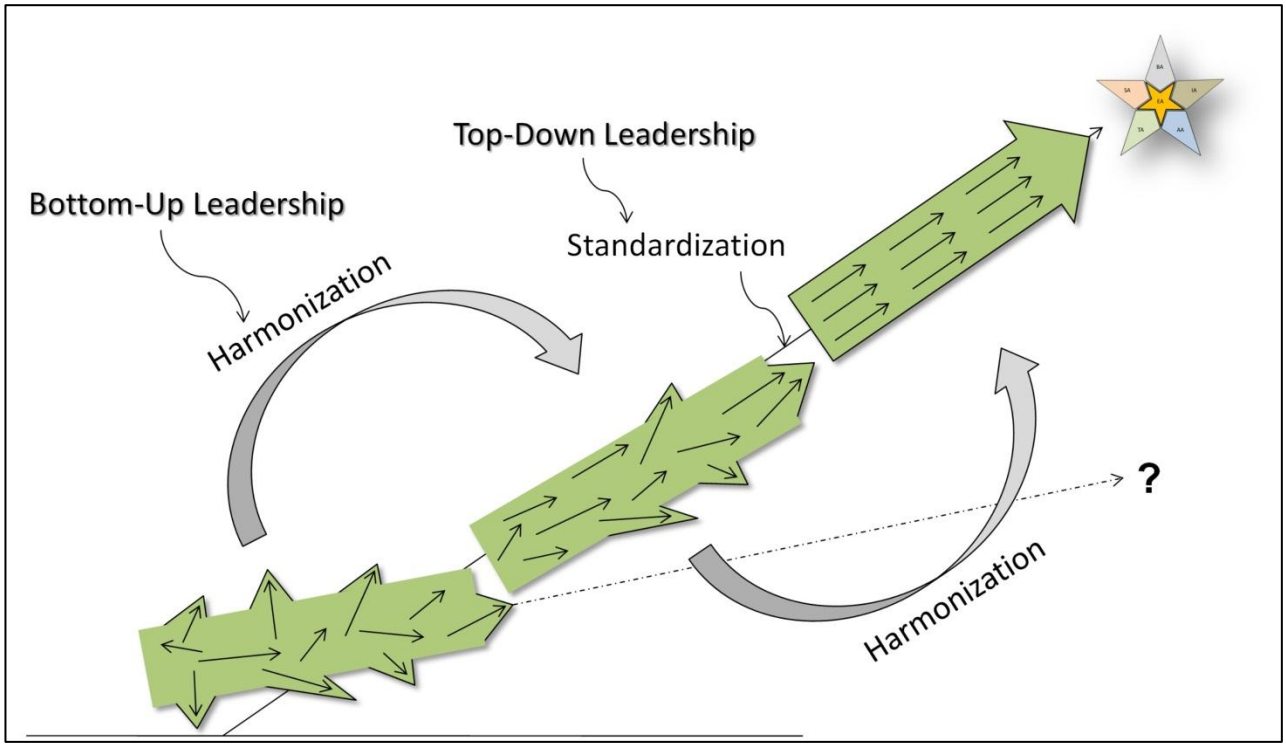
Government of New Brunswick
Enterprise Architecture Program

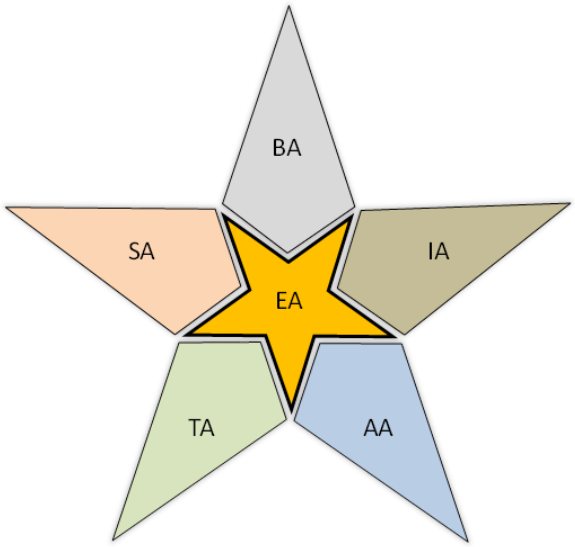
Leading the journey to excellence



Executive Council Office (ECO)
Office of the Chief Information Officer (OCIO)

September 2013

Government of New Brunswick
Enterprise Architecture Program



Government of New Brunswick
Enterprise Architecture Program

Published by:
Province of New Brunswick
P.O. Box 6000
Fredericton, NB E3B 5H1
CANADA

ISBN 978-1-4605-0311-9

Contents

Message from the Chief Information Officer for the Government of New Brunswick

Change is good – but not always easy! In a very short timeframe the Government of New Brunswick established the Office of the Chief Information Officer, within the Executive Council Office, and gave it a mandate that would enable new levels of efficiencies and change management across all of its organizations – a first!

We have been fortunate that the professionals we needed to work with were already aware of the need to change, and that they embraced the catalytic role of the OCIO to enable it. In order to succeed, the adoption of a common language, even a foreign one, was required in order to jointly define what our future would look like. We adopted TOGAF® as the framework to guide our efforts, and this manual is the result of many long hours of research and development by a core team in consultation with many stakeholders.

The manual contains the charter for our Enterprise Architecture Program as well as the *What*, *How,* and *Who* answers we all seek when we need to move into a new direction. Such an undertaking can never be "right" and it will need to be improved continuously. We live in a very dynamic and complex environment that evolves faster than we can design and agree on it. This manual describes the *Direction* that we understand needs to be taken and *What* we need to do in order to get there effectively. It is a systematic approach and a systemic approach that will reconcile many different viewpoints so that we can harmonize and rationalize.

We have already lived many of the positive effects from this change initiative, and many more will come by staying the course. The new bodies we have formed, such as the Architecture Review Board, are poised to lead the enterprise toward results that were unachievable months ago but are now within reach. There is something powerful happening when so many great minds come together from so many different domains of our society to architect its future.

Besides thanking the Chief Technology Officers, Vice-Presidents, Chief Information Officers and Senior IT Leaders in all of the GNB public bodies, I must thank the Enterprise Architecture Program Office staff for their leadership in shaping and implementing this Program and in particular Navid Kheradmand, our Project Lead, who rose to the challenge and kept us on track through a program development journey that lasted a year and half, which included the development of this manual. The Office of the CIO is now prepared for the ongoing operations of this program so that we can reap the full benefits.

If you are reading this, you are a stakeholder of this program and we acknowledge your interest in helping us make the most of it – thank you!

Christian Couturier
Government Chief Information Officer

Executive Summary

The mandate of the Executive Council Office - Office of the Chief Information Officer (ECO-OCIO) is to lead, enable, and assure the effective and efficient use of Information Management & Information and Communications Technology (IM&ICT) investments across all four parts (Part I – Core Government; Part II – Education; Part III – Health; and Part IV – Crown Corporations and others) of the Government of New Brunswick (GNB). The GNB Enterprise Architecture (EA) Program spans all government IM&ICT investments and is the cornerstone program of the OCIO.

Enterprise architecture creates the blueprint of the enterprise and provides the roadmap to build such an enterprise. EA is an enabler for business transformation and provides an assurance that the whole enterprise moves efficiently and effectively towards fulfilling its strategies and objectives, and therefore towards its mission and vision. In other words, EA is not only about *doing things right*, but also about *doing the right things*.

EA results in improved management and quality of information, more efficient business and information technology operations, better return on existing investments, reduced risk for future investments, and a faster, simpler, and cheaper procurement process.

EA encompasses five major domains, namely business architecture, information architecture, application architecture, technology architecture, and security architecture. Currently, business architecture at GNB is led by the Office of Strategy Management and Government Renewal Office, while the rest of the architecture domains are led by the OCIO under the GNB EA Program.

The government has articulated its strategies and objectives on the GNB Strategy Map (part of business architecture). On this map, the OCIO is responsible for the *"information readiness"* enabler with an objective to provide *"Access to relevant, timely, and quality information"*. The roadmap to achieve this objective has been defined on the GNB EA Roadmap, which illustrates current and future vision states of the rest of the architecture domains (information, application, technology, and security) with a set of building blocks to achieve these future vision states.

With the aim to achieve *information readiness* and in consideration of the GNB's strategies (stronger economy, enhanced quality of life, and living with our means), the EA Roadmap defines the ultimate future vision of the EA Program as: *"High value personalized services provided to citizens and other stakeholders anytime, anywhere, and via any device in a seamless, integrated, and cost effective manner."*

The program enables and promotes standardization and harmonization of IM&ICT investments across government and ensures a better alignment of these investments with government business strategies and objectives. By doing so, the program ensures that the government is enabled to deliver on its IM&ICT related strategies, objectives, measures, initiatives, and action plans.

The GNB Enterprise Architecture Program Manual (this document) provides a formal description of the scope, governance structure, and planning framework of the program. This manual is the single authoritative source of information on the structure and components of the GNB EA Program.

The Open Group Architecture Framework (TOGAF®)

The OCIO has adopted The Open Group Architecture Framework (TOGAF®) as the standard for the GNB EA practice and as a guiding methodology to manage and run the GNB EA Program. A Non-Commercial Corporate Licence Agreement for TOGAF® Version 9.1 has been signed between the Government Chief Information Officer (GCIO) and The Open Group's Chief Operating Officer. The use of TOGAF® 9.1 materials throughout this document is permitted under this agreement. A copy of this agreement is provided at the end of this document.

1. Introduction

1.1. Defining Enterprise

The Open Group Architecture Framework (TOGAF®) Version 9.1 defines "enterprise" as any collection of organizations that has a common set of goals. For example, an enterprise could be a government agency, a whole corporation, a division of a corporation, a single department, or a chain of geographically distant organizations linked together by common ownership.

The term "enterprise" in the context of "enterprise architecture" can be used to denote both an entire enterprise - encompassing all of its information and technology services, processes, and infrastructure - and a specific domain within the enterprise. In both cases, the architecture crosses multiple systems, and multiple functional groups within the enterprise.

Confusion often arises from the evolving nature of the term "enterprise". An extended enterprise nowadays frequently includes partners, suppliers, and customers. If the goal is to integrate an extended enterprise, then the enterprise comprises the partners, suppliers, and customers, as well as internal business units.[1]

For the purposes of our program, the term "enterprise" shall mean the collection of GNB public bodies as a whole unless otherwise specified.

