



Government of Ontario IT Standard (GO-ITS)

Number 56

OPS Enterprise Architecture:
Principles and Artefacts

Appendix A - OPS Enterprise Architecture Principles

Version 1.5

Status: Final

Prepared for the Information Technology Standards Council (ITSC) under the
delegated authority of the Management Board of Cabinet

CONTENTS

| | |
|---|-----------|
| INTRODUCTION | 3 |
| 1. ENTERPRISE ARCHITECTURE PRINCIPLES | 5 |
| 2. BUSINESS ARCHITECTURE PRINCIPLES | 8 |
| 3. INFORMATION ARCHITECTURE PRINCIPLES | 10 |
| 4. APPLICATION ARCHITECTURE PRINCIPLES | 13 |
| 5. TECHNOLOGY ARCHITECTURE PRINCIPLES | 20 |
| 6. SECURITY ARCHITECTURE PRINCIPLES | 28 |
| 7. PRIVACY DESIGN PRINCIPLES FOR PERSONAL INFORMATION..... | 40 |
| <i>LEGISLATIVE REQUIREMENTS</i> | <i>42</i> |
| 8. COPYRIGHT INFORMATION..... | 50 |

OPS EA Principles

Introduction

1. Enterprise Architecture Principles

The overarching vision for the EA is that it will be iterative and evolving, and will guide the development of an integrated information environment that will enable cost effective solutions to meet new business requirements. The global Enterprise Architecture Principles are corollary to those stated in the *Information & Information Technology Directive* and lay the fundamentals for the development and evolution of domain-specific principles. The intent of these basic generalizations is to ensure that the practice of architecture is holistic and continues to fulfill its intended purpose.

2. Business Architecture Principles

The Business Architecture principles are domain-specific principles built upon the foundation provided by the global Enterprise Architecture principles. The intent of these basic generalizations is to guide the use and evolution of the OPS Business Architecture methodology.

3. Information Architecture Principles

In general, the Information Architecture principles have been developed based on the premise that principles are formally defined statements of beliefs that enable decisions, clearly lead to a single course of action and are enduring.

In the OPS, *Information Architectures* are formal representations of business information describing information holdings, their structures, relationships and information infrastructure within the enterprise.

Information Architectures document the organization's business and technology environment, and can include, but are not limited to, business services and processes, business locations, computer applications, databases, data marts, data warehouses, communications networks, access channels, data components and data services.

4. Application Architecture Principles The Government of Ontario's application architecture principles provide the foundation for enterprise application development initiatives.

5. Technology Architecture Principles Technology Architecture principles are described in this subsection grouped under the following major headings:

- Technology Principles; and
- Infrastructure Service Principles

6. Security Architecture Principles This section presents security architecture principles grouped under the following categories:

- Administration;
- Availability;
- Accountability;
- Authorization;
- Assurance; and
- Awareness and Training

7. Privacy Design Principles Privacy design principles support the informed consent and the control a person has on his or her personally identifiable information. Ten design principles are listed.

1. Enterprise Architecture Principles

The overarching vision for the EA is that it will be iterative and evolving, and will guide the development of an integrated environment that will enable cost-effective solutions to meet new business requirements. The global Enterprise Architecture Principles are corollary to those stated in the *Information & Information Technology Directive* and lay the fundamentals for the development and evolution of domain-specific principles. The intent of these basic generalizations is to ensure that the practice of architecture is holistic and continues to fulfill its intended purpose.

EAP #1: Mission-driven

The Ontario enterprise architecture practice is mission-driven and aimed at promoting progress towards the goals of the Ontario Government.

Rationale:

A business-led architecture is more successful in meeting strategic goals, responding to changing mission needs, and meeting citizens' expectations.

Implications:

- Ensure architectural descriptions demonstrate how the business serves the current government's priorities and the needs of citizens;
- To the extent possible, design artifact type definitions to facilitate integration with descriptive representations of other jurisdictions, thereby allowing Ontario to collaborate with other governments; and
- Follow the precept that architecture practice is not an end unto itself.

EAP #2: Simplification

The Ontario Enterprise Architecture facilitates simplified government operations.

Rationale:

An Enterprise Architecture that is explicit and pragmatic enables transformation of programs and services and minimizes enterprise redundancy.

Implications:

- Optimize lines of business and business solutions to benefit the enterprise as a whole;
- Maintain an EA practice designed to reduce complexity and enable integration to the maximum extent possible; and
- Make best practices available to ensure architectural representations from all five architecture domains provide a minimal set of information sufficient to describe fully problems, opportunities and solutions.

EAP #3: Reuse

Reuse of enterprise business and IT components reduces cost and complexity.

Rationale:

Reuse minimizes development, maintenance and support costs through the deployment of common well-understood components.

Implications:

- Define architecture practices in each domain to produce and promote practical mechanisms for reuse;
- Ensure reuse is one of the criteria of quality assurance review;
- Encourage and reward reuse throughout the enterprise; and
- Processes, applications and components are designed to meet reuse objectives

EAP #4: Explicitness

Explicit architecture facilitates creating and changing an enterprise and its business solutions.

Rationale:

Formally developed and documented enterprise architectures form a baseline and provide an effective foundation for managing change.

Implications:

- Define architecture practices in each domain to produce and promote pragmatic and useful artefact-type definitions;
- Communicate best practices for artefact creation; and
- Grow and maintain an accessible collection of descriptive representations to provide an evolving picture of the enterprise. These representations are for the most part artefacts contributed by projects that reflect the state of some part of the organization at the project's conclusion.

EAP #5: Holistic

Enterprise architecture is the comprehensive view that results from the combined perspectives of five architectural disciplines: business; information; application; technology; and security.

Rationale:

To provide business value over time enterprise architecture contains interrelated information covering all aspects of the enterprise at all levels of abstraction.

Implications:

- Establish and mature the architecture practise in the five architecture disciplines;
- Ensure artifact type definitions include the means by which transformation and alignment are provable;
- Ensure enterprise architecture review requirements include a set of artefacts from each domain sufficient to contribute meaningfully to an enterprise view; and
- Include transformation and alignment as criteria for architecture review.

2. Business Architecture Principles

The Business Architecture principles are domain-specific principles built upon the foundation provided by the global Enterprise Architecture principles. The intent of these basic generalizations is to guide the use and the evolution of the OPS Business Architecture methodology.

BAP# 1: BUSINESS PLANNING

Business Architecture supports strategic and operational planning.

Rationale:

Business architecture practice includes the discipline and tools required to enable business strategic and operational planning.

Implications:

- Ensure business goals are aligned with enterprise priorities;
- Position the business in the context of the broader enterprise;
- Develop business model to meet operational objectives and strategic goals; and
- Analyze business risk and develop strategies for risk management

BAP #2: COMMON VOCABULARY

Business Architecture facilitates the development of a common business vocabulary.

Rationale:

A common business vocabulary enhances communication and understanding of the business.

Implications:

- Engage and consult with business stakeholders to ensure mutually agreeable business vocabulary; and
- Ensure the business vocabulary is explicit.

BAP #3: SIMPLE AND FLEXIBLE

Business Architecture enables simple and flexible business process design.

Rationale:

Opportunities for increasing efficiency, effectiveness, and quality can be identified and realized through simple and flexible business processes.

Implications:

- Analyze business processes to simplify, integrate, eliminate redundancy, and increase efficiency;
- Identify common business processes for reuse; and
- Design business processes to enable business agility.

BAP#4: TECHNOLOGY AGNOSTIC

Business architecture is not constrained by technology.

Rationale:

Business architecture describes the business model independently of supporting technology and provides the foundation for analysis of opportunities for automation.

Implications:

- Eliminate technology constraints when defining business architecture; and
- Ensure automated processes are described at the business process level for analysis and design.

BAP #5: CLIENT CENTRIC

Business Architecture uses a client centric approach.

