Management and Use of Information & Information Technology (I&IT) Directive

Management Board of Cabinet

February 28, 2014
TABLE OF CONTENTS

PURPOSE .............................................................................................................................................. 1
APPLICATION AND SCOPE ............................................................................................................... 1
PRINCIPLES ........................................................................................................................................ 1
   ENABLE PUBLIC POLICY DELIVERY THROUGH THE USE OF INFORMATION AND INFORMATION TECHNOLOGY ........................................................................................................ 1
   ENSURE PRUDENT INVESTMENT IN INFORMATION AND INFORMATION TECHNOLOGY TO SUPPORT BUSINESS ENDS .................................................................................. 2
   MANAGE RISKS ASSOCIATED WITH THE I&IT PORTFOLIO ......................................................... 2
MANDATORY REQUIREMENTS ........................................................................................................... 2
   1. Governance .................................................................................................................................. 2
   2. Infrastructure ................................................................................................................................ 3
   3. Service Management .................................................................................................................... 3
   4. I&IT Solution Choices .................................................................................................................. 4
   5. Enterprise Architecture and Standards ......................................................................................... 4
   6. Management of I&IT Assets .......................................................................................................... 5
   7. Project Management ..................................................................................................................... 5
   8. Information Management ............................................................................................................. 6
   9. I&IT Security ................................................................................................................................. 7
   10. Identity, Authentication and Authorization ................................................................................ 7
   11. Risk Management ....................................................................................................................... 7
RESPONSIBILITIES .......................................................................................................................... 9
   MANAGEMENT BOARD OF CABINET (MBC) ...................................................................................... 9
   MINISTER OF GOVERNMENT SERVICES (MINISTER) ....................................................................... 9
   INFORMATION AND INFORMATION TECHNOLOGY DEPUTIES COMMITTEE (IITDC) .................. 9
   INFORMATION AND INFORMATION TECHNOLOGY PROJECT APPROVAL COMMITTEE (ITPAC) 9
   DEPUTY HEADS (DEPUTY MINISTER OR EQUIVALENT AND AGENCY HEADS) ......................... 9
   CHIEF ADMINISTRATIVE OFFICERS ............................................................................................ 10
   I&IT ORGANIZATION ...................................................................................................................... 10
   CORPORATE ARCHITECTURE REVIEW BOARD (ARB) ................................................................. 11
   POLICY MANAGEMENT AUTHORITY (PMA) ................................................................................. 11
   INTERNAL AUDIT DIVISION ........................................................................................................... 11
   PROGRAM MANAGERS .................................................................................................................. 12
   ALL OPS AND APPLICABLE AGENCY STAFF ................................................................................. 12
APPENDIX A: DEFINITIONS ............................................................................................................... 13
PURPOSE

The purpose of this Directive is to establish policy and control parameters for the management and use of information and information technology (I&IT) in the Ontario Public Service (OPS). This Directive is supported by a policy framework that elaborates expectations pursuant to it.

Compliance with this Directive and the supporting I&IT policy framework will enable more efficient operations and improved delivery of government programs.

APPLICATION AND SCOPE

This Directive applies in its entirety to all ministries.

All Advisory and Adjudicative agencies are subject to this Directive.

If an agency, as defined under the Agency Establishment and Accountability Directive, is receiving I&IT services or products from the OPS, a list of these services and products, as well as the corresponding application of this Directive, in whole or in part, will be attached as a schedule to the Memorandum of Understanding with the agency concerned.

Ministries or agencies seeking exemptions from the mandatory requirements of the Management and Use of I&IT Directive must receive prior Management Board of Cabinet approval.