1.2. Defining Enterprise Architecture (EA)

There are numerous definitions of EA, all with slightly different nuances, but all describing a close and symbiotic relationship between business strategy and technology investment.

Gartner defines EA as “the process of translating business vision and strategy into effective enterprise change by creating, communicating, and improving the key principles and models that describe the enterprise’s future state and enable its evolution. The scope of the enterprise architecture includes the people, processes, information and technology of the enterprise, and their relationships to one another and to the external environment. Enterprise architects compose holistic solutions that address the business challenges of the enterprise, and support the governance needed to implement them.”

1.3. Purpose of an EA

Any structure, based on its purpose, requires a well architected blueprint that defines and describes the materials for the structure, the way to build the structure, and the ultimate shape of it. Similarly, any organization, as a structure, requires a blueprint that describes the components of the organization, their relationships, and the way to achieve the mission and vision of the organization. Building or managing an organization without architecture resembles building a structure without a blueprint.

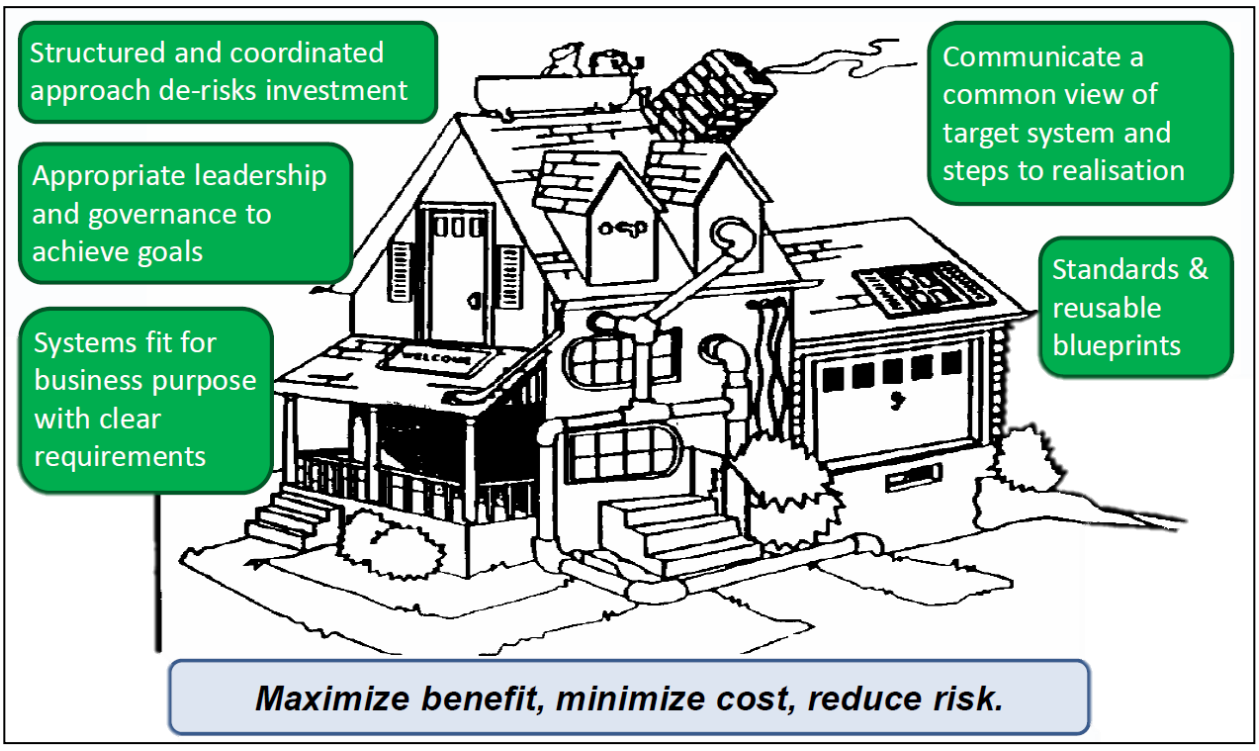
[1] TOGAF® 9.1 Online Guide, http://pubs.opengroup.org/architecture/togaf9-doc/arch/, Section 1.2

Enterprise architecture creates the blueprint of the enterprise and provides the roadmap to build such an enterprise. EA is an enabler for business transformation and provides an assurance that the whole enterprise moves efficiently and effectively towards fulfilling its strategies and objectives, and therefore towards its mission and vision. In other words, EA is not only about *doing things right*, but also about *doing the right things*.

EA defines the future state business processes, information, technologies, and organization in a coordinated fashion to deliver more effective and efficient services to the public. Therefore, EA is responsible for providing strategies, standards, best practices, guidelines, and recommendations for all the components of an enterprise that play a role in or have an impact on achieving enterprise goals and objectives.

According to TOGAF®, "the purpose of enterprise architecture is to optimize across the enterprise the often fragmented legacy of processes (both manual and automated) into an integrated environment that is responsive to change and supportive of the delivery of the business strategy."[2]

The following graphic depicts well the purpose of an EA:



Source: ATE06 – Stakeholder Commitment and Management, Architecting-the-Enterprise Limited Copyright © 2012

[2] Ibid

1.4. Benefits of an EA

EA brings a lot of benefits to organizations. With respect to Information Management (IM), EA plays a leadership role in transforming and improving the management of information by providing and managing a plan for improved information governance. The goals and benefits of such a plan for GNB is to:

- Get value from its information and provide analytics-driven information;
- Provide a horizontal and/or enterprise view of its information;
- Get a holistic view of clients (by major programs), suppliers and/or employees;
- Improve the response to Requests for Information;
- Improve stewardship of the government's information assets;
- Standardize government data to enable sharing and reuse, and to reduce duplication;
- Improve the efficiency of business processes by better managing the information within;
- Improve service delivery;
- Improve the compliance to legislation and policies;
- Improve data quality across the enterprise;
- Improve efficiency and cost-effectiveness in organization information and data management;
- Establish clear decision making rules and processes for shared data;
- Improve access to information across the enterprise; and
- Enables quality information for Enterprise eServices and eGovernment.

With respect to Information and Communications Technology (ICT), EA results in:

– "A more efficient business operation:
  - Lower business operation costs
  - More agile organization
  - Business capabilities shared across the organization
  - Lower change management costs
  - More flexible workforce
  - Improved business productivity

– A more efficient IT operation:
  - Lower software development, support, and maintenance costs
  - Increased portability of applications
  - Improved interoperability and easier system and network management
  - Improved ability to address critical enterprise-wide issues like security
  - Easier upgrade and exchange of system components

– Better return on existing investment, reduced risk for future investment:
  - Reduced complexity in the business and IT
  - Maximum return on investment in existing business and IT infrastructure
  - The flexibility to make, buy, or out-source business and IT solutions
  - Reduced risk overall in new investments and their cost of ownership

- Faster, simpler, and cheaper procurement:
  - Buying decisions are simpler, because the information governing procurement is readily available in a coherent plan
  - The procurement process is faster - maximizing procurement speed and flexibility without sacrificing architectural coherence
  - The ability to procure heterogeneous, multi-vendor open systems
  - The ability to secure more economic capabilities"[3]

1.5. What is an architecture framework & why TOGAF®

TOGAF® defines architecture framework as "a foundational structure, or set of structures, which can be used for developing a broad range of different architectures. It should describe a method for designing a target state of the enterprise in terms of a set of building blocks, and for showing how the building blocks fit together. It should contain a set of tools and provide a common vocabulary. It should also include a list of recommended standards and compliant products that can be used to implement the building blocks."

"TOGAF has been developed through the collaborative efforts of over 300 Architecture Forum member companies from some of the world's leading companies and organizations. Using TOGAF results in enterprise architecture that is consistent, reflects the needs of stakeholders, employs best practice, and gives due consideration both to current requirements and the perceived future needs of the business.

Developing and sustaining an enterprise architecture is a technically complex process which involves many stakeholders and decision processes in the organization. TOGAF plays an important role in standardizing and de-risks the architecture development process. TOGAF provides a best practice framework for adding value, and enables the organization to build workable and economic solutions which address their business issues and needs."[4]

1.6. What is an EA Program

An EA Program formally establishes:

- governance and planning frameworks with a set of principles for the practice of EA throughout GNB;
- processes and structure for the development and management of EA deliverables;
- measures to gauge progress made and the effectiveness of the results of adopting EA practices; and
- training and development opportunities for the EA stakeholders in the government.

[3] Ibid
[4] Ibid

1.7. Purpose of an EA Program

An EA program facilitates the alignment between the business strategy and related architecture elements by ensuring that the information management and technological responses are well defined and meet the needs of the business. As a program, EA allows for a balanced and consistent top-down planning in architectural projects.

EA as a function empowers GNB to leverage its business, information, and technology to enable the modernization of public services, support innovation, and generally reduce service delivery costs.