Rationale:

Business models are designed to meet the requirements of Government business areas. These business areas exist to meet the needs of target groups.

Implications:

- Ensure that the target group is well defined and understood; and
- Define strategic goals, business objectives, and performance measures in terms of the outcomes for the target group.

3. Information Architecture Principles

Introduction

In general, the Information Architecture principles have been developed based on the premise that principles are formally defined statements of beliefs that enable decisions, clearly lead to a single course of action and are enduring.

In the OPS, *Information Architectures* are formal representations of business information describing information holdings, their structures, relationships and information infrastructure within the enterprise.

Information Architectures document the organization's business and technology environment, and can include, but are not limited to, business services and processes, business locations, computer applications, databases, data marts, data warehouses, communications networks, access channels, data components and data services.

Information Architecture Principles

1. **FORMALLY DEFINED:** Information Architectures Describe Information Linkages
2. **ALIGNMENT WITH BUSINESS NEEDS:** Information Architectures Ensure Alignment
3. **CLEAR AND CONSISTENT:** Information Architectures Facilitate Data Quality
4. **INTEGRITY, ACCESSIBILITY AND AVAILABILITY:** Information Architectures Enable Integrity, Accessibility and Availability

More specifically:

IAP #1: FORMALLY DEFINED

Information Architectures fully describe information structures and connect business information via information flows.

Rationale:

- Well-defined information and data designs contribute to strategic decision-making processes and service delivery.

Implications:

- Ensure the business information and data needs are clearly communicated;

- Document the business information flows and linkages to enable a clear understanding by the data owners/custodians; and
- Establish formal data administration processes.

IAP #2: ALIGNMENT WITH BUSINESS NEEDS

Information architectures ensure information requirements are aligned and integrated to meet business needs.

Rationale:

- Well specified designs maximize alignment and integration of information holdings with business processes.

Implications:

- Organize and document information holdings using information architecture processes, methods and standards;
- Engage and consult with business program areas to define information requirements; and
- Model, design, and develop information holdings using a top-down, enterprise-wide architecture approach.

IAP #3: CLEAR AND CONSISTENT

Information Architectures facilitate data quality through clear and consistent definitions.

Rationale:

- A well-defined Information vocabulary enhances communications through clear and consistent definitions.

Implications:

- Establish a well-defined and common vocabulary to adhere to when defining information holdings;
- Establish business information standards to improve data quality, integrity and reliability;
- Develop clear information and data definitions to enable data sharing, integration, exchange and reuse across the enterprise; and
- Reconcile and align with corporate information and data definitions.

IAP #4: INTEGRITY, ACCESSIBILITY AND AVAILABILITY

Information architectures provide an underlying framework to enable information integrity, accessibility and availability.

Rationale:

- Information needs to be concise and accurate (integrity), accessible, and available, as required by the business.

Implications:

- Defines processes that provide for integrity, accessibility and availability of the information and data;
- Ensure information owners and custodians are aware of the sensitivity of their information holdings they own/manage; and
- Adhere to information architecture modeling standards, best practices, and guidelines.

4. Application Architecture Principles

Introduction

The Government of Ontario's application architecture principles provide the foundation for enterprise application development initiatives. It defines how applications should be designed to gain maximum interoperability.

Benefits of well-documented application architecture principles:

- ☐ Ease of integration of applications and application services.
- ☐ Efficient reuse of existing application assets.
- ☐ Faster deployment of new applications.
- ☐ Better responsiveness to changing business needs.

The application principles (APs) listed below provide guidelines for the design or purchase of applications and application components across the Government of Ontario.

AP #1: TRACEABILITY

The Application Architecture must enable business processes.

Rationale:

- Aligns to business;
- Build for change;
- Facilitates transformation of business architecture;
- Enhances traceability to business requirements;
- Maximize the effectiveness of the development project; and
- Minimizes requirement mismatch

Implications:

- Need to ensure conformance to Enterprise Architecture practice in the creation of artifacts;
- Need to follow a Systems Development Life Cycle methodology or applicable standard; and
- Need to document stakeholder requirements well

AP #2: FLEXIBILITY

Application Architecture must be highly modular, multi-tiered, flexible, and loosely coupled.

Rationale:

- Optimizes for agility;
- Minimizes integration complexity;
- Simplifies implementation, deployment and maintenance;
- Enhances scalability, upgradeability, supportability;
- Enables service and component reusability;
- Ensures services are componentized;
- Facilitates and improves maintainability;
- Enables technology platform changes with minimum effect on business processes; and
- Enables Component-Based Architecture (CBA) & Services-Oriented Architecture (SOA)

Implications:

- Need to implement n-tier architecture pattern;
- Need to utilize application design patterns;
- Need to establish a common approach to integration;
- Must consider component- or services-based architectures; and
- An enterprise Services-Oriented Architecture strategy may need to be in place

AP #3: INTEGRABILITY

Application Architecture must reduce integration complexity and foster application simplicity.

Rationale:

- Reduces costs;
- Streamlines business processes;
- Facilitates reuse;
- Improves integration;
- Minimizes application impacts (e.g., potential delays in project completion);
- Decreases application maintenance and support;
- Minimizes duplication and multiple systems; and
- Increases application flexibility

Implications:

- Need to follow standards (industry, open-standard, technology, security, etc.);
- Need to plan for integration;
- Need to develop loosely-coupled interfaces; and
- Need to publish integration points

AP #4: MODULARITY

The Application Architecture must follow a service-based approach.

Rationale:

- *Hides the complexity of heterogeneous IT environments from business user;*

- *Allows internal and external business processes to be combined and recombined to support flexibility in business process execution;*
- Enhances business agility;
- Provides an IT architecture that is more flexible, agile, and cost effective;
- *Helps to ensure better interoperability;*
- Supports services transformation;
- Improves Service Offering;
- Potential for cost reductions through IT asset re-use;
- Creates opportunities for new business/services integration;
- Better software and faster build (composite applications); and
- Promotes collaboration

Implications:

- *Use standards-based approach; and*
- *Security and privacy awareness heightened*

AP #5: BUY VERSUS BUILD

The Application Architecture must support the concept of reuse before buy and buy before build.

Rationale:

- Reduces costs;
- Aligns to business requirements; and
- Minimizes application development, maintenance and support costs and related resource implications

Implications:

- Need to conduct a fit/gap and cost-benefit analysis;
- Need to comply with I&IT directives and operating policies;
- Need to be market-aware;
- Need to plan for integration; and
- Need to follow the acquired solution guidelines for conformance to EA practice

AP #6: CONSOLIDATION

The Application Architecture must promote consolidation first and integration second.

Rationale:

- Reduces cost;
- Reduces integration complexity;
- Facilitates consolidation of similar functions;
- Streamlines similar application into single systems;
- Minimizes duplication of solutions;
- Increases reuse across the enterprise; and

- Simplifies application maintenance and support

Implications:

- Need to conduct a fit/gap and cost-benefit analysis;
- Need to comply with I&IT directive;
- Need to plan for consolidation; and
- Need to follow the acquired solution guidelines for conformance to EA practice

AP #7: INTEROPERABILITY**Application Architecture must enable interoperability.****Rationale:**

- Supports inter-jurisdictional initiatives;
- Helps to view the OPS as a single enterprise;
- Facilitates consolidation of similar functions;
- Facilitates data sharing between internal and external partners;
- Supports streamlining processes; and
- Reduces cost

Implications:

- Need for enforced security standards;
- Require open or industry standards; and
- Need to use standardized interface

AP #8: REUSABILITY**The Application Architecture must assist with designing applications for reuse.****Rationale:**

- Reduces cost;
- Fosters enterprise reuse;
- Encourages future reusability of its common components/services and applications;
- Promotes application assembly and component integration;
- Increases number of application/common components/services available for use by other new applications; and
- Ensures consistency in the development of components/services

Implications:

- Need to reuse existing application components or services where feasible;
- Need to employ Component Based Architecture or Services-Oriented Architecture (SOA) as preferred architecture best practices; and

- An enterprise Services-Oriented Architecture strategy may need to be in place

AP #9: SHAREABILITY

The Application Architecture must take a portfolio approach to analyzing, planning, designing, governing, and optimizing enterprise applications.

