style="list-style-type: none"> • Compared to duplicative systems needed across an enterprise, a single enterprise-wide solution will reduce development and operational costs and will leverage skills across the enterprise. • Business units will benefit from improved quality and reduced risk by using proven and tested enterprise-wide services.
Implications	<ul style="list-style-type: none"> • When assessing systems for business use, the preference will be: <ol style="list-style-type: none"> 1. Reuse 2. Buy 3. Build • A reliable repository of all enterprise systems must be managed and available so that all can understand what systems and capabilities exist already for reuse. • Infrastructure to support reuse must be in place. • Use of common enterprise-wide systems may prolong the use of legacy technology and limit innovations. • Allowances may be needed by the business units to allow the use of enterprise-wide systems. • Consistent application development and maintenance processes are defined and used.

8. Use of Open Standards	
Statement	IMT assets and services must favour using open standards where appropriate.
Rationale	<ul style="list-style-type: none"> • Maximize options for selection of technology products and services and prevent lock-in to a particular vendor, it helps ensure support from multiple vendors for their products, and facilitate supply chain integration. • Improve interoperability and enable integration across systems.
Implications	<ul style="list-style-type: none"> • Open standards may lack the maturity or completeness required for a given solution; therefore they have to be carefully evaluated before adoption. • Interoperability, open, and industry standards must be followed unless there is a compelling business reason to implement a non-standard solution. • Defined and approved standards must be selected, following the sequence of international, regional, national, and organizational standards. • Support for open standards is a necessary criterion in the acquisition of IMT solutions.

9. Application Interoperability	
Statement	IMT Applications must minimize client-side dependencies, by utilizing standards and web based delivery, where applicable.
Rationale	<ul style="list-style-type: none"> • Minimize reliance on client software, operating systems, or browser versions. • IMT applications will be easier to update, integrate, and evolve.
Implications	<ul style="list-style-type: none"> • IMT application development and procurement must include an assessment of support for open standards. • Concessions may be needed in user requirements. • New applications must be tested for compatibility in a variety of up-to-date environments to ensure no client-side dependencies are present. • An exemption process must be defined for cases where dependencies cannot be avoided.

10. Service Oriented Architecture	
Statement	IMT Applications must support tiered designs, favouring a Service Oriented approach.
Rationale	<ul style="list-style-type: none"> • Supports the addition of independent, cross-functional interfaces on any potential device, form-factor, or platform. • IMT applications are easier to update, integrate, and evolve.
Implications	<ul style="list-style-type: none"> • Application design must be reviewed at defined stages. • Legacy integration may require wrapping existing application functionality as web services to act as reusable SOA artifacts. • Service representation is defined by using business processes, rules, policies, service interfaces, and service components related to a specific common business function.

11. Data Management	
Statement	Data management practices are defined and implemented consistently throughout the Government of Alberta.
Rationale	<ul style="list-style-type: none"> • A common practice increases the ability for business units and their application systems to communicate and interoperate. • Data management ensures that we know where the right information is and can obtain it when and where we need it. • There is a cost and risk associated to poorly managed quality data.
Implications	<ul style="list-style-type: none"> • Must educate the enterprise stakeholders to understand the relationship between management of data, value of data, sharing of data, and accessibility to data. • All data assets must be identified and categorized as corporate, shared, or departmental. Management must be performed at the appropriate level. • There must be a mechanism to identify, document, and analyze data issues including data quality. • Data must be captured once and stored once, as an authoritative source. • Managed replication of data must be allowed when it is proven necessary for response time, availability, security, or ease-of-use. • Data must be encapsulated by application(s) or service(s) responsible for managing the data integrity. All updates to that information must be through the encapsulating application(s) or service(s). • Related metadata (e.g. workflow and audit information) must be stored with the relevant information in the appropriate repository via the appropriate system. • A common data management practice and its governance structure must be defined.

12. Data Sharing	
Statement	When sharing data, standardized data structures and security practices are defined and implemented.
Rationale	<ul style="list-style-type: none"> • Common data sharing practices reduce costs and risks when building and maintaining application integrations. • The protection of data is consistent between applications. • If integrity of data is questionable, all conclusions reached on retrieved data are in question.
Implications	<ul style="list-style-type: none"> • Data is passed across the enterprise in a consistent format, which may require transformation from participating systems. • Data classifications need to be considered before sharing data. • Common core data model standards must be developed and implemented. • Controlled vocabulary standards must be developed and implemented. • An enterprise metadata standard must be developed to communicate and facilitate reuse in all types of applications, and to improve the management of information quality. • Quality control measures must be implemented to ensure the integrity of the data.

13. Data Accessibility	
Statement	Data is readily available for its intended audience.
Rationale	<ul style="list-style-type: none"> • Enterprise access to data leads to efficiency and effectiveness in decision-making and affords timely response to information requests and service delivery. • Staff time is saved and consistency of information is improved.
Implications	<ul style="list-style-type: none"> • Data must be considered from an enterprise perspective to allow access by a wide variety of users. • Discoverability and access to appropriate data must be simplified and consistent processes must be developed, approved, and communicated. • Discoverability and access to appropriate data must meet sharing and exchange of data requirements, such as customer service, reporting, analytics, and forecasting (business intelligence) requirements. • Access privileges to data and systems must be granted at appropriate levels.