1.8. Benefits of an EA Program

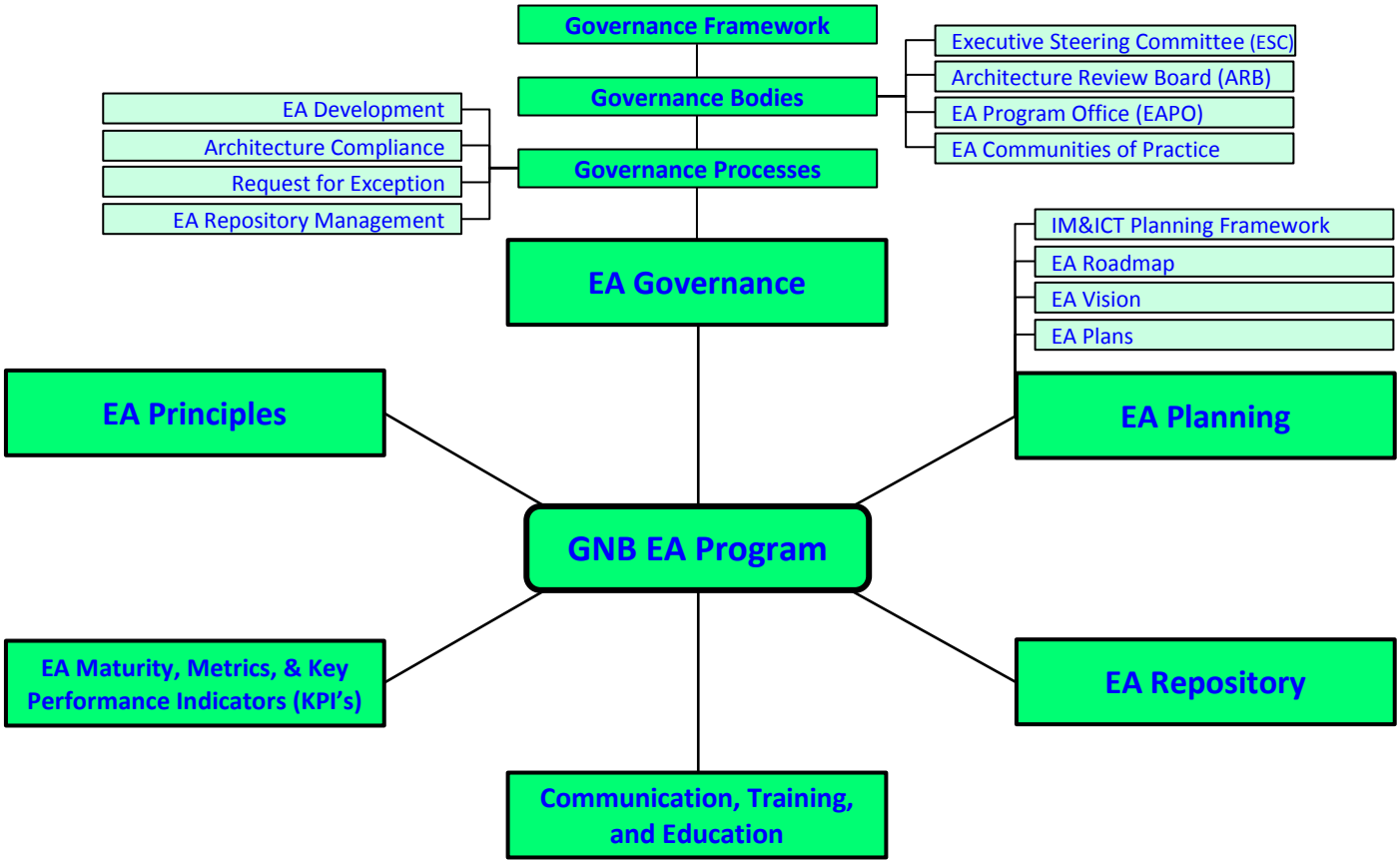
An EA Program is perpetual, and promotes:

- Effective delivery of change - within an EA Program, changes are planned and implemented in an integrated manner that ensures current business operations are not adversely affected;
- Alignment of enterprise projects to business strategies - EA provides response to business and technology strategic initiatives by utilizing effective analysis of gaps identified in the architecture;
- Reduction of risk - EA includes the identification of standards, processes and governance that, when followed, will reduce certain risk issues;
- Coordination and control - Having a formal EA Program with defined management and governance exercises control over a complex range of business and technical activities; and
- Compliance - utilizing policies and standards to guide the EA program will ensure consistency.

1.9. GNB EA Program Manual

The GNB EA Program Manual (this document) provides a formal description of the scope, governance structure, and planning framework of the EA Program. This manual is the single authoritative source of information on the structure and components of the GNB EA Program.

The rest of this document is dedicated to describing the GNB EA Program and its components in detail. First the scope of the program is clarified and then the governance structure, including the EA governance framework, major governance bodies, and governance processes are introduced, followed by the EA Principles. Then, the IM&ICT Planning Framework and its major building blocks, namely EA Roadmap, EA Vision, and EA Plans are presented. Next, the EA Repository is presented, then communications, training, and education for the EA Program is discussed and finally there is a discussion on the EA maturity, metrics, and key performance indicators (KPI's). The diagram below shows the components of the program.

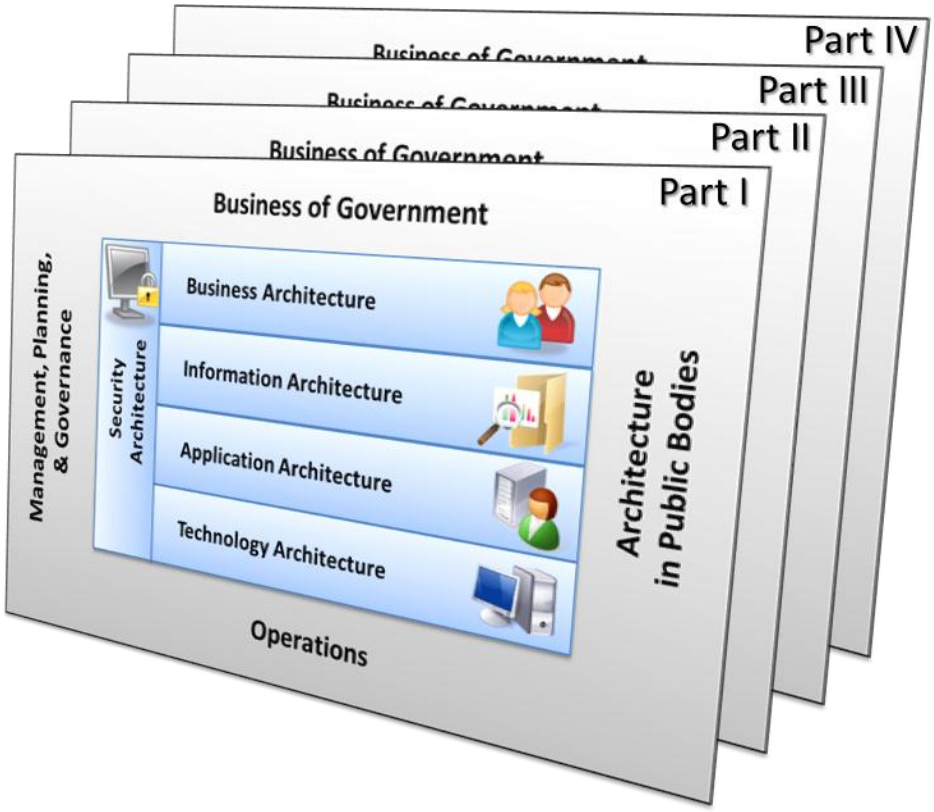


GNB EA Program Components

2. GNB EA Program

The GNB EA Program spans all four parts of the government and is one of the cornerstones of the OCIO meeting its mandate from the government.

The EA Program encompasses the five major architecture domains, namely business, information, application, technology, and security architectures. As the diagram below illustrates, security architecture spans the other four domains.



GNB EA Program Scope

Short descriptions of these domains are provided below. Please refer to Appendix A for further details on enterprise architecture domains.

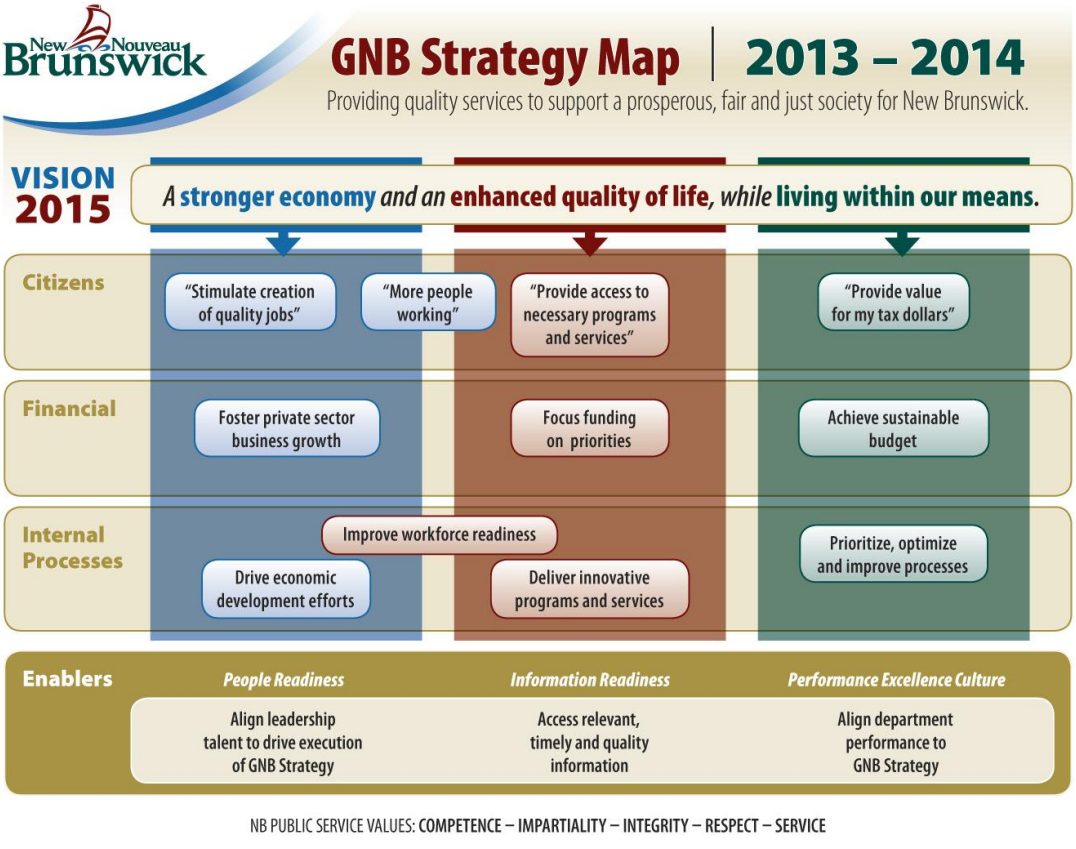
Business Architecture (BA) "describes the business strategy, models, processes, services and organizations. It provides the foundation upon which the other EA domains base their decisions."[5]

[5] Infosys, "A Governance Framework", 2005

Currently, Business Architecture at GNB is led by the Executive Council Office - Office of Strategy Management (OSM) and Executive Council Office - Government Renewal Office (GRO). The major building blocks of the government's business architecture are:

- GNB's Directory of Services (maintained by the OCIO);
- Government Directory (maintained by Service New Brunswick, SNB);
- GNB's Performance Excellence Process, including the Strategy Map, Balance Scorecard, and Lean Six Sigma Process Improvements (led by the OSM);
- Several strategies by various public bodies. Examples are "Growing Together" economic growth strategies, the Economic Development Action Plan and Strategic Framework to Support Priority Growth Sectors in New Brunswick (led by the Department of Economic Development), and The New Brunswick Energy Blueprint (led by the Department of Energy and Mines); and
- SOMIA's (Strategies, Objectives, Measures, Initiatives, and Actions) and Government Renewal Plan (both managed by the GRO).