Rationale:

- *Optimizes application investment;*
- *Improves reusability;*
- *Improves application planning; and*
- *Enhances IT asset management*

Implications:

- *Reduces of the number of applications;*
- *Focuses on application gaps; and*
- *Enables an enterprise-wide application planning and prioritization approach*

AP #10: UPGRADABILITY

The Application Architecture must anticipate and plan the replacement and transition of legacy applications.

Rationale:

- Minimizes likelihood and risk of developing and deploying applications that are functionally deficient
- Reduces likelihood of implementing solutions which are high-cost/high-maintenance
- Assists with planning for the replacement of applications - reduces 'crisis' replacement and maintenance efforts
- Facilitates a responsive enterprise I&IT posture that can respond to to changing requirements over time

Implications:

- Need to establish a legacy renewal strategy
- Both business and IT must work together in the search for the best possible replacement
- Need to develop priorities for the replacement of obsolete, legacy and redundant systems

AP#11: COMPLIANCE

Application solutions must be developed using standard, common methodologies.

Rationale:

- Standardizes development methodologies;
- Increases likelihood of high quality deliverables; and
- Reduces cost through common methodologies and tools

Implications:

- Systems Development Life Cycle standards must be adopted to maximize the effectiveness of the development process; and
- Training will be required to support standard methodologies

AP #12: SUPPORTABILITY

The Application Architecture and applications must be documented comprehensively.

Rationale:

- Aligns to business;
- Facilitates transformation of business architecture;
- Enhances traceability to business requirements;
- Maximizes the effectiveness of the development project;
- Minimizes requirement mismatch potential; and
- Supports future maintenance of the system

Implications:

- Need to ensure adherence to EA practice in the creation of artifacts;
- Need to ensure the application design reflects the application architecture principles, practices, and standards;
- Need to ensure the requirements traceability by cross-referencing the system requirements with design elements; and
- Need to follow a development methodology and/or applicable standard

AP #13: SECURITY

Applications must meet the Security Architecture requirements.

Rationale:

- Aligns to security policy, standards & procedures;
- Facilitates transformation of security requirements;
- Enhances traceability to security requirements;
- Maximize the effectiveness of secure applications; and
- Minimizes security exposures

Implications:

- Need to ensure conformance to EA practice in the creation of application security artifacts;

- Need to ensure the application design reflects the security architecture principles, practices, and standards;
- Need to ensure the requirements traceability by cross-referencing the security requirements with design; and
- Need to follow a secure application development best practices

5. Technology Architecture Principles

Overview

The principles are the foundation of the technology architecture that provides an effective framework within which the OPS Information & Information Technology (I&IT) organization can make decisions about their business, service offerings, its management style and structure as it relates to the use and implementation of technology.

These principles provide guidance for understanding how technology, services, patterns, blueprints, components, delivery levels, responsibilities, etc. are required to develop, deliver, and manage technology. They also help determine the impact of potential changes to the technology architecture

Any changes to these principles may require changes to other documents, such as standards, other domain architecture documents, technical reference models, and agreements between service providers and service consumers. Similarly, other architecture domain stakeholders should also refer to these principles whenever any change to their own domain architecture is being considered.

Description of Technology Architecture Principles

Technology Architecture Principles, Rationale, and Implications

The principles are statements of intent or purpose related to the use of technology which enables I&IT systems to be of benefit to the OPS business. The principles describe preferred practices to be followed when implementing new or upgraded technology, services, patterns, blueprints and components.

Each principle is supported by statements that explain the rationale and benefits for following it as well as any implications, i.e. requirements, both for the business and I&IT, necessary to implement the principle in terms of resources, costs, and activities/tasks.

Categories of Technology Architecture Principles

The following groupings have been used:

- Technology Principles
- Infrastructure Service Principles

Technology Principles

TP #1: Ownership

As identified by the Architecture Governance framework, all models, patterns, blueprints, components, services, and technologies shall have owners. They shall be responsible for their planning, management, administration and support.

Rationale:

- Ensure accountability/alignment for all I&IT services, patterns, blueprints, components and technologies

Implications:

- Define new ownership roles and responsibilities as required (who)
- Must identify services, patterns, blueprints, components, and technologies (what)

TP #2: Enterprise Technology Integration Model

There shall be an Enterprise Technology Integration Model that defines basic technology architecture concepts such as patterns, blueprints, components, services, quality levels, infrastructure catalogues and portfolios, etc., as well as the interrelationships between them.

Rationale:

- Establishes common concepts, vocabulary
- Reduces miscommunication between I&IT stakeholders
- Reduces model building/design effort

Implications:

- Model must be maintained, and communicated

TP #3: Quality Level Metric (QLM) Approach

Technology implementations require QLM negotiations and tradeoff discussions to occur as early as possible in the design process between business stakeholders and systems stakeholders including application architects, technology architects, service providers and operations and maintenance staff.

Quality level metrics considered must be comprehensive and include the following categories and aspects:

CONVENTIONAL

- Scalability (throughput and response time)
- Availability
- Recoverability (transaction recoverability/rollback)

EXTENDED

- Security

- Integrity
- Integrability
- Usability
- Sourceability
- Interoperability
- Supportability
- Affordability

ADAPTIVENESS / MODIFIABILITY

- Reusability
- Upgradeability
- Incremental “capacity on demand” for any quality level
- Changing presentation logic
- Changing business logic
- Integrating new sources/consumers into the application

Rationale:

- Facilitates non-functional requirements gathering
- Avoids narrow discussions of requirements - business stakeholders will have a clearer idea of the system they are asking for / getting
- Better acceptance from the business on the system that is ultimately delivered – fewer surprises for both the business and I&IT
- Better fit of applications into the infrastructure
- Better security and protection of privacy

Implications:

- Need to ensure that processes, such as product selections, vendor of record, planning, requirements gathering, has the quality level metrics as part of the requirements
- Need to document, publish and enforce the requirement for quality level metrics when developing solutions, services and infrastructure

TP #4: Infrastructure Maintenance

Infrastructure maintenance, other than critical repairs, will be subject to SDLC rigour similar to that for a new application/technology deployment initiative.

Rationale:

- Reduce maintenance costs
- Redirect resources to strategic maintenance initiatives
- Reduce the risk of unsupported infrastructure that may result to significant unplanned downtime

Implications:

- Need to define maintenance release strategy
- Need to communicate release strategy to OPS business community
- Requires a process to effect management cultural change
- Need to re-evaluate maintenance as a training vehicle

TP #5: Rationalization of Products and Platforms

The variety of I&IT products and platforms shall be rationalized. Technological diversity shall be controlled and minimized.

Rationale:

- Reduce cost of information technology
- Increase interoperability between products and platforms by eliminating islands of technology
- Leverage I&IT skills and resources
- Reduce maintenance complexity and costs
- Leverage vendor partnerships

Implications:

- Need to establish and communicate technology standards
- Need to move I&IT decisions towards standards-based decisions
- Requires migration path from current I&IT environment to a reduced set of technologies
- May require application and technology changes
- Requires a process to effect culture change in both I&IT and business clients
- Policies, standards and procedures that govern acquisition of technology must be tied directly to this principle

TP #6: Product Selection

Products shall be selected with regard to optimizing quality level metrics such as availability, technology standards, uniformity, the ability to integrate with existing systems, cost and comply with OPS security and privacy requirements must be considered.