PRINCIPLES

The management of information and information technology in the OPS is governed by the following principles:

Enable public policy delivery through the use of information and information technology

a) The I&IT Organization is a strategic partner and service provider to business areas across the OPS in supporting government priorities and delivering government information and services to the public.

b) The I&IT Organization will be accountable for evolving with technology to provide creative and innovative solutions in order to meet existing and emerging citizen and customer expectations.

c) The I&IT Organization will be accountable for enabling collaboration, sharing, distribution and efficient and timely access to data, information and services.
**Ensure prudent investment in information and information technology to support business ends**

d) Information and information technology are assets that must be managed strategically, cost-effectively and transparently by the I&IT Organization to support public accountability and prudent use of public funds, including exploring strategic opportunities to partner with the broader public sector and other jurisdictions.

e) Collaboration between I&IT and business areas must be transparent, with active governance processes that support strategic and timely decision-making.

f) The I&IT Organization will be accountable for standardizing the OPS technology environment and maximize re-use of existing I&IT solutions, where appropriate, in order to simplify user experience, reduce duplication, maximize efficiencies, and reduce lifecycle costs.

**Manage risks associated with the I&IT portfolio**

g) Government information, systems and resources must have integrity, and be protected and secure.

h) I&IT projects must achieve clear deliverables, add value to the OPS, be completed on time and within budget, and serve a clear business or strategic need.

**MANDATORY REQUIREMENTS**

1. **Governance**

Ministries must:

1.1 Consult with their assigned I&IT Cluster when developing and/or updating Memoranda of Understanding with agencies.

The I&IT Organization must:

1.2 Establish appropriate I&IT governance bodies in accordance with corporate governance frameworks.

Ministries, applicable agencies, and the I&IT Organization must:

1.3 Participate as appropriate in, and comply with decisions of, cluster and corporate I&IT governance bodies.
2. **Infrastructure**

Ministries, applicable agencies and the I&IT Organization must:

2.1 Use OPS I&IT infrastructure services; and

2.2 Migrate to supportable infrastructure within a timeframe acceptable to the Corporate Chief Information Officer (CCIO).

The I&IT Organization must:

2.3 Provide I&IT infrastructure services that are cost-competitive for the OPS.

3. **Service Management**

Ministries must:

3.1 Acquire, develop or procure\(^1\) all I&IT services and products from or through the I&IT Organization. I&IT services are defined in the I&IT Service Catalogue or designated as a Mandatory Central Common Service supplied by the I&IT Organization per the Procurement Directive.

Applicable agencies must:

3.2 Use the I&IT services that are specified to apply to them in their Memoranda of Understanding, as defined in the I&IT Service Catalogue.

Ministries and the I&IT Organization must:

3.3 Proactively work to identify service needs and assess opportunities for new I&IT services.

The I&IT Organization must:

3.4 Provide I&IT services for the OPS;

3.5 Define I&IT services in the I&IT Service Catalogue;

3.6 Design I&IT services in consultation with clients to meet their needs and that are supported by transparent and predictable billing arrangements;

3.7 Ensure that I&IT services are subject to performance measurement and management and are periodically amended to ensure responsiveness to client needs; and

3.8 Manage assets and information that support I&IT service delivery effectively, efficiently, securely and strategically.

---

\(^1\) Refer to the Procurement Directive for procurement requirements.
4. **I&IT Solution Choices**

Ministries and applicable agencies must:

4.1 Re-use existing I&IT solutions that are available and recommended by their I&IT Cluster, where appropriate and feasible.

Ministries and the I&IT Organization must:

4.2 Collaborate on I&IT solutions that support the OPS’ interactions with the public, including internet channels and the use of social media.

The I&IT Organization must:

4.3 Develop or approve I&IT solutions, including mobile applications, that are run on the OPS I&IT infrastructure, in accordance with applicable policies;

4.4 Design or acquire I&IT solutions in consultation with clients to align with OPS strategies and priorities and meet clients’ needs and input;

4.5 Support re-use of existing I&IT solutions through identification, selection, management, promotion, and governance of I&IT solutions;

4.6 Ensure that all new applications enable the sharing of machine-readable data where appropriate and in accordance with applicable policies and standards; and

4.7 Manage Government of Ontario web presence (both internet and intranet) in accordance with applicable policies, standards, and guidelines.