The figure below is the GNB Strategy Map, which defines three major strategies, namely *stronger economy*, *enhanced quality of life*, and *living within our means*, and a set of objectives for each of these strategies relevant to citizens, financial, and internal processes. The Strategy Map also identifies a set of enablers and objectives that support the fulfillment of these strategies and objectives of which is the *information readiness* enabler.



GNB Strategy Map, 2013 – 2014

The OCIO is responsible for "*Information Readiness*" to enable *access to relevant, timely, and quality information*.

Below are the descriptions of the rest of the architecture domains, which are led by the OCIO under the GNB EA Program.

Information Architecture (IA) "identifies, documents, and manages the information needs of the enterprise, assigns ownership and accountability for this information, and describes how data is stored by and exchanged between stakeholders."[6]

Application Architecture (AA) "defines the specification of technology enabled solutions in support of the Business Architecture. Provides a view of how services should be bundled to support a business process."[7]

Technology Architecture (TA) "defines the strategies and standards for technologies and methods used to develop, execute, and operate the AA. It provides frameworks, technical patterns, and services that support application requirements."[8]

Security Architecture (SA) describes the organization's existing and planned controls that ensure that information is available and can continue to be used for the purposes it is collected for while maintaining its confidentiality, and integrity.[9]

GNB EA Roadmap and Vision define the major building blocks for the rest of the architecture domains (information, application, technology, and security architectures). The EA Roadmap is sometimes referred to as: the GNB IT Plan. Please refer to Appendix E for the details on these building blocks.

[6] Ibid
[7] Ibid
[8] Ibid
[9] National Institutes of Health enterprise architecture, http://enterprisearchitecture.nih.gov/

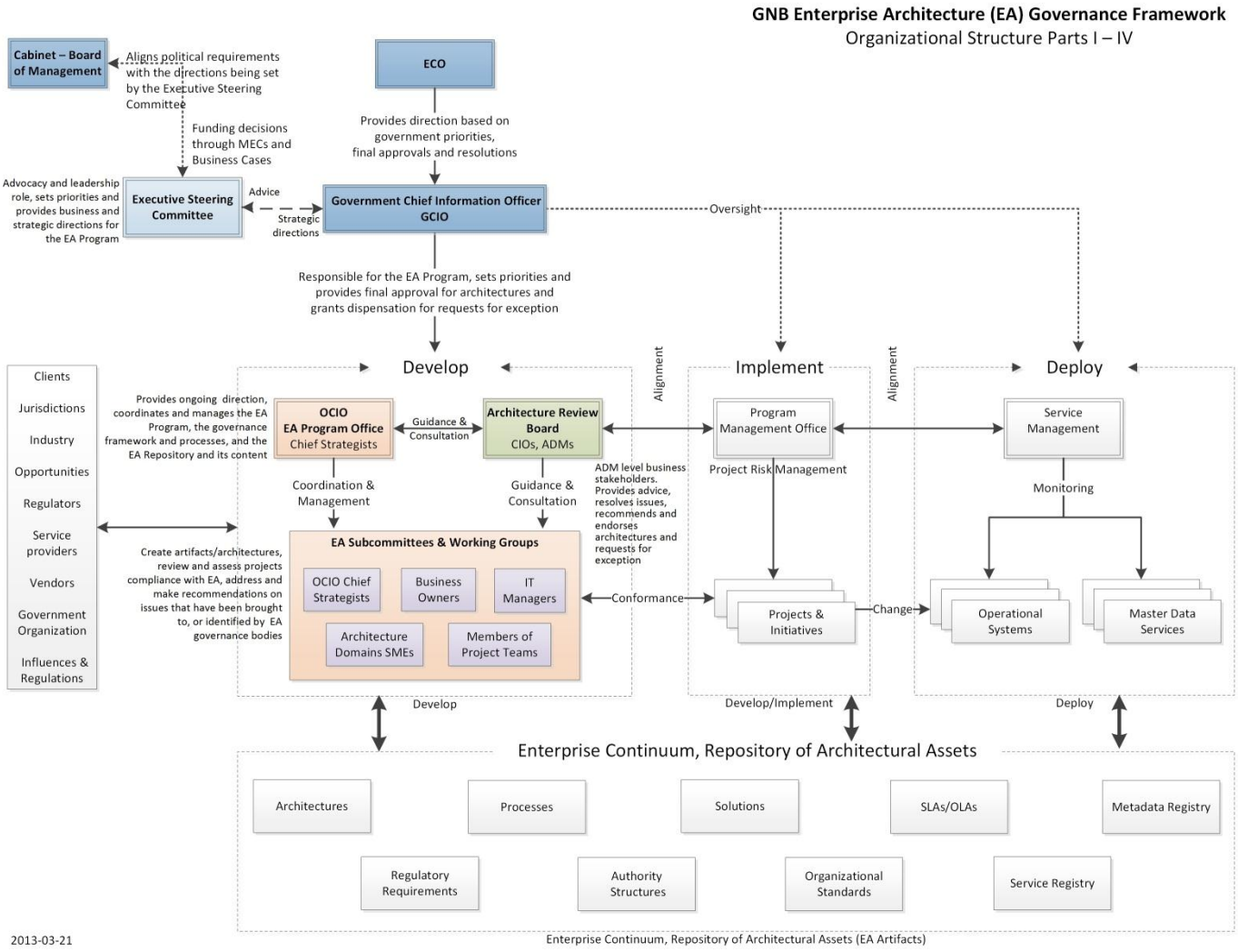
3. EA Governance

3.1. EA Governance Framework

According to TOGAF®, conceptually, “architecture governance is an approach, a series of processes, a cultural orientation, and set of owned responsibilities that ensure the integrity and effectiveness of the organization's architectures.”[10] Please refer to TOGAF® 9.1 Online Guide, Figure 50.1 for a conceptual structure of an architecture governance framework.

TOGAF® suggests an organizational structure for EA governance. This structure has been adopted and adapted to the GNB environment and the new mandate of the Office of the CIO. This organizational structure is illustrated in the figure below. In the following sections, each of the three major governance bodies, namely the Executive Steering Committee (ESC), the Architecture Review Board (ARB), and the EA Program Office (EAPO), are briefly described. Please refer to Appendix B for the Terms of References of these bodies.

[10] TOGAF® 9.1 Online Guide, http://pubs.opengroup.org/architecture/togaf9-doc/arch/, Section 50.2



GNB EA Governance Framework

3.1.1. Executive Steering Committee (ESC)

The Executive Steering Committee (ESC) provides the governance that is essential to make "Enterprise" Architecture work for GNB (including Parts I, II, III, and IV). The focus of the ESC is on the holistic aspects of Information Management (IM) and Information and Communications Technology (ICT), including understanding and directing the linkage among GNB strategy, business transformations, information governance transformations, and technology directions and investments at the enterprise-wide level.

In an advocacy and leadership capacity, ESC members:

- Enhance and endorse the GNB Enterprise Architecture (EA) Roadmap;
- Influence all GNB IM & ICT stakeholders to align to and buy into the EA Roadmap;

- Support the GCIO in engaging stakeholders towards delivering the EA Roadmap;
- Ensure the alignment of GNB strategy and business transformation with IM & ICT priorities;
- Recognize and promote the value of EA and its accomplishments;
- Foster understanding of GNB business drivers, direction, strategy, trends and how they impact the future of GNB;
- Provide strategic direction for EA;
- Provide sponsorship and support cross-GNB commitment to EA;
- Ensure that GNB EA is part of strategic decision-making processes;
- Promote the use of Business Capability Modeling (a top-down planning technique that focuses on business outcomes) for effective IM & ICT planning.
- Provide insight into how to identify and address foreseeable areas of conflict;
- Provide insight into the EA long-term vision and the requirements and constraints of the environment under which public bodies operate;
- Promote an enterprise wide IM & ICT planning framework;
- Where appropriate, support funding requests through Memorandums to the Executive Council (MEC) presented to the Board of Management (BoM).

3.1.2. Architecture Review Board (ARB)

The Architecture Review Board (ARB) ensures consistency and completeness of the holistic GNB Enterprise Architecture (EA), evaluates compliance, assesses the impacts of the "next big project" of the "Enterprise" Architecture, and promotes EA within the public bodies.

The ARB:

- Reviews and recommends, architectures (EA Development Process);
- Evaluates compliance to recommend to GCIO (Compliance Assessment Process);
- Evaluates Requests for Exception to recommend to GCIO (Dispensation Process); and
- Provides guidance to EA sub-committees and working groups.

3.1.3. EA Program Office (EAPO)

Enterprise Architecture Program Office (EAPO) is located within the Office of the Chief Information Officer (OCIO) of the Executive Council Office. It is a permanent Enterprise Architecture (EA) Program management office whose purpose is to cultivate EA throughout GNB. One of the primary responsibilities of the office is to promote and support the Government of New Brunswick (GNB) through the application of EA.

The EAPO coordinates and manages the EA Program, EA Communities of Practice, the governance framework and processes, and the EA Repository and its content. It is responsible to ensure that EA projects are carried out consistently and successfully in compliance with GNB recommended methods, standards, and strategies.

The EAPO provides:

- A central repository for architecture standards, methods, processes and policies;
- The authority to enforce architecture governance; and

- A forum to cultivate EA throughout the organization.

3.1.4. EA Communities of Practice

EA Communities of Practice ensure the proper development and evolution of the architectural domains, namely information, application, technology, and security. These communities provide horizontal alignment, collaboration, and engagement of subject matter experts in the architectural domains throughout the government.

The communities:

- Collaborate in preparing next iterations of the GNB EA Roadmap;
- Influence the practice of EA by participating in the development of EA plans to align with the EA Roadmap;
- Participate in the EA strategic initiatives and action plans for each domain;
- Influence the development of public bodies' EA roadmaps and operational plans;
- Encourage the alignment of public bodies operational plans with the EA plans;
- Review domain architectures and enterprise directives, as needed;
- Promote active participation in the domain sub-committees and working groups;
- Raise awareness of EA successes in each domain;
- Support proper domains maturity and capabilities.

3.2. EA Governance Processes

In order to successfully implement the EA governance framework, there are key governance processes in the EA Program which define the relationships among governance bodies and their decision making approaches. Governance processes are in place to make sure that the EA Program efficiently and effectively fulfills its vision and delivers value to its stakeholders through formal, clear, and well-defined procedures.