Rationale:

- Increase capability for data, application and infrastructure service sharing
- Reduce complexity, cost and risk of technology environment
- Reduce integration and system management costs
- Ensure effective use of skills, vendor relationships and reuse of design and development assets
- Protect critical assets and increase the level of trust in service delivery

Implications:

- Technology evaluation and selection process needs to reflect integration criteria
- May constrain the selection of technology

TP #7: Portfolio of Products

A portfolio approach should be adopted for planning and management of I&IT of vendor supported I&IT products, including software, hardware, and infrastructure

Rationale:

- Improved planning, management, risk assessment and flexibility to meet changing business needs
- Leverage both I&IT and vendor skills

- Reduce maintenance complexity and costs
- Reduce overall risk to the business

Implications:

- Need to define and implement a lifecycle management process for I&IT products
- Business cases must include the cost of maintaining products and vendor-supported releases as well as any migration costs

TP #8: Infrastructure

The design, implementation and delivery of infrastructure shall adhere to the OPS technology architecture principles. The order of preference for infrastructure and infrastructure components will be to reuse, buy and then build.

Rationale:

- Reduce maintenance complexity and cost of the infrastructure
- Protect existing I&IT investments as needed
- Increase the quality of I&IT solutions
- Increase efficiency and utilization of I&IT resources
- Optimize quality level metrics

Implications:

- Need to define and implement lifecycle management process for I&IT products
- May limit the choices of I&IT solutions

TP #9: Security/Privacy Design, Robustness and Resiliency

Security and Privacy must be designed into systems as an integral part of the technology design process. Systems shall be designed with robustness and resilience and so disaster recovery measures shall be put in place for all critical systems and services that have been identified through a business impact analysis and business continuity planning.

Rationale:

- Avoid unexpected costs and delays by treating it as and “add on” after other design work has been completed.
- Avoid unintentional breach of OPS Security/Privacy policies
- Maintenance of public confidence in the OPS
- Protection against theft, loss, damage, or unauthorized modification, destruction or disclosure of I&IT assets
- To ensure critical program area services and systems are available through a recovery plan or a contingency plan

Implications:

- Security/Privacy requirements must be determined with all stakeholders as part of the QLM negotiation process
- Must support business driven security requirements based on legislation, policies, and business needs
- A consistent, trusted and effective security model must be developed for use across all applications, data, systems, and infrastructure

- Effective security & privacy administration processes and tools for assurance and accountability shall be required
- Threat and Risk Assessment (TRA) & Privacy Impact Assessment (PIA) processes shall be used to identify threats and risks and select cost effective controls which meet control objectives
- A Vulnerability Assessment (VA) process shall be used to identifying and quantifying vulnerabilities in a system.
- Program managers need to have business impact analysis and business continuity planning process developed and implemented
- Program managers need to be part of the process to conduct the business impact analysis and selection of contingency and business continuity plans
- Business impact analysis should be coordinated with value/risk analysis to identify potential countermeasures to exposures to the Ministry during the design of new business processes.
- I&IT shall facilitate the necessary Disaster Recovery Plans to support the Business Continuity plans

Infrastructure Service Principles

ISP #1: Service Development Life Cycle Framework

All I&IT infrastructure services shall be defined and managed in accordance with a formal service development life cycle framework and process.

Rationale:

- Business and I&IT organizations need a framework within which service development can be structured and managed to ensure on-time, on-budget delivery of effective services
- Effective allocation of work, roles and responsibilities
- Manage technology and service development risk through well-understood decision-making and risk review process
- Orderly transition from business requirement through architecture to service development and deployment

Implications:

- A service development life cycle framework must be in place to provide guidance, best practices on required deliverables, roles and responsibilities
- Service development should not continue beyond the service launch unless there is a formal agreement with management and business based on the life cycle model

ISP #2: Decomposition and Componentization of Services

All I&IT infrastructure services, whether purchased or developed internally, shall be architected using the Service Decomposition Framework that identifies the IT component set, and IT components used to build the IT service offering.

Rationale:

- Provides a logical structure for the definition of OPS I&IT infrastructure services with both internal and external service value chain is represented in a consistent manner
- Ensures I&IT infrastructure services can be built by integrating, brokering, creating service elements rapidly and ensures that service interdependencies are captured and risk/impact assessment capabilities are achieved
- Enable service elements and component reuse
- Ensures consistency in the development of service elements and selection/acquisition of service components
- Ensures services are componentized that drives utility computing model in delivery, offering, pricing and consumption on a “per-unit” basis

Implications:

- An enterprise Service Decomposition Framework must be in place
- An enterprise service planning process needs to be in place to take full advantage of this framework
- Common vocabulary needs to be consistent throughout the enterprise and definitions are understandable and available to users

ISP #3: Portfolio of Infrastructure Services

A portfolio approach should be adopted for planning and management of I&IT infrastructure services.

Rationale:

- Improved planning, management, risk assessment and flexibility to meet changing business needs
- Reduce overall risk to the business

Implications:

- Need to incorporate portfolio approach within and ITSM framework
- Business cases must include the cost of maintaining services

ISP #4: Infrastructure Service Quality Level Metric (QLM) Approach

Solutions, services, and infrastructure must be designed to optimize the quality level metrics. Quality level metrics considered must be meaningful, measurable and when required, enforced by and SLA. It must be comprehensive and include the following categories and aspects:

- Facilitating cost effective capacity changes (scalability/affordability)
- Ability to work with common service management disciplines (integrability/supportability)
- Orientation towards centralized monitoring/management of services and service components (supportability/affordability)
- Provide proper security controls to comply with OPS Security and Privacy Policies.

Rationale:

- Facilitates interoperability of services, systems and applications to smaller or larger platforms without extensive retooling

- Increase reusability of hardware or software
- Increase quality and effectiveness of I&IT solutions

Implications:

- Need to ensure that processes, such as product selections, vendor of record, planning, requirements gathering, has the quality level metrics as part of the requirements
- Need to document, publish and enforce the requirement for quality level metrics when developing solutions, services and infrastructure
- Need to ensure service management process, resources, tools, governance are in place
- Must consider service management as part of technology evaluation criteria & estimates (may limit choice of IT solutions).
- May require changes to existing technologies
- Architecture and design must integrate with ITIL processes
- End client perspective and SLA negotiation required

6. Security Architecture Principles

Introduction

These Security Architecture Principles present the fundamentals for cost-effective security to safeguard the organization's assets and resources and provide the foundation for ongoing risk mitigation. The principles are based on accepted industry security architecture, information assurance and security model design principles.

Categorizing the Security Architecture principles

The six principles underpinning the OPS security architecture model are:

1. Administration;
2. Availability;
3. Assurance;
4. Accountability;
5. Authorization; and
6. Awareness and Training

Each principle is described through one or more sub-principles. Each principle and sub-principle is elaborated upon using the following structure:

- **Number, Name and Description** – one or two words that encapsulate the intent of the principal or sub-principle, followed by a brief textual description;
- **Rationale** – a benefit statement;
- **Implications** – a brief textual description of the actions required for compliance

Administration

Principle 1 – Administration – *Protection of I&IT Assets*

OPS I&IT assets and resources will be protected from loss, destruction or unauthorized use or disclosure in accordance with its value, sensitivity and applicable legal requirements.

Rationale:

The appropriate implementation of I&IT security measures will be cost-effective and risk-appropriate investments.

Implications:

OPS ministries, I&IT Clusters and service providers must effectively assess management and mitigate risks by defining, communicating, developing, improving and implementing:

- I&IT security measures that adhere to OPS-wide requirements (i.e., standards, directives, operating policies and procedures, and guidelines).
- Information Security and Privacy Classification measures consistent with OPS policies and corporate requirements;
- Adequate security policies, standards and guidelines in a manner consistent with OPS-wide requirements;
- Security plans at the organizational level that are based on business-driven requirements; and
- Adequate security processes, procedures, and organizational governance structures that are commensurate with the value, risk, vulnerability and sensitivity of the assets being protected

Principle 2 – Administration – *Responsive and Cost-Effective*

The design and implementation of OPS security infrastructure (e.g., identification, authentication and authorization services and mechanisms) will be as secure, pluralistic, simple, efficient, cost-effective, reusable and transparent to the end-user as possible.