5. **Enterprise Architecture and Standards**

Ministries and applicable agencies, supported by the I&IT Organization, must:

5.1 Develop and maintain Business Architecture for their I&IT projects and ensure compliance with applicable OPS directives and policies in this architecture.

Ministries, applicable agencies, and the I&IT Organization must:

5.2 Participate in the architecture governance process for their I&IT projects at both cluster and corporate levels;

5.3 Adhere to Government of Ontario Information Technology Standards (GO-ITS); and

5.4 Participate in and ensure Architecture Review Board review of all cross-cluster and enterprise-wide projects, common infrastructure projects, projects which have an extensive or unique impact on the business and technology environment, and any other projects as identified by the CCIO, by Management Board of Cabinet Support Branch, or by I&IT Strategy and Cyber Security Division, Ministry of Government Services, or a cluster CIO.
The I&IT Organization must:

5.5 Establish Enterprise Architecture and architecture policies and standards, and govern appropriate execution of Enterprise Architecture; and

5.6 Establish Government of Ontario Information Technology Standards (GO-ITS) and govern their use.

6. Management of I&IT Assets

Ministries, applicable agencies and the I&IT Organization must:

6.1 Manage the portfolio of I&IT assets that they own using approved I&IT asset management policies, standards and approaches, including but not limited to:
   a. tracking I&IT assets and maintaining accurate inventories and performance information;
   b. proactively identifying the extent to which their remaining life meets required performance (i.e. technical and business needs);
   c. recommending expenditure plans to optimize performance and decrease portfolio risks through asset renewal and/or decommissioning, including the identification of priority initiatives; and
   d. capitalizing investments per the Ministry of Finance Tangible Capital Asset Accounting Policy.

6.2 Report on the infrastructure and business application assets that they own through the reporting process and tools developed by the CCIO, to support cluster and OPS-wide asset management reporting and investment portfolio recommendations; and

6.3 Safeguard OPS I&IT assets that are in their custody, and provide information on the movement of assets in their custody to the asset owner to support tracking and reporting.

The I&IT Organization must:

6.4 Provide cluster and OPS-wide I&IT asset management portfolio reporting and expenditure plan recommendations, including the identification of OPS-wide priority asset management initiatives and OPS-wide strategies and tools; and

6.5 Establish I&IT asset management policies and standards and institute appropriate governance to ensure their implementation.

7. Project Management

Ministries, applicable agencies, and the I&IT Organization must:

7.1 Manage I&IT projects and project portfolios in accordance with corporate OPS-wide project management methodologies and frameworks\(^2\);

\(^2\) OPS Integrated Project Management Framework and Methodology, and Project Portfolio Management Framework.
7.2 Ensure that I&IT projects proceed through a project review and decision process at identified project lifecycle transitions, in accordance with the Policy on the I&IT Project Gateway Process. The Policy takes precedence over the corporate project management methodologies and frameworks in the event of a conflict;

7.3 Manage I&IT projects in an integrated fashion³;

7.4 Report on I&IT projects and project portfolios through a reporting process and tool approved by the CCIO. Local applications for reporting on projects may be used until decommissioned; and

7.5 Report to Management Board of Cabinet on major I&IT projects through the corporate quarterly Major I&IT Projects Reporting process.

8. Information Management

Ministries, applicable agencies and the I&IT Organization must:

8.1 Manage their information in accordance with corporate policy, standards, guidelines, and best practices;

8.2 Deliver training on information management that is specific to ministry or agency needs;

8.3 Apply records schedules approved by the Archivist of Ontario to information holdings; and

8.4 Provide information to clusters for the purpose of developing annual cluster-level information management plans.

The I&IT Organization must:

8.5 Develop information management policies, standards, guidelines and best practices;

8.6 Support compliance with corporate policies, standards, guidelines and best practices on information management;

8.7 Develop annual information management plans;

8.8 Deliver or support delivery of information management training in ministries; and

8.9 Support planning and implementation of enterprise content management by ministries and provide ongoing support.

³ The OPS Unified I&IT Project Methodology (UPM) identifies all the activities to be considered, and provides an integrated phased methodology guideline for managing I&IT projects in the OPS.
9. **I&IT Security**

Ministries, applicable agencies, and the I&IT Organization must:

9.1 Adequately safeguard information according to its sensitivity level and take steps to ensure that the confidentiality, availability and integrity requirements of all information, systems and resources are met;

9.2 Implement security controls appropriate to levels of risk in accordance with security policy or security testing and evaluation recommendations to minimize risk or mitigate vulnerabilities to information, systems and resources;

9.3 Identify security requirements for new solutions that must be included in program design;

9.4 Ensure that assessments and reviews of security controls are periodically performed and testing conducted, including prior to implementation of a major change or upgrade, or whenever security incidents occur; and

9.5 Provide security awareness training to all users and ensure that they receive any additional training that may be required by their job function or in view of the sensitivity of the information, systems and resources to which they have access.

The I&IT Organization must:

9.6 Develop I&IT security policies, standards and guidelines.

9.7 Develop I&IT security awareness training for OPS staff.

10. **Identity, Authentication and Authorization**

Ministries, applicable agencies, and the I&IT Organization must:

10.1 Ensure that the identities of all users of non-public information and information technology are known and that access to their information, systems and resources is managed appropriately and only provided via an approved authentication process consistent with Identity, Authentication and Authorization (IAA) policies.

11. **Risk Management**

Ministries, applicable agencies, and the I&IT Organization must:

11.1 Collaborate to manage I&IT risks in accordance with applicable policies, and exercise prudence in accepting residual risks.

---

4 Major changes are those that have the potential to impact either a large number of users or a critical service, either as part of the change implementation or as a result of a high-risk change failure.
Ministries and the I&IT Organization must:

11.2 Ensure appropriate internal audit coverage of enterprise and ministry I&IT risks and controls.

The I&IT Organization must:

11.3 Identify I&IT risks and develop appropriate mitigation strategies in accordance with applicable policies; and

11.4 Appropriately manage I&IT risks, in accordance with I&IT risk management frameworks and policies.
RESPONSIBILITIES

Management Board of Cabinet (MBC)
The responsibilities of MBC include:

- reviewing and approving exemption requests from the mandatory requirements of this Directive;
- reviewing the Major I&IT Projects Report on a quarterly basis; and
- approving major I&IT projects costing $20M or more.

Minister of Government Services (Minister)
The responsibilities of the Minister include:

- establishing, amending, replacing or rescinding policies on the management and use of I&IT that are consistent with this Directive, setting out more detailed operational requirements for ministries, clusters and agencies;
- approving exemptions from any requirements of the policies for the management and use of I&IT made pursuant to this Directive;
- periodically reporting to MBC on the making of policies, for the purpose of demonstrating prudence and due diligence; and
- periodically making recommendations to MBC on updating this Directive.

Information and Information Technology Deputies Committee (IITDC)
The responsibilities of IITDC include:

- recommending policies to the Minister pertaining to the management of information and information technology that are consistent with this Directive;
- providing advice to the Minister with respect to I&IT policy setting consistent with this Directive; and
- ensuring alignment of I&IT strategy and policy with the government’s business directions.

Information and Information Technology Project Approval Committee (ITPAC)
The responsibilities of ITPAC include:

- approving I&IT projects, or recommending I&IT projects to MBC, in accordance with the Policy on the I&IT Project Gateway Process.