According to TOGAF®, "Governance processes are required to identify, manage, audit, and disseminate all information related to architecture management, contracts, and implementation. These governance processes will be used to ensure that all architecture artifacts and contracts, principles, and operational-level agreements are monitored on an ongoing basis with clear auditability of all decisions made."

The following sections provide a brief description of the governance processes. Please refer to the Appendix C for the detail description of these processes.

3.2.1. EA Development

EA development process includes adoption, development, amendment, and approval of EA capabilities and assets including artifacts, standards, guidelines, best practices, policies, etc.

3.2.2. *Architecture Compliance*

Ensuring the compliance of individual EA initiatives and assets with the approved enterprise architectures is an essential aspect of architecture governance. An Architecture Compliance review is a scrutiny of the compliance of a specific initiative or asset against established architectural criteria and objectives.

3.2.3. *Request for Exception (Dispensation)*

There are cases in which an EA initiative or a subject area (design, operational, service level, or technology) does not comply with approved enterprise architectures. These non-compliance cases are either known at the initiation stage or are revealed through Architecture Compliance reviews.

In these cases, the non-compliant subject area can be adjusted or realigned in order to meet the compliance requirements. However, if the subject area, despite best efforts utilized, cannot comply with approved architectures and/or needs more time to come into compliance, dispensation can be requested for the subject area following the Dispensation process.

3.2.4. *EA Repository Management*

The EA Repository Management comprises of a set of workflows to manage the EA repository, its content, and its collaboration environments (the activities in green).

3.2.5. *Processes External to EA Program*

The EA Assurance and Strategic Sourcing processes are external to the EA Program; however, they have touch points with the EA processes and therefore their existence and impact need to be recognized in the EA context.

4. EA Principles

According to TOGAF®, principles are “general rules and guidelines, intended to be enduring and seldom amended, that inform and support the way in which an organization sets about fulfilling its mission. In their turn, principles may be just one element in a structured set of ideas that collectively define and guide the organization, from values through to actions and results.”[11]

A set of Enterprise Architecture (EA) Guiding Principles has been introduced as part of the new responsibilities for the Office of the Chief Information Officer (OCIO). These guiding principles are as follows:

- **Simple, fast, stable and fair (systematic and system-wide)**
- **Common language, architecture, standards and shared enterprise-wide services**
- **Develop solutions for agility and information reuse**

In line with these guiding principles and the quality attributes described in Appendix D, a set of working principles applicable to Information, Application, Technology, and Security Architecture domains have been established.

The main purpose of these principles is to provide direction for the goals and objectives of the GNB EA Program in providing high value personalized services to citizens and other stakeholders anytime, anywhere, and via any device in a seamless, integrated, and cost effective manner. This is achieved through enabling information readiness by delivering relevant, timely, and quality information.

These EA principles are mainly adopted and adapted from industry best practices and recommendations. The structure of these principles is based on the widely adopted template for the presentation of principles. Below is the list of principles. Please refer to Appendix D for the details on each of these principles.

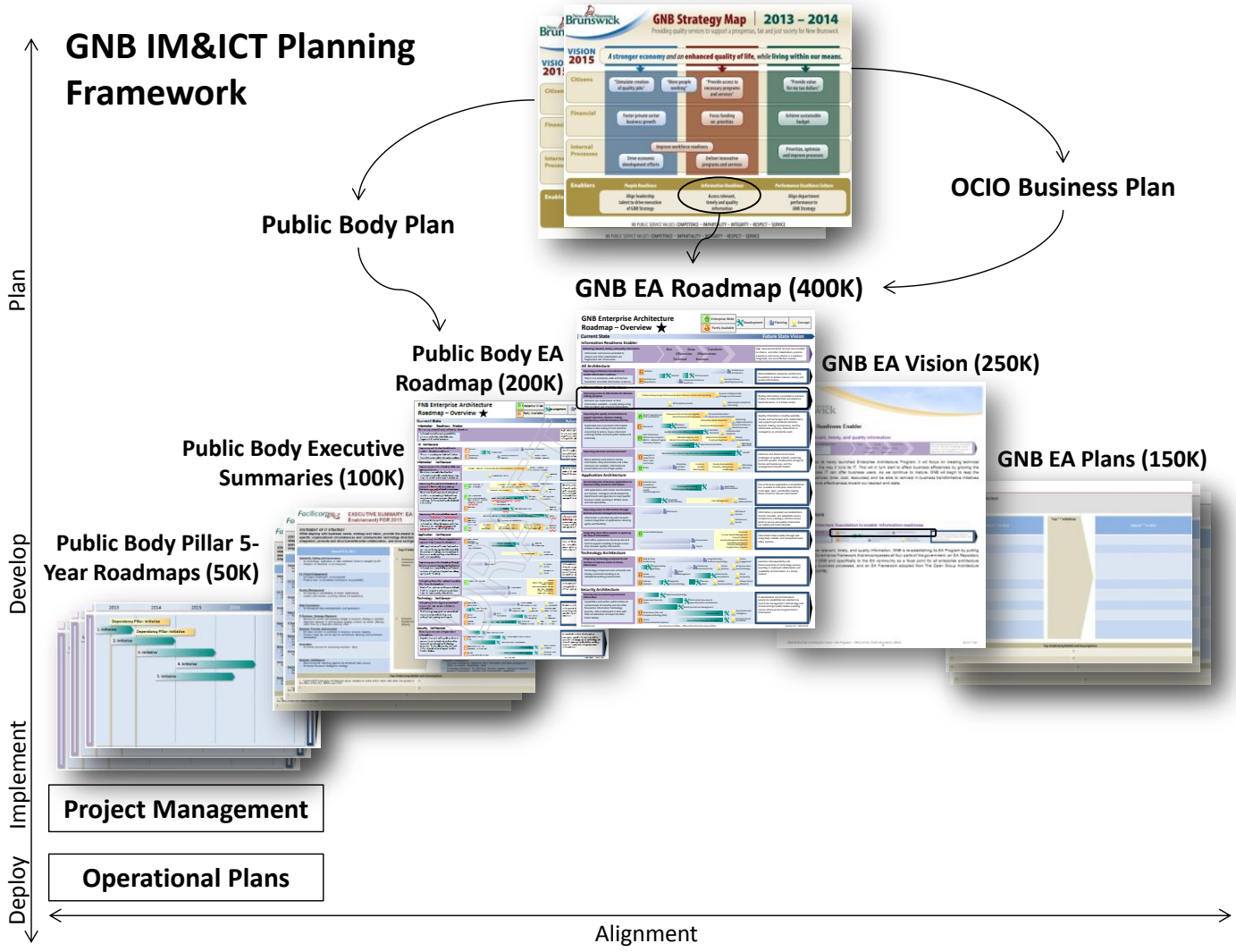
- Application of Principles
- Enabling Business and Information Readiness
- Compliance
- Standardization, Harmonization, and Normalization
- Sharing and Integrating EA Artifacts
- Interoperability
- Information Quality is Everybody's Business
- Information is a Valuable Enterprise Asset
- Discoverability and Accessibility of Information
- Service Orientation
- Robust, Reliable, Accepted, Supported, and Sustainable Technology
- Risk-based Mitigation

These principles will regularly be reviewed by EAPO and ARB to ensure their relevance and consistency.

[11] TOGAF® 9.1 Online Guide, http://pubs.opengroup.org/architecture/togaf9-doc/arch/, Section 23.1

5. EA Planning

The diagram below illustrates the GNB IM&ICT Planning Framework and its components, mainly GNB EA Roadmap, EA Vision, and EA Plans. The major deliverable of this planning framework is the EA Roadmap, which is derived from GNB Strategy Map (business architecture) and presents the building blocks for the rest of the architectural domains (information, application, technology, and security).



GNB IM&ICT Planning Framework

5.1. EA Roadmap

EA Roadmap acts as a harmonization means describing the current environment and the future vision state of EA and identifies a set of building blocks to achieve the future state. The Roadmap pinpoints the priorities and areas of improvements in different domains of architectures.

As mentioned before, the OCIO is responsible to enable *"Access to relevant, timely, and quality information"*. With the aim to fulfill this objective and consideration of the GNB's strategies (stronger economy, enhanced quality of life, and living with our means), EA Roadmap defines the ultimate future vision of the EA Program as *"High value personalized services are provided to citizens and other stakeholders anytime, anywhere, and via any device in a seamless, integrated, and cost effective manner."*

EA Roadmap is endorsed by the Executive Steering Committee and is reviewed annually. The current version of the EA Roadmap is presented in the next page.

5.2. EA Vision

EA Vision describes in details the building blocks identified in the EA Roadmap, the rationale for these building blocks considered to be on the Roadmap, and the current and future vision of them. A complete version of the Vision document is provided in Appendix E.

5.3. EA Plans

EA plans describe more detailed planning for each track of the Roadmap (comprised of a building block or a set of building blocks) in a form of current and future state in a specific timeframes and the top initiatives during the set timeframes.

GNB Enterprise Architecture Roadmap – Overview ★

Enterprise Wide | Partly Available | Development | Planning | Concept

Current State → Future State Vision

Information Readiness Enabler

Delivering relevant, timely, and quality information

Information and services provided to citizens and other stakeholders are fragmented and of low value.

Run → Grow → Transform
Efficiencies → Effectiveness
Technical → Business

High value personalized services are provided to citizens and other stakeholders anytime, anywhere, and via any device in a seamless, integrated, and cost effective manner.

All Architecture

Improving architecture foundation to enable information readiness

There is no enterprise-wide architecture foundation to enable information readiness.

Artifacts; SLA/SLO; EA Governance; EA Reference Architecture; Architecture Repositories; Enterprise Architecture Repository; Business Process Modeling Repository

Well established enterprise architecture foundation to deliver relevant, timely, and quality information.

Information Architecture

Improving access to information for decision making purposes

Decisions are made based on best information available , usually taking a long time to collect and interpret information.

Traditional Reporting & Self-Service BI, Best-of-Breed, Analytics & Forecasting; Business Intelligence (BI) Strategy and Framework; BI Competency Centre; Optimizing BI, Analytics & Forecasting

Quality information is provided to decision makers to make informed and evidence-based decisions in a timely matter.

Improving the quality of information to support eServices, decision making, transparency, and information economy.

Duplicated and inconsistent information resides in silos making it hard and time consuming to access, reuse, share and exchange within and with public bodies and externally.