Rationale:

The impact of security mechanisms and services on business productivity is minimized, encouraging compliance with the security policies and practices of the OPS by way of a well-considered security model at the ministry, program and I&IT Cluster level.

Implications:

- Include zones of control and trust considerations in solution design when dealing with access control;
- Implement solutions in a manner that is consistent with the security tenet of limiting access based on end-user role (e.g., OPS staff members, System

Administrators, third party partners, commercial users and private/individual consumers of OPS-offered services).

- Develop and implement security mechanisms and I&IT infrastructure that are neither intrusive nor invasive.
- Develop and implement security mechanisms and I&IT infrastructure that conform with OPS policies and standards regarding identity management, authentication and authorization (IAA), including:
 - Single system sign-on solutions;
 - Multi-factor authentication schemes; and
 - Authentication and authorization solutions based on smart-card and biometric approaches.

Principle 3 – Administration – *Auditable Compliance*

The security of I&IT systems must be auditable, as required for compliance with statutory, contractual, and policy requirements as well as *de facto* standards of care that may apply across jurisdictional boundaries.

Rationale:

Audit schedules for I&IT systems are consistent with the security models and plans for technology solutions. Audit activities of I&IT systems assess compliance with OPS standards, legal, statutory, contractual and technical standards for security.

Implications:

- Ensure ongoing security compliance and control;
- Ensure security-appropriate standards of care are met regarding safeguarding of I&IT assets (e.g., inter-jurisdictional data sharing, multi-jurisdiction access to OPS I&IT resources and infrastructure);
- Ensure 3rd party and non-OPS service providers comply with OPS I&IT security policies, standards and requirements; and
- OPS I&IT Security models, plans, programs and governance groups must define, improve and communicate:
 1. Security policies, standards and guidelines related to;
 - Security research findings valuable to the enterprise;
 - Policy management guidance and tools relating to I&IT security (including PKI policy management);
 - Training programs and materials and resources related to information security and privacy classification, security trust models; and
 - Best practice guidance for developing security trust management models including criteria for determining appropriate trust levels;
 2. Security processes including:
 - Security communications and marketing;
 - Security awareness and training;
 - Resources and training materials relating to security awareness;

- Best practices for risk assessment and mitigation; and
 - Best practices for assuring compliance with OPS I&IT security framework requirements and requisite security control structures
3. Security structure-related information including:
 - People, processes and technology requirements; and
 - Criteria for application and infrastructure alignment
 4. Auditing, monitoring and logging requirements including:
 - Risk assessment development approaches; and
 - Inclusion of security-related components in systems development life cycle
 5. Legal ramifications for non-compliance including the need to establish security and privacy service level agreements with Service Providers.

Principle 4 – Administration – *Commensurate Controls*

All I&IT systems will be designed, built and implemented to incorporate the level of assurance, security, privacy controls, auditability and control functions necessary and appropriate to the sensitivity and value of information assets and/or resources that they consume, control, utilize or manage.

Rationale:

Target architectures, including those for technology refreshes or upgrades to legacy applications, will be in compliance with security requirements.

Implications:

The OPS organization must define and communicate:

1. Security policies, standards and guidelines related to;
 - Information and data sensitivity and classification requirements for the organization;
 - Criteria for determining appropriate level of assurance (Confidentiality, Integrity, Availability) required to access information assets and IT resources;
 - Identity requirements for I&IT solutions, assets, resources and applications;
 - Authentication requirements for I&IT solutions, assets, resources and applications;
 - Access control mechanisms; and
 - Audit trail requirements for both internal and external locations.
2. Security processes related to:
 - Communications;
 - Compliance;

- Security testing and evaluation (ST&E);
- Governance (review, endorsement and approval); and
- Audit (exceptions and appeals).

Principle 5 – Administration – *Conform to Policies & Standards*

An I&IT enterprise architecture will include a security architecture. The security architecture will conform to I&IT security policies, standards and guidelines as well as any related processes.

Rationale:

Security practices and standards developed at the I&IT Cluster, Ministry of business unit level must be aligned with and conform to corporate I&IT requirements for I&IT Cluster practice.

Implications:

- Ensure compliance with security policies, standards and guidelines;
- Ensure ongoing compliance of OPS I&IT systems and solutions with requirements specified in corporate enterprise architecture and I&IT systems/technology specifications and standards;
- Demonstrate the support and commitment of senior management through the security communication process for OPS policies, standards and guidelines.
- Communicate OPS security policies, standards and guidelines throughout the entire organization as required.
- Define and publish:
 1. Security directives and policies
 2. Security standards and guidelines including:
 - Information Security and Privacy Classification requirements;
 - Criteria for determining appropriate level of assurance;
 - Security processes;
 - Communications plans, resources, strategies, etc.;
 - Compliance requirements and expectations;
 - Review and approval processes, structures and policies;
 - Exemption, exception and appeals processes;
 - Monitoring- and auditing-related requirements; and
 - Security awareness and training materials.

Principle 6 – Administration – *Conform to Statutory Requirements*

Compliance with FIPPA, MFIPPA, PHIPA and successor legislation is a mandatory requirement.

Rationale:

The enterprise security architecture, security standards and guidelines will enable implementation of access and privacy related statutory and regulatory requirements (e.g., *Freedom of Information and Protection of Privacy Act* and related statutes, *Ontario Government Privacy Design Principles*).

Implications:

The OPS enterprise security architecture, security policies, standards and guidelines must be designed to enable implementation of the access and privacy requirements of the *Freedom of Information and Protection of Privacy Act* and the *Ontario Government Privacy Design Principles*.

Availability**Principle 1 – Availability – Security Process Support**

I&IT enterprise security architecture addresses availability of information assets, I&IT-based resources holding and supporting security infrastructure, processes and structures.

Rationale:

The enterprise security architecture will support key security processes such as monitoring and incident response, business continuity and contingency planning (business Impact/Risk Assessment and Analysis), disaster recovery, security configuration and capacity planning and security operations measures.

Implications:

The OPS security standards and guidelines and operations processes must address:

- Monitoring and reporting;
- Incident response;
- Business continuity planning;
- Disaster recovery (DR) and contingency planning;
- Security design and implementation;
- Security configuration and capacity planning;
- Assurance;
- Forensics; and
- Security operations planning (e.g., identity and access control, identity [user id] management).

Principle 2 – Availability – Controls Consistent with Risk & Value

Safeguards to protect against breaches of security will be implemented to reduce potential risk to I&IT assets and resources.

Rationale:

The safeguards and level of response to threats will be consistent with the value, vulnerability and sensitivity of protected assets or resources.

Implications:

The OPS I&IT enterprise security architecture policies and procedures must include:

- A statement defining what constitutes a breach of security and a delineation of which incidents and occurrences are security events rather than security incidents (Metaphorical example: rattling the door knob to see if it is locked vs. trying to pick the lock).

The OPS I&IT enterprise security architecture policy, standards and guidelines must define requirements for:

- Information data sensitivity classification;
- Safeguards to prevent security incidents including patch management; and
- A comprehensive set of mechanisms to assist with the detection, correction, recovery and response to security breaches.

The OPS I&IT security operational processes must define:

- Responses to threats that are consistent with the value and sensitivity of the I&IT assets and resources; and
- Commitment to and demonstrable ability to support evidence preservation requirements of the enterprise.

Assurance**Principle 1 – Assurance – Standards-based Security Services**

The OPS will adopt and comply with industry-accepted/standard approaches regarding due-diligence and standards of care in order to ensure the secure delivery of OPS I&IT-based services and seamless and incident-free information exchange with and between non-OPS parties.

Rationale:

Security measures will comply with OPS and industry standards and security will be upheld when parties interact either in a Government-to-Government (G2G), Government-to-Citizen (G2C), or Government-to-Business (G2B) context.