Deputy Heads (Deputy Minister Or Equivalent And Agency Heads)
The responsibilities of Deputy Heads include:

- ensuring ministry and applicable agency compliance with this Directive and policies and standards made pursuant to the Directive;
• articulating ministry strategies, priorities and service needs;
• ensuring that ministries and applicable agencies acquire, develop or procure all I&IT services from or through the I&IT Organization;
• ensuring one accountable executive is assigned as a project sponsor to each I&IT project;
• participating in I&IT governance bodies and processes as required; and
• providing CIOs with notice of agency MOUs under development where I&IT may be asked to provide service to an agency.

Chief Administrative Officers

The responsibilities of CAOs, or other Assistant Deputy Minister as appointed by the Deputy Minister, include:

• providing controllership for ministry resources, including providing oversight for ministry I&IT budgets and expenditures.

I&IT Organization

The responsibilities of the Corporate Chief Information Officer (CCIO) and I&IT Corporate Offices include:

• providing leadership and direction to ministries on this Directive and all policies made under this Directive;
• monitoring compliance with the approved policy framework;
• interpreting this Directive and the related policy framework, and resolving any disputes in relation to the interpretation or application of this Directive;
• developing and maintaining the I&IT policy framework, including policies, standards, guidelines and best practices;
• ensuring that corporate I&IT strategies support delivery of ministry strategies, priorities and service needs;
• managing their program resources and budgets;
• establishing and governing corporate Enterprise Architecture approaches and artefacts;
• developing, maintaining and delivering infrastructure services for the OPS;
• developing I&IT asset management approaches and accordingly acquiring, managing and disposing of IT infrastructure assets;
• leading development of enterprise directions for I&IT and integrating I&IT planning with broader OPS planning processes through appropriate vehicles, including the I&IT Capital Plan, Asset Management Plan and Enterprise I&IT Plan;
• providing leadership and direction to ministries and clusters on public facing IAA implementation responsibilities and plans;
• supervising the provision and maintenance of public facing IAA implementations; and
• establishing key I&IT processes and governance structures, as well as providing a secretariat function for corporate governance committees.

The responsibilities of Cluster Chief Information Officers (CIOs) include:

• managing their program resources and budgets;
• ensuring cluster compliance with this Directive and all policies made under the Directive;
• providing strategic I&IT advice to cluster ministries and managing the strategic partnership with ministry clients;
• advocating for and on behalf of ministry clients with respect to their business needs that can be met by I&IT;
• providing I&IT products and services to client ministries;
• creating an annual Cluster I&IT operational plan;
• ensuring professional management of I&IT projects for which the Cluster is responsible, in accordance with applicable policies;
• establishing Cluster Enterprise Architecture approaches and artefacts;
• supporting ministry clients in developing and maintaining their Business Architecture;
• managing relationships with I&IT service providers, including Infrastructure Technology Services;
• supporting and delivering horizontal initiatives;
• supporting or representing ministry and agency clients on corporate I&IT governance bodies; and
• reviewing agency Memoranda of Understanding content pertaining to I&IT requirements and providing advice about the appropriateness and capability of the I&IT Organization to provide the service, and the corresponding requirements for agencies to comply, in whole or in part, with this Directive.

Corporate Architecture Review Board (ARB)

The responsibilities of Corporate ARB include:

• approving the architecture, design and delivery of I&IT solutions for the I&IT Organization;
• providing leadership, direction and approval related to Enterprise Architecture within the context of this Directive;
• approving business, logical and physical architecture of reviewed projects; and
• approving Government of Ontario Information Technology Standards.

Policy Management Authority (PMA)

The responsibilities of the PMA include:

• recommending public facing Identity, Authentication and Authorization policies, standards and guidelines to the Minister; and
• reviewing and approving public-facing IAA services in accordance with OPS policy.

Internal Audit Division

The responsibilities of Ontario Internal Audit Division include:

• conducting periodic assurance and consulting engagements of pertinent activities to assess compliance with this Directive and associated policies and standards;
• communicating with appropriate management about the risks identified and the severity of those risks; and
• working with management to identify the needed management action plans to mitigate the risks noted during the course of an audit, and conducting follow-up as required.
**Program Managers**

The responsibilities of program managers include:

- ensuring their staff comply with this Directive and all policies made under this Directive; and
- managing their program resources and budgets.