IM & IT Legislation & Policy Framework; Framework (Acts & Policies) Upgrade, New Enterprise IM Program(s); Provincial Information Governance and Framework; Information Waste Reduction; Optimizing Digital Information; Directories; Business Capabilities; Inventories & Assessments; Current Architecture & Maturity Levels; GeoNB, AddressNB, NBRoads, NBWater; Geo Data Standards; Enterprise Data Standards; Land Information Infrastructure Program; NB911 – Address Program; Toponymy Program; Metadata Registry and Master Data Management Hubs; Master Client, Business, Employee Registries; Shared Enterprise Data; Publications, GeoNB; Open Government Data; Optimizing Open Data

Quality information is readily available, shared, and exchanged with stakeholders, and supports personalized eServices, decision making, transparency, and the information economy. Information is managed as an enterprise asset.

Improving eServices and eGovernment

Many websites exist and are mainly informative. Only eCommerce and a few eServices are available. Information & presentation are not of high quality.

One Patient One Record, Drug Information System, Electronic Medical Records; eHealth; www.gnb.ca; www.snb.ca; Part II sites; Part III sites; BizPal; Marketing and Web Functions; Customer Contact Mechanisms; Standardized websites, intranets, LOB systems, mobile apps; Optimizing eServices

eServices and eGovernment meet challenges of quality eHealth, eLearning, economic growth, employment, energy to homes and businesses, and the management of public bodies.

Application Architecture

Harmonizing line of business applications to improve timely access to information

LOB applications with similar functionalities are sourced, managed ,and developed by departments and agencies to meet specific business needs resulting in limited reuse and interoperability.

Social Services; Compliance; Transportation; Health; Land Management; Licensing & Permitting; Tax & Revenue Management; Application Rationalization; Integrated Service Delivery; Case Management; Platform Rationalization

Line of business applications and platforms are reusable at enterprise level and are more agile, open, and flexible making faster access to relevant information.

Improving access to information through business process management and services

Information is provided by point-to-point custom integration of applications reducing agility and flexibility.

SOA Centre; All Channel Services; Software as a Service

Information is provided via standardized, shared, reusable, and adoptable service components, creating a common access point to secure and quality information via mobile and multi-channels.

Integrating back office systems to speed up the flow of information

Back office systems are disconnected and hard to support resulting in longer access time to lower quality information.

Provincial Mail System; Procurement; Payroll; Financials; Human Capital Management; Projects / Grants; Identity Management Services; Help Desk and Support; Facilities Management; Supply Chain / Logistics

Information flows readily through well integrated, reliable, and transparent back office systems.

Technology Architecture

Integrating technology components and services to improve access to timely information

Technology components are untrusted and loosely connected resulting in an suboptimal working environment.

Web & Video Conferencing; Integrated Video Conferencing Strategy; Citizen Engagement; Single Desktop Strategy; Professional Productivity Tools; Virtual Desktop; Bring-Your-Own-Device Strategy; Asset Management; Server Virtualization; Data Centre Consolidation; Cloud Computing; Telecom Contracts; Integrated Telecom Strategy; Service Block; Unified Communications; Citizen Centric Networks

Seamless interoperability and interconnectivity of technology services resulting in improved collaboration and availability of information in a timely manner.

Security Architecture

Ensuring secure access to government information

Capabilities exist within public entities at various levels of maturity and are often focused on Information Technology Security. Risk is addressed in silos with little consideration of impact to other Public Bodies.

Cyber Security Strategy; Government Security Policy; Information Assurance & Operational Security Standards; Identity and Access Management; Governance, Risk, and Compliance Strategy (GRC); Enterprise GRC; Security Business Intelligence; Ad hoc Intrusion Detection Systems; Security Event Management Center; Enterprise Event Correlation

A standardized set of information assurance capabilities are selected via sound risk management methodology and shared amongst public bodies enabling secure, timely access to government information.

Illustrative only

Executive Council Office – Office of the Chief Information Officer

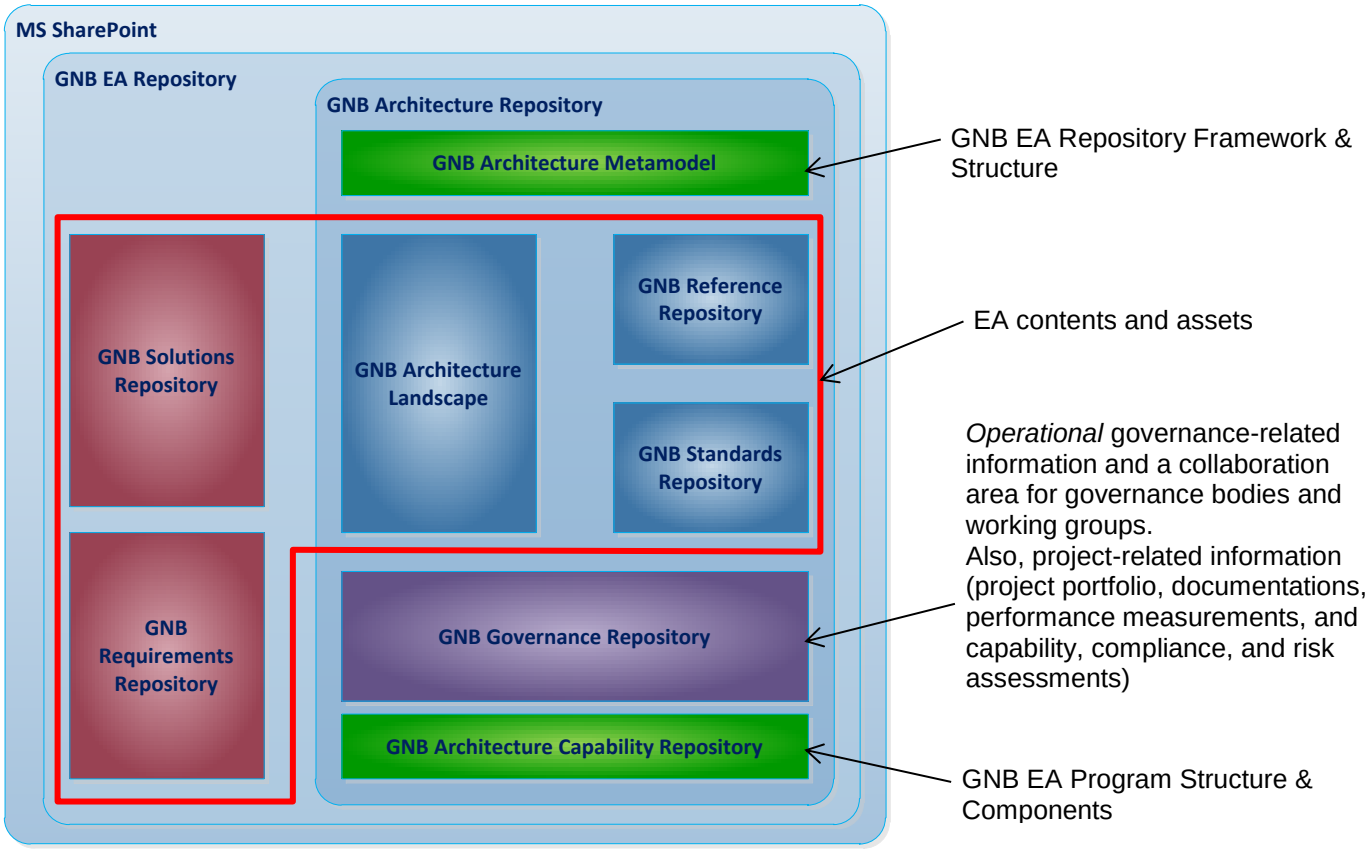
Version 1.0 – 2013-05-22

6. EA Repository

GNB EA Repository is the home for all the EA assets. It has been developed using Microsoft SharePoint, as an interim solution. The EA Repository has been built to follow TOGAF® 9.1 recommendations on structuring an architecture repository.[12] This repository acts as the focal point to collect, review, and publish architectural assets throughout GNB. It also provides collaboration environments for the EA community and governance entities.

According to TOGAF®, "operating a mature Architecture Capability within a large enterprise creates a huge volume of architectural output. Effective management and leverage of these architectural work products require a formal taxonomy for different types of architectural asset alongside dedicated processes and tools for architectural content storage.

TOGAF provides a structural framework for an Architecture Repository that allows an enterprise to distinguish between different types of architectural assets that exist at different levels of abstraction in the organization."[13] The diagram below depicts the GNB EA Repository and describes its sub-repositories.



http://gnbsp.gnb.ca/sites/EARep-RepAE/GNBGR/ADWGs/AIM/SitePages/Home.aspx

[12] For an overview of an architecture repository, please refer to Chapter 41 of the TOGAF® 9.1 Online Guide.
[13] TOGAF® 9.1 Online Guide, http://pubs.opengroup.org/architecture/togaf9-doc/arch/, Section 41.1

7. Communication, Training, and Education

Communication, training, and education are important elements of the EA Program and are supported by the OCIO's Communication and Learning (CL) team. The purpose of the CL team is to facilitate communication and learning within the OCIO, Public Bodies, and external stakeholders. The CL Analyst under the EAPO fulfills these responsible for the EA Program.

Specifically, the Communication and Learning Analyst:

- Provides strategic communication and learning advice to the EAPO team;
- Develops and maintains communication and learning plans;
- Designs and delivers Education, Training, and Awareness (ETA) materials, such as presentations and learning modules;
- Oversees and manages EA Program online presence;
- Ensures stakeholder engagement; and
- Ensures continuous improvement of communication processes and practices.

8. EA Maturity, Metrics, & Key Performance Indicators (KPI's)

EA is an enabler for business/government transformation and therefore the ultimate strategic value of an EA Program should be measured based on the positive impact that it has on the business and the realization of GNB strategy.

The EA Program strategic metrics are derived from the OCIO Business Plan (2012-2015). This plan establishes a goal and a set of objectives (milestones) for the evolution of the EA capability. The goal and objectives are stated below:

Goal:

By March 31, 2015, the OCIO will be strategically leading, coordinating and enabling enterprise-wide IM and ICT planning in partnership with GNB's public bodies and the private sector, to enable GNB strategy.

Objectives:

- By March 31, 2013, the OCIO will have improved alignment of IM and ICT planning to facilitate information and infrastructure re-use and sharing.
- By March 31, 2014, the OCIO will have produced enterprise-aligned IM and ICT plans, roadmaps and architectures to proactively align future requirements.
- By March 31, 2015, the OCIO will have a mature and continuously improved Enterprise Architecture Framework.