Implications:

OPS I&IT security architecture must define and improve:

- Security processes and structures;
- Communication strategies, materials, plans and resources;
- Compliance-related information resources and training tools;

- Asset control and protection strategies, services and mechanisms;
- Monitoring and auditing protocols, processes and techniques; and
- Enterprise-wide understanding of the legal ramifications for non-compliance with security-related policies, directives, and statutory/regulatory requirements.

OPS Security Standards and Guidelines must include control requirements for third parties.

Principle 2 – Assurance – Policy Compliance & Appropriate Response

As per Management Board of Cabinet approved OPS directives, operating policies, procedures and guidelines, ministries (and related scheduled agencies, boards and commissions as required) will comply with corporate policies and standards related to security as a minimum. These organizations may supplement or enhance corporate I&IT security-related standards and guidelines where and when needed or appropriate for their specific organization.

Rationale:

The viability, protection, safeguarding, integrity, confidentiality and availability of I&IT assets and resources necessary to support programs and services will be assured.

Implications:

Security services and mechanisms will be employed as required, including: confidentiality, integrity, availability, reliability, authentication, authorization, accountability, and auditability.

Security and privacy review requirements must be included in all contractual and related arrangements involving access to OPS I&IT resources or exchange of information assets in the custody and care of the Ontario Government (e.g., Memoranda of Understanding, Service Level Agreements) with parties external to the OPS.

Principle 3 – Assurance – Accountability for Risk Acceptance

I&IT architecture or systems which do not comply with approved I&IT Security Directives, Policies, Standards, Guidelines or Processes must be formally reviewed and risk accepted by both the Program Director and Corporate Security Officer.

Rationale:

The appropriate level of oversight, accountability, management visibility/transparency and decision-making will be applied with respect to the implementation and operation of I&IT systems that are non-compliant with OPS I&IT security requirements.

Implications:

Need to design:

- Risk management processes consistent with the value and sensitivity of I&IT assets and resources.

Need to ensure that security processes include:

- Compliance reviews and documented approvals; and
- Periodic review of risk accepted systems as required.

Accountability

Principle 1 – Accountability – Ownership and Sensitivity Determination

All OPS I&IT assets and resources must be accounted for and have an owner, steward and custodian identified, documented and designated.

Rationale:

The value and sensitivity of all I&IT assets will be safeguarded in accordance with OPS I&IT security directives, policies, standards and guidelines and the applicable statutory frameworks.

Implications:

- Determine and assign responsibilities, accountabilities, obligation, conditions and rules for designating accountability and authority to parties for securing assets and resources;
- Have a process to inventory all OPS I&IT assets and resources and designate person(s) accountable for same;
- Develop security plan, processes and structures at the program level;
- Exercise proper employment of the information and data sensitivity classification requirements of the OPS;
- Design reasonable security measures and ensure they are implemented in order to safeguard the confidentiality, integrity and availability of I&IT assets and resources;
- Define a threat/risk mitigation process for design and development of enterprise-architecture and I&IT systems and infrastructure; and
- Acknowledge delegation or contracting-out of operational activities in I&IT Cluster – must ensure that outsourcing or contracting out activities do not fetter lines of accountability of business owner and program heads.

Principle 2 – Accountability – *Parties Adhere to Security Policies*

Parties are accountable for the appropriate and responsible use of I&IT assets and resources in support of the goals and objectives of the overall OPS I&IT enterprise security architecture.

Rationale:

Adherence to enterprise security policies and standards is essential to achieve and maintain required levels of security.

Implications:

- Ensure enterprise architecture and systems are managed, operated and used appropriately, and to ensure remedies are available to the OPS in the event of a breach;
 - Parties who do not adhere to security policies and standards may be subject to disciplinary actions;
- Respond as appropriate to education and training requirements relating to I&IT security policies, guidelines, standards and directives;
- Ensure job descriptions outline responsibilities regarding security-related matters;
- Ensure proper vetting, document and approval of rules, conditions and obligations of employment; and
- Ensure appropriate and ongoing security auditing, monitoring, logging and reporting activities are carried out.

Authorization**Principle 1 – Authorization – Auditable Rule-Based Access**

Access to information and information technology assets and systems must be controlled on the basis of business rules, conditions and obligations.

Rationale:

Access controls for operational systems must be demonstrably auditable.

Implications:

Enable security, privacy and confidentiality by limiting access to information and I&IT assets and resources in accordance with the principles of least privilege and separation of duties.

Using data and information classification and sensitivity requirements and related operating procedures, define the safeguards required for information holdings according to their classification.

Principle 2 – Authorization – Restricting Secure Facilities Access

Access to secure locations will be restricted to those with legitimate requirements. Security measures must isolate protected assets and resources from threats, consistent with the value and sensitivity of the information and data holdings.

Rationale:

I&IT assets must not be vulnerable to security threats or hazards.

Implications:

Ensure that standards are defined, approved, implemented, and enforced for safeguarding access to secure facilities and I&IT assets.

Awareness and Training

Principle 1 – Awareness and Training – *All OPS Employees Responsible*

Awareness of Information and IT security is the responsibility of every OPS employee and agent.

Rationale:

Awareness and training facilitates the consistent execution of I&IT security programs and plans across the OPS and an adequate and uniform security posture for the organization.

Implications:

- Include security and privacy responsibilities in job descriptions and contracts;
- Train all employees and agents in security procedures and incident reporting processes; and
- Include compliance related wording (including compliance monitoring) in the Conditions of Employment as appropriate.

Principle 2 – Awareness and Training – Managers Responsible for Security Awareness and Training

Awareness and training programs are an integral and on-going component of the OPS I&IT security and it is the manager's responsibility to ensure staff members are adequately trained.

Rationale:

A security awareness culture within the Ontario Public Service will reduce the overall threat of security breaches through human error or negligence.

Implications:

- Train all employees in security procedures, policies and standards as well as incident reporting protocols; and
- Include compliance (including compliance monitoring) in the Conditions of Employment.

References

- Management Board of Cabinet Directive: *Information and Information Technology Security* – March 3, 1998 (for historical alignment)
- Management Board of Cabinet Directive: *Information and Information Technology Security* – August 5, 2005
- *Information Security and Privacy Classification, Office of the Chief Information Privacy Officer – OCIPPO – June 2006*
- *Data Matching Directive* – Corporate Security Branch
- Information and Information Technology Security: *Operating Procedure on Usage of I.T. Resources* – June 2006, Corporate Security Branch
- Information and Information Technology Security: *Operating Procedure on Internet, Intranets and Extranets* – January 2007, Corporate Security Branch
- British Standard – *ISO/IEC 27002:2005 (17799) Information System Security Code of Practice*
- US Department of Commerce – National Institute of Standards and Technology (NIST) Special Publications
- *META Structured Transformation Program Reference Model for Achieving Information Security* - 2003

7. Privacy Design Principles for Personal Information

Objectives:

To ensure that the government:

- protects the privacy of individuals with respect to personal information about themselves held by institutions,
- provides individuals with a right of access to that information as stated in the Freedom of Information and Protection of Privacy Act (FIPPA).

This means the Government of Ontario's Enterprise Information & Information Technology Architecture in all its stages, from planning through development, will, at a minimum, comply with FIPPA legislation.

Background

The mandate of the Enterprise Information and Information Technology Architecture (EIA) project was to develop a business-driven, top-down, government-wide architecture that would provide a framework and foundation for all information and information technology projects across the Government of Ontario. The resulting enterprise architecture serves as a management tool to co-ordinate initiatives across the government and to manage the impact of emerging technologies.