**All OPS and Applicable Agency Staff**

The responsibilities of all OPS and applicable agency staff include:

- acting in accordance with this Directive, as well as policies and standards made pursuant to the Directive.
APPENDIX A: DEFINITIONS

In this Directive:

“agencies” means classified agencies (including boards or commissions) as defined in the Agency Establishment and Accountability Directive;

“applicable agencies” means all agencies required to comply with this Directive in whole or in part by their Memoranda of Understanding;

“application” means automated processes that are designed and created to meet business needs;

“Business Architecture” is a business-driven disciplined process that decomposes the businesses goals and strategies, the assets and the processes needed to execute them as well as their impact on business goals;

“CCIO” means the OPS Corporate Chief Information Officer;

“CIO” means OPS cluster Chief Information Officers;

“clusters” means the OPS Chief Information Officers and their staff;

“Directive” means this Management and Use of Information and Information Technology (I&IT) Directive;

“Enterprise Architecture” means the discipline of planning, designing, building and maintaining a set of models that represent the enterprise. It illustrates the manner in which the operations, systems and technology components of a business are, or will be, organized;

“I&IT Assets” mean information assets, infrastructure assets and business application assets;

“I&IT Organization” means the Office of the Corporate Chief Information Officer and all I&IT clusters;

“I&IT Project” means a project as defined by the OPS Integrated Project Management Framework and Methodology and relating to I&IT;

“I&IT Services” means services provided to one or more customers, by the I&IT Organization. An IT Service is based on the use of information technology and supports the customer’s business process. An IT Service is made up from a combination of people, processes and technology and should be defined in a service catalogue.

“IAA” means Identification, Authentication and Authorization where:

Identification means creating and issuing a persistent verified electronic identifier (based on assessment of evidence that has been presented to support the claimed identification) and – on first time access – mapping the electronic identifier to the program enrolment;

Authentication means establishing at the start of each online session the validity of that electronic identification, as appropriate, based on assurance level; and
Authorization means granting or denying access to online information or services based on the transaction or program specific business rules of the online service.

“information” means information in any form, in any medium and at all stages of its lifecycle, including information created, recorded, transmitted or stored in digital form or in other intangible form by electronic, magnetic, optical or any other means, but does not include a mechanism or system for creating, sending, receiving, storing or otherwise processing information;

“information management” means applying common management principles (planning, directing, controlling, evaluating) to information assets. It involves establishing disciplined and consistent practices related to the planning, creation, capture or collection, organization, use, accessibility, dissemination, storage, protection and disposition of information assets;

“information technology” means the equipment, software, services and processes used to create, store, process, communicate and manage information, including process control technology;

“infrastructure” means the physical hardware and software that supports the flow and processing of information, including networks, platforms, wireless devices, access points, mobile devices, photocopiers, printers, mainframe and personal computing devices, servers and data repositories, operating systems and related software and telecommunications infrastructure equipment and hardware;

“machine-readable data” means data that can be processed by computers without users manually entering it. Most commonly-used database files can be easily converted to this format;

“major I&IT projects” means I&IT projects with a projected expenditure of $20M or more;

“MBC” means Management Board of Cabinet;

“Minister” means the Minister of Government Services;

“ministry” means a ministry of the Ontario Government;

“non-public information” means government information that is subject to valid privacy, security or privilege limitations or has otherwise not been made public;

“OPS” means the Ontario Public Service ministries;

“public information” means government information that is not subject to valid privacy, security or privilege limitations.

“security testing and evaluation” means any assessment required to evaluate I&IT security, including but not limited to Threat/Risk Assessment, vulnerability assessment, penetration test, and security review, including compliance assessments; and

“service management” means the discipline for managing information technology (IT) with a focus on the customer’s perspective of the quality of the IT Services, and their effectiveness in supporting business outcomes and strategies.