In order to measure the achievement of these objectives, the OCIO has identified two major KPI's, as described below, which are reported quarterly on the GNB's balance scorecard:

Enterprise Architecture Capability Maturity

A previous assessment[14] on the GNB EA capability in April 2010 indicated that the maturity of GNB EA was very low (level 1) at the time. In this assessment, a number of issues, including the lack of a formalized EA Program, were identified.

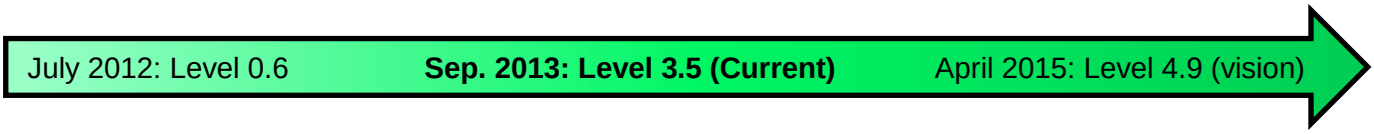
In order to address these issues and take advantage of EA benefits and values, OCIO defined EA as one of its cornerstones and made the commitment to improve EA maturity throughout GNB. Using the U.S. Department of Commerce's Architecture Capability Maturity Model (DOC ACMM V. 1.2)[15], the maturity of EA prior to establishing the GNB EA Program in July 2012 indicated the level of 0.6.

By establishing the current EA Program through the AIM Project during 2012 and 2013, the maturity of EA capability has been improved to level 3.5 (with 78% achieved at this level). The vision for the GNB EA maturity is to achieve level 4.9 (with 87% achievement) by March 31, 2015, as per the identified objectives under the OCIO Business Plan.

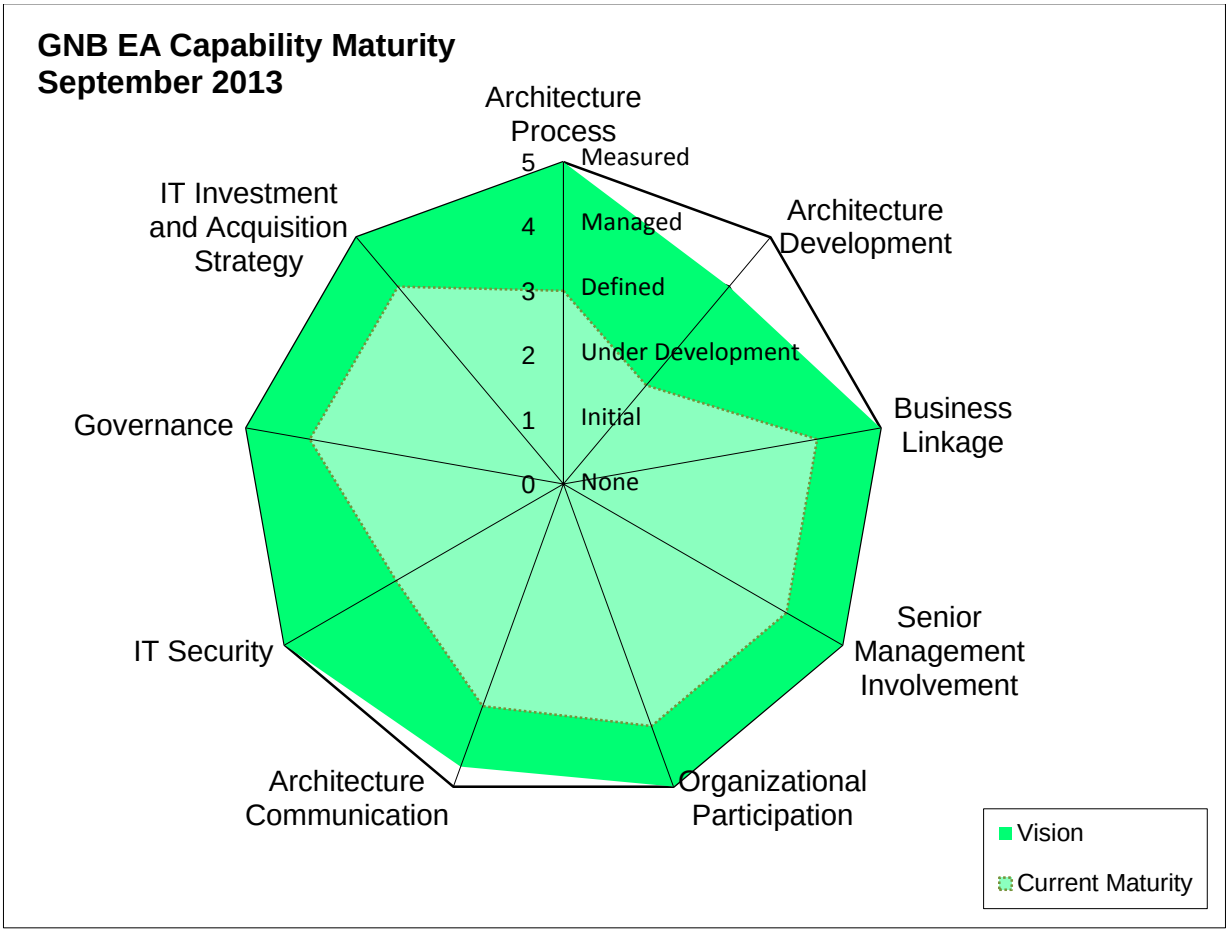
[14] Based on the Enterprise Architecture Maturity Model of the National Association of State Chief Information Officers (NASCIO)

[15] This is the maturity model provided in TOGAF® 9.1 specification, Chapter 51. For the complete guide, please refer to http://ocio.os.doc.gov/ITPolicyandPrograms/Enterprise_Architecture/PROD01_004935

The diagrams below depict the timeline on the GNB EA Maturity progress and also the 9 EA elements under the DOC ACMM with their current and vision maturity levels:



The GNB EA Capability Maturity Progress



GNB EA Capability Maturity

IM&ICT Plan Alignment Index

This index is to measure the level of alignment among IM&ICT public bodies' plans and the GNB Strategy. The target under this measurement is to have by March 31, 2015 at least 90% of the public bodies submitting a plan and at least 70% align directly with GNB Strategy.

Based on the current EA maturity, critical successful factors for the GNB EA Program are to:

- garner and keep EA stakeholders aware of GNB EA benefits, developments, and content offerings;
- gain commitment from EA stakeholders to contribute to the EA Program; and
- continually work with EA governance entities to promote EA at the executive levels and to resolve EA issues.

Based on these success factors, in addition to the above mentioned strategic measures, there are also the following measures.

Communication, Training, and Education (measuring awareness & communication)	**Target 2013-2014**	**Target 2014-2015**
% of internal stakeholders received awareness through the GNB EA Program Tour/Road Show, the EA Symposium, and/or other venues	**40%**[a]	**60%**
Number of venues used to reach out to external stakeholders	**4**[b]	**5**
Number of employees received training in different skills relevant to EA	**84**[c]	**160**
Number of EA educational materials developed & published	**0**	**10**

[a] *Based on the total count of 1,056 GNB IT Full Time Equivalent (FTE's) as internal stakeholders*

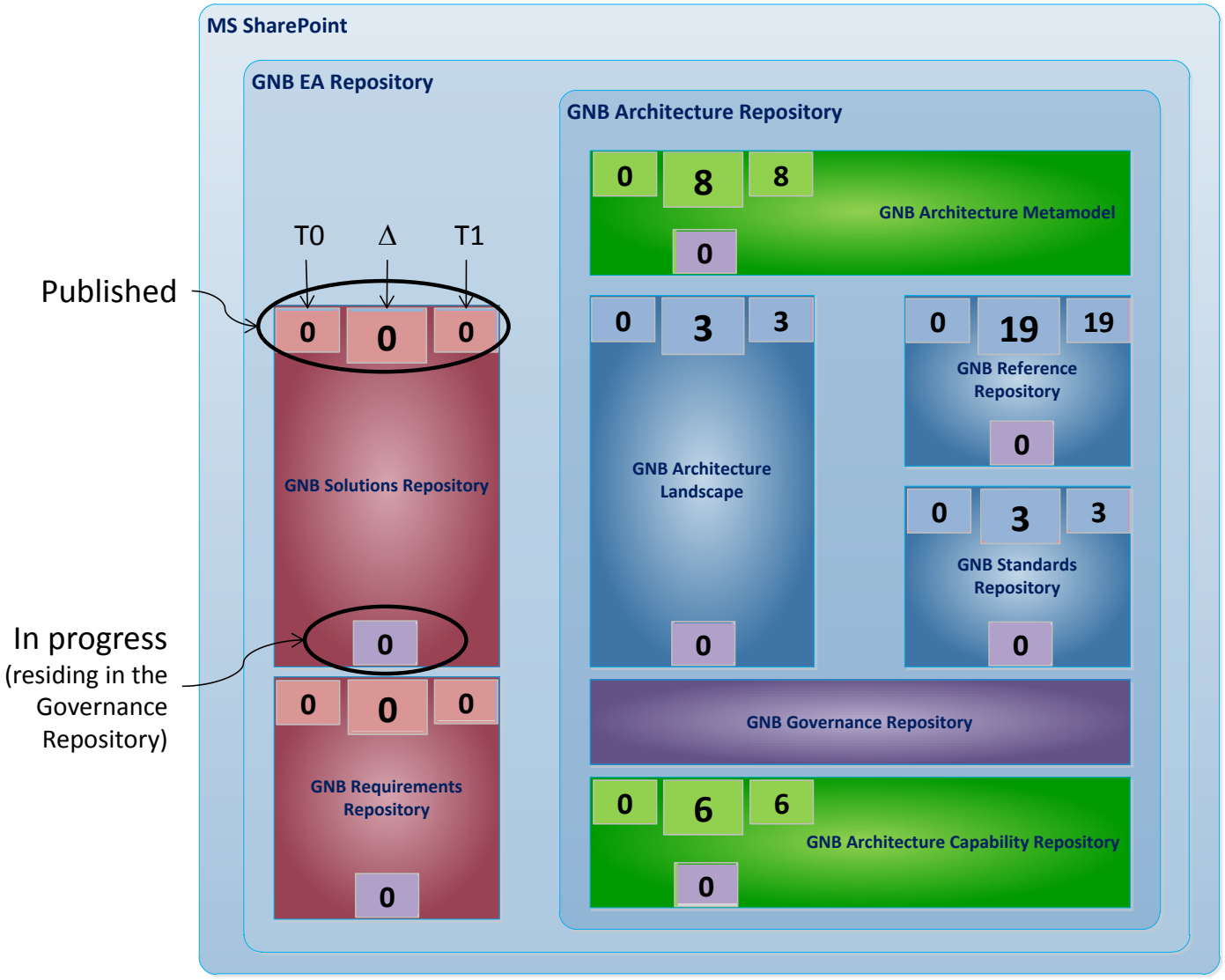
[b] *Article in Canadian Government Executive Magazine; Presentation at Canada's Government Technology Event (GTEC) 2013; 2013 Atlantic Provinces Reverse Trade Show; Conférence Tribunes des CIOs, Montréal, Québec*