In Ontario, data protection legislation provides the business direction regarding how personal information is to be collected, used, disclosed and retained. For the most part, the objective with technology design in the past has been to ensure that the data being captured is kept in a secured manner. While data security is essential to the achievement of privacy protection, security does not equal privacy. Privacy relates to the informed consent and the control a person exerts regarding the collection, use and disclosure of their personally identifiable information. Security is concerned with the authentication, integrity, confidentiality and non-repudiation aspects of the data. Since the introduction of Ontario's Freedom of Information and Protection of Privacy Act, the power of Information Technology (IT) to collect, match, manipulate and re-use information has grown exponentially. The capacity of IT to collect, process, store and link information, including personal information, from separate government programs has increased the ability to manage, maintain and provide accurate information. This increase in the power and capacity of IT introduces real and perceived risks to personal privacy if the technology is not designed at the outset to build in privacy. Modern technologies, including commercial "off-the-shelf" offerings, and technology driven business redesign pose new privacy risks if not implemented and managed carefully. In addition to violating the spirit or legal obligations of privacy legislation, they risk the accidental or deliberate creation of the capacity for overt or covert data surveillance and profiling of individuals. Limiting a technology's ability to conduct surveillance ensures privacy.

The use of privacy design principles is one part of a two part process to ensure that new initiatives meet privacy protection requirements. Incorporating the privacy design principles at the beginning of business and I & IT planning cycles will ensure that, proposals be developed whose business and systems details conform to privacy

objectives. It will also ensure that I & IT initiatives clearly identify any circumstances where privacy may be at risk and any specific design and implementation initiatives that need to be introduced.

This approach should preclude inappropriate investments in strategies and development work, or the need to substantially revise such projects after an assessment of the project's privacy impact. A privacy impact assessment (PIA), the second part of the privacy compliance process, is an MBC requirement prior to approval of projects that involve changes in the management of personal information held in trust by government programs.

The Government of Ontario is committed to ensuring the personal privacy of Ontario's citizens. The privacy of individuals must be an integral component of the design of new technology or information systems, not only at the beginning but throughout the development and maintenance of the technology or system.

The Purpose of Privacy Design Principles

Provincial, Territorial and Federal Ministers responsible for the Information Highway confirmed the importance of privacy protection at their June 12, 1998 meeting. The Ministers agreed to support the Canadian Standards Association Model Privacy Code as a minimum privacy standard and urged their colleagues and industries within their respective jurisdictions to meet or exceed the CSA Standard in their operations. The Ontario government is committed to keeping the personal information it collects accurate and, secure. It is also committed to I & IT that has privacy design principles built in at the outset. Privacy design principles support the informed consent and the control a person has on his or her personally identifiable information. Developing I & IT that is built on privacy design principles will ensure that individuals can make informed decisions about the purposes for which their personal information is collected or disclosed. The privacy design principles adhere to the *Freedom of Information and Protection of Privacy Act (FIPPA)* under legislation. The principles also reflect the CSA Model Privacy Code and the Fair Information Practices that embrace an international standard regarding privacy. These principles provide a framework used in the development and ongoing refinement of the Government of Ontario's Enterprise Information and Information Technology Architecture and will ensure that the government protects the privacy of individuals with respect to personal information about themselves held by institutions and to provide individuals with a right of access to that information.

In a number of the principles, reference is made to the use of privacy impact assessments (PIA). The need for a PIA is dependent on the extent and significance of the changes or additions to be made in a technology or in an information system; a full PIA may not be required to evaluate and address privacy concerns in all cases.

All information or information technology projects which involve changes in the management and/or use of personal information must satisfy the PIA requirements before MBS approvals for funding or ministry approval to begin the project. In some cases, a full PIA will be required before the project can begin, whereas, in other cases, the PIA can be completed in stages aligned with the project. Guidelines and processes for determining PIA requirements will be developed.

LEGISLATIVE REQUIREMENTS

The *Freedom of Information and Protection of Privacy Act* (FIPPA) applies to Ontario's provincial ministries and most agencies, boards and most commissions, as well as community colleges and district health councils.

The Act requires that the government protect the privacy of individuals with respect to personal information about themselves held by institutions, and to provide individuals with a right of access to that information. The Act also gives individuals the right to request access to government information.

The Freedom of Information and Protection of Privacy Act (FIPPA) establishes the obligations of institutions

to protect the privacy of individuals with respect to personal information about themselves held by institutions and to provide individuals with a right of access to that information. R.S.O. 1990, c. M.56, s. 1.@

The act defines personal information, as

" recorded information about an identifiable individual, including,

- (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,*
- (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,*
- (c) any identifying number, symbol or other particular assigned to the individual,*
- (d) the address, telephone number, fingerprints or blood type of the individual,*
- (e) the personal opinions or views of the individual except where they relate to another individual,*
- (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,*
- (g) the views or opinions of another individual about the individual, and*
- (h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual; ("renseignements personnels")*

and records systems as

"personal information bank" means a collection of personal information that is organized and capable of being retrieved using

an individual's name or an identifying number or particular assigned to the individual; ("banque de renseignements personnels")

"record" means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, and includes,

*(a) correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, a machine readable record, any other documentary material, regardless of physical form or characteristics, and any copy thereof, and
(b) subject to the regulations, any record that is capable of being produced from a machine readable record under the control of an institution by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution; ("document") R.S.O. 1990, c. F.31, s.2.*

The Act further requires institutions to be open about the personal information under their control by requiring that

A head shall cause to be included in a personal information bank all personal information under the control of the institution that is organized or intended to be retrieved by the individual's name or by an identifying number, symbol or other particular assigned to the individual. R.S.O. 1990, c. F.31, s.44.

Personal Information Bank Index

The responsible minister shall publish at least once each year an index of all personal information banks setting forth, in respect of each personal information bank,

*(a) its name and location;
(b) the legal authority for its establishment;
(c) the types of personal information maintained in it;
(d) how the personal information is used on a regular basis;
(e) to whom the personal information is disclosed on a regular basis;
(f) the categories of individuals about whom personal information is maintained;
and
(g) the policies and practices applicable to the retention and disposal of the personal information. R.S.O. 1990, c. F.31, s. 45. @*

FIPPA represents the Legislature's recognition that privacy is not absolute. Competing interests regarding individual privacy include the person's or data subjects interest in fully controlling how the government collects, uses and discloses his or her personally identifiable information, the public interest (e.g., public safety), and governmental requirements (e.g., reducing welfare fraud). For example, there are specific provisions which provide the authority, without consent, to collect, disclose, or refuse disclosure of

personal information for limited purposes relating to law enforcement, or to disclose in compelling circumstances the health and safety of an individual with notice sent to the last known address.

The requirements of FIPPA are the absolute minimum requirements for the protection and management of personal information that need to be followed. There are some cases where there are legislated exemptions regarding a program or specific records exempt from the requirements under FIPPA.

Over time the structures of government, the roles of programs, and interpretations of the public interest may change and be reflected in new or amended statutes. Accordingly, these design principles will evolve and be refined to reflect the statutory changes.

RELATED REQUIREMENTS

There are a number of information management requirements that must be considered in the development of I & IT projects. These principles address privacy. Related but separate requirements not addressed in these principles include access to non-personal government information, recorded information management (RIM), and responsibilities under archives legislation.

PRIVACY DESIGN PRINCIPLES

The component architectures of EA are business, information, application, security and technology. Each of the privacy design principles must be applied against each of these components.

In addition to the privacy design principles, consideration should be given to incorporating the privacy enhancing advantages of particular technologies which permit anonymity, pseudonymity, improve security and maintain segregation of personally identifiable data to limit surveillance risks.

In addition to the requirements of FIPPA, which form the basis of the Privacy Design Principles, the following specific Design Principles apply.

1. Accountability

Privacy Principle

Ontario government ministries and agencies are accountable for personal information that is under their custody or control. This includes situations where ministries are in possession of the personal information (custody) or situations where ministries retain the ability to manage, restrict or administer the collection, use or disclosure of the personal information in the hands of third parties (control).

Design Principle

Information and Information Technology sponsors will designate a point of accountability through individual(s) to be held accountable for managing the privacy of personal information in the design and development and implementation of initiatives.

Accountability practices include:

1. Ensuring all privacy design principles have been incorporated

into the technology design, overseeing the organization's privacy impact assessments, initial and ongoing security risk assessments.

2. Ensuring information systems are capable of providing access to personal information on request and have the capacity to record who has/had access to the personal information and for what purpose.
3. Ensuring staff managing the data are trained on privacy protection requirements.
4. Ensuring information systems are transparent and documented so that individuals can be informed about how their personal information is collected, used and disclosed.
5. Establishing regular security and privacy compliance audits commensurate with risks to the data subjects and governmental operations, utilizing as appropriate internal auditors, public oversight agencies and external independent auditors

2. Identifying the Purpose for Collecting Personal Information

Privacy Principle

Ministries and agencies will identify the purpose for which personal information is lawfully collected at or before the time the information is collected.

Design Principle

Organizations must clearly identify and document the purpose(s) for which they collect personal information. The identification of collection purposes must be conducted in a systematic and evidence based fashion. Systems design must ensure the systems outcome is limited to the purposes for which personal information may be lawfully collected, used and disclosed. Attention must also be paid to all instances where personal information is disclosed regularly to other programs.

3. Limits for Collecting Personal Information

Privacy Principle

FIPPA prohibits the collection of personal information unless the collection is expressly authorized by statute, used for law enforcement or is necessary for the proper administration of a lawfully authorized activity.

Design Principle

Limits on the collection of personal information must be incorporated into the design of information systems to ensure that extraneous or unnecessary personal information is not collected. A privacy impact assessment should be completed in all cases where significant changes to collection practices are proposed or where additional personal information is to be collected for purposes other than for those previously identified or authorized.

Common multi-program identifiers must be avoided for use with unrelated programs. Distinct identifiers for unrelated programs are required to reduce the opportunity for improper data matching. Design strategies that are based on data subject anonymity or pseudonymity are the preferred approach for applications that aggregate data from multiple programs for data mart/warehouse business analysis.

4. Obtaining Consent

Privacy Principle

While consent is not the only legal means authority by which to collect, use, and disclose and destroy personal information, obtaining consent will often be the preferred approach.

Design Principle

An information management system should be designed to capture the subject's consent or lack of consent to the collection, use or disclosure of their personal information. Consent should never be assumed. The design of the technology used in any interaction with clients should include the ability to identify in the system whether consent was provided or not and/or whether it was required or not.

Consent can be provided by traditional methods such as a signature on a mandated form, or through the use other means such as the use of access cards. For example, where an individual initiates a transaction with the Government of Ontario by using an ATM machine, it can be implied that consent has been given for the use of the personal information for the business transaction. However, consent could not be implied for other uses or disclosures that an average customer would not reasonably expect to be required to execute the transaction.

5. Limits For Using, Disclosing, And Retaining Personal Information

Privacy Principle

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as specifically authorized by law. Personal information should be retained only as long as necessary for the fulfillment of those purposes.

Design Principle

It cannot be assumed that where an individual has provided personal information for one purpose, the information may be used or disclosed to another Government body for an unrelated purpose.

Information systems must be designed to ensure that personal information cannot be used or disclosed for unauthorized purposes.

FIPPA requires that where personal information is used or disclosed for purposes other than those described in the Directory of Records, the circumstances of such use or disclosure must be attached or linked to the personal information. Information systems must be designed to record/reveal such attachments or links.

Data matching, or the aggregation of personally identifiable information from distinct program databases, whether for periodic, or data mart/warehouse functions, is only permitted when in compliance with the Management Board Directive on Data Matching.

6. Keeping Personal Information Accurate

Privacy Principle

Personal information should be accurate, complete and timely. The individual who provides the personal information must have access to the data kept on file about them.

Design Principle

Information systems should be designed to ensure that personal information can be accessed and corrected upon request, or that a record of an individual's disagreement with the accuracy of the record can be attached to the original record. The technology should have the ability to identify when data has been changed or modified, by whom, and for what reason in order to ensure accountability.

A history of correction transactions is to be retained. The technology should be designed so that this historical information or any inaccurate information is not routinely disclosed to persons other than the data subject. Anyone who has accessed inaccurate or historical information that is changed must be informed regarding the changes in a timely manner.

7. Safeguarding Personal Information

Privacy Principle

All personal information shall be protected by security safeguards appropriate to the sensitivity of the information and the risks to both data subjects and the government inherent in the information management architecture.

Design Principle

Organizations should conduct information classification reviews to determine the appropriate level of security to be applied to personal information. The level of security is dependent upon the sensitivity of the information, its value to authorized programs, and its value to unauthorized individuals or organizations.

Initiatives that have the potential to increase the accessibility of personal information in an information system should implement the most recent standards regarding encryption and Public Key Infrastructure (PKI).

Methods to protect personal information could include:

- data encryption
- access controls
- remote access two-way user authentication
- log in and password management
- monitoring and auditing of employee access to personal information
- risk assessments.

8. Openness

Privacy Principle

Ministries/agencies shall be open about the policies and procedures that apply to the management of personal information. Specific information about policies and practices

relating to the management of personal information shall be readily available. An individual shall be informed of the existence, use and disclosure of his or her personal information.

This principle is essential to the operation of Principle #1 - Accountability and Principle #2 - Identifying the Purpose for Collecting Information.

Design Principle

An information system involving personal information should be transparent, so that individuals can verify how their information is being collected, used, or disclosed or destroyed. The types of transactions, the linkages within the system and the way in which personal information is collected, used, disclosed and retained must be clearly visible to data subjects and to system users. When requested, ministries and agencies should be able to provide a full description of all circumstances where the organization discloses an individual's personal information to third parties.

Who has the authority to access what information and for what purpose must be clearly identified. When program or legislative changes are made to a program, information about the change in the policy and the technology must also be available upon request. Consequently, information system changes must be clearly documented and readily available, unless to do so would reveal details about security-related activities.

9. Persons Will Have Access to Their Personal Information***Privacy Principle***

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of his or her information and have it amended as appropriate.

Design Principle

An information system should be able to provide an individual with copies of the personal information that is kept on files stored throughout the information management system without disrupting the on-going operation of the organization.

Information systems must be designed to facilitate access by individuals to their personal information retained on the system, except where such access is not legally permitted (e.g. certain law enforcement information). Upon request, an explanation must be available to the individual explaining in easily understood terms what the data fields mean, e.g. what personal information is retained in each field. The system should be designed to provide this information at the least cost possible to the individual. This principle complements Principle # 8 - Openness, in terms of how specific requests for more detailed information by individuals need to be addressed in information systems. Individuals have the right to disagree and to correct their personal information. An information management system must be able to amend or annotate any personal information that is subject to disagreement regarding accuracy. The system must also have the capacity to notify third parties to whom incorrect personal information has been disclosed within the year preceding the correction of the changes to information or the letter of disagreement.

10. Challenging Compliance

Privacy Principle

An individual shall be able to address a challenge concerning compliance with privacy requirements to a designated individual.

Design Principle

Ministries and agencies are accountable for the management of personal information under their custody or control and must respond to inquiries raised by individuals with respect to the management of their personal information. The use of agents or outsourcing does not reduce this obligation. Agent or outsourcing agreements must specify the mechanisms to ensure the ministry or agency can meet its compliance obligations. Compliance issues may be raised directly with individual ministries/agencies or may be communicated through the Office of the Information and Privacy Commissioner.

Information systems should be designed so that all transactions made on an individual's file can be traced for accountability purposes. It should identify who input changes to a file, when the input was initiated and for what purpose.

A history of transactions should be retained for a determined length of time for audit purposes, to respond to privacy complaints or to support requests for information from an individual. Unless otherwise specified in legislation, FIPPA requires a minimum one-year retention period after the PI has been used. In most information systems, the program's record retention schedules and archive requirements will exceed the FIPPA minimums.

8. Copyright Information

© Queen's Printer for Ontario 2010