[c] *16 (including EAPO): Elevating EA (soft skills)*
84 across four parts of GNB: Advanced Application of TOGAF®

The ARB Priorities (measuring the governance performance)	**Target 2013-2014**	**Target 2014-2015**
Number of priorities addressed & completed	**10**	**10**

EA Repository Dashboard (measuring EA content population and offering)

EAPO generates a regular report on the contents published and in progress in the EA Repository. This report is called EA Repository Dashboard and is presented to the ARB on a regular basis. The dashboard, as of September 2013, is provided below:



GNB EA Repository Dashboard, September 2013

Appendices

Appendix A: Enterprise Architecture Domains
Appendix B: EA Governance Bodies' Terms of References
Appendix C: EA Governance Processes
Appendix D: EA Principles
Appendix E: EA Vision

Appendix A: Enterprise Architecture Domains[16]

1. Business Architecture

Government needs reliable and cost effective operations. Business architecture provides the mechanism to clearly illuminate how strategy, processes, business structure, and staff can best be utilized to deliver reliable and cost effective operations. With this clarity, government can enable new functions and services with the right resources and technology, effectively and efficiently.

Business architecture initiatives (at the enterprise-level) have a strong focus on improving business performance (across multiple organizations). These benefits come in many forms, including:

- **Business decisions improvement**: Business architects create a clear and complete picture of the government's business model, strategy, and high-level operational processes. This results in enabling a more objective and structured decision-making process. What-if scenarios help government officials make complex choices on government services, transformations, operational processes, investments and reduction of costs. Most of these decisions will eventually have an impact on IT.
- **Business function rationalization**: Business architects create a rationalized view of business capabilities. This creates a foundation for making application portfolio investment decisions that align with business goals and strategies. By further decomposing these business capabilities, common services (for administrative operations and service delivery) are identified. This becomes a roadmap for service-oriented-architecture (SOA) view of the application portfolio.
- **Business process improvement**: By creating an end-to-end view of the organization's major business processes, business architects provide the basis for improved process management and continual process improvements.
- **Better business IT alignment**: Business architecture creates common definitions and vocabulary across the enterprise. This provides a common view of business capabilities, processes, and strategic needs for business and IT leaders.
- **Focus on value to the organization and the client:** Business architecture can help government analyze key value chains[17]. By understanding these value chains, it will help to remove roadblocks, reduce risks, and improve efficiency in processes and technology. This should result in better bottom line results.
- **Find synergies in generic processes:** By identifying the individual steps of business processes and their dependencies, government can make informed decisions and eliminate duplicate operations, processes, and technologies across organizations and functions. By consolidating and standardizing common operations, government can redirect budget, technology, and staff to focus on the government's value-chains.
- **Provide the blueprint for business transformation:** Business architecture provides the framework and methods to analyze and plan. The Enterprise Architecture provides the

[16] The content of this appendix provided by the OCIO-EAPO chief strategists.
Source: National Institutes of Health enterprise architecture, http://enterprisearchitecture.nih.gov/, except where indicated.

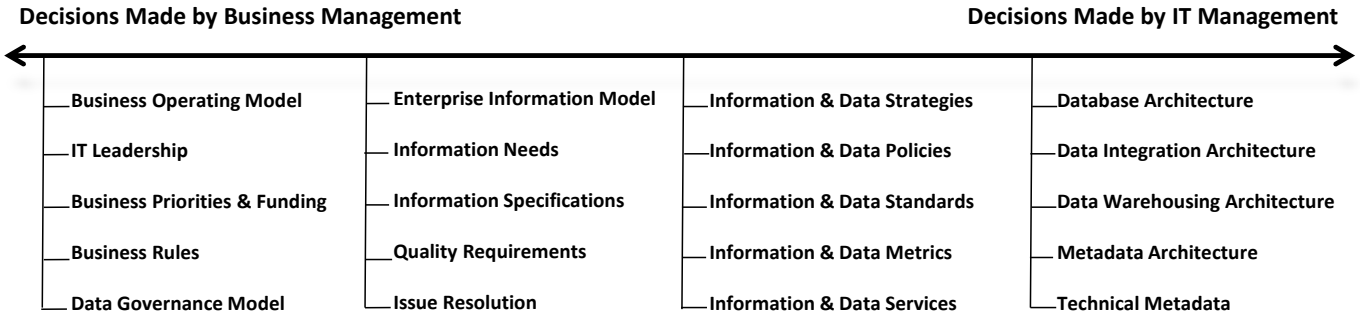
[17] Value chains are the functions and services that yield the most value for the organization and provide the clients with the necessary services, products, and information.

governance framework to recommend to government officials how the government should transform its structure, processes, technology, and staff.

The interdependencies of business architecture and information technology call for collaborative practices and organizational models. This connection is best structured as a true enterprise architecture practice, one that gives equal emphasis to business, information and technology concerns. This balanced model is GNB's view of enterprise architecture.

2. Information Architecture

Enterprise Information Architecture (EIA)[18] serves as the basis for governing enterprise information to respond to government business objectives and processes, and to integrate technological infrastructure and applications. It results from business architecture, an enterprise and a horizontal analysis that first defines an organization-wide strategic vision for analytics, finding, sharing, re-using, and managing enterprise information efficiently, independently of the applications involved. The following demonstrates the relationship between the business and IT and what type of decisions are made with each. Note that the relationship is a continuum and neither business nor IT makes the decisions in isolation.



Information Architecture is also the driving force behind the various Information Management (IM) services components such as:

- Web Content Management (WCM)
- Publishing Public Information
- Online Services
- Collaboration (external: with other jurisdictions, partners, investors, suppliers)
- Portals
- Information Access Tools (e.g. searches, navigation, discovery)
- Request for Information
- Records Management (RM)
- Digital Assets Management (DAM)
- Document Management (DM) and Collaboration (internal)
- Correspondence Management
- Process Automation (Workflows, BPMS)
- e-Mail Management
- Imaging
- Electronic Forms
- Integration, Interfaces
- Transformation, Conversion

[18] IT Toolbox Wiki: http://wiki.ittoolbox.com/index.php/Topic:Information_Architecture

- Master Data Management
- Business Intelligence
- Performance Measurements
- Data Mining
- Archives

Together with the Business Architecture, Information Architecture maps business information systems or "applications" and enterprise data to business processes. Information Architecture also specifies which parts of the business process are supported by each application and where each type of data is stored and managed.

Sample sub-architectures of IA could include:

Domain	Description
Presentation Architecture	Consists of the development (in cooperation with other stakeholders) and the provision of standards for portals, screens, forms, etc. and a governance model to enforce them in the enterprise.
Data Architecture	Through data models, the Data Architecture identifies the data the organization manages to perform its mission. For example, access and distribution models identify enterprise data stores and information flows.
Metadata Standards & Metadata Registry	Consists of the development and the provision of data standards for commonly used data derived from international and national standards, the provision of a framework to departments for creating data standards, the provision of a registry to communicate approved standards and a governance model to enforce them in the enterprise.
Integration Architecture	The Integration Architecture consists of models that identify how information and applications are integrated to support enterprise analytics and end-to-end business processes and operations. It also includes the organization's strategy for information integration and application integration.
Records Architecture	Consists of models that identify how records (structured and unstructured) are managed and how applications are integrated with these components.
Access to Information Architecture	Consists of models that identify how access to information is achieved by enterprise applications such as websites, intranets and ERP, and to meet requests to information. This architecture includes how user interfaces meet for example, the Official Languages Act and policies and the government brand policy. This architecture uses specifically the Business Reference Models from the Business Architecture.
Business Intelligence and Performance Measurements Architecture	Consists of semantic models that identify how data is mapped and merged to achieve enterprise intelligence and provide data to measure enterprise performance.

Data Governance	Consists of processes, policies, and laws affecting the way GNB directs, administers and controls information. Today these are decentralized. Examples: • Right to Information and Protection of Privacy Act (Executive Council) • Personal Health Information Privacy and Access Act (Health) • Official Languages Act (Premier's Office) • *Documents Regulation* • *Services and Communications Regulation* • Archives Act (DSS) • *General Regulation– Archives Act* • Public Records Act (Attorney General) • Electronic Transactions Act (Attorney General) • *Exclusion Regulation – Electronic Transactions Act* • Fees Act (Finance) • Queen's Printer Act (Attorney General) • Common Business Identifier Act (SNB) • Department Specific Legislation • Language of Service Policy / Language of Work Policy • Records Management Policy • Microfilming Policy • Directory of Services Memorandum of Understanding (DSS) • Government Directory Memorandum of Understanding (SNB)

3. Application Architecture

Application Architecture (AA) represents the organization's application portfolio and identifies the business systems that enable and support the execution of the business processes. It provides a cross reference of application to business functions and processes to illustrate application boundaries.

The need for applications arises from the requirements coming from the business and information domains. As with the definitions of all domains, the application architecture concepts involve a certain amount of abstraction. While a cohesive set of screens or web pages may feel like an application to the user, the backend (unseen by the user) may combine parts from different systems, platforms, and languages with purchased components and software hosted by business partners. It is becoming less useful to talk about "an application", and more useful to deliver integrated functionality to end users.

4. Technology Architecture

Technology Architecture describes the organization's current and future technical infrastructure and specific hardware and software technologies that support the information systems. It provides guidance and principles for implementing technologies that are proven to work well with existing and planned technologies.

A technical architecture might be comprised specifically of the following areas:

Technical Area	Description

Networks	Consists of the major technical elements required to provide data and Internet communications between users and locations around the globe, as well as communications with business partner sites (e.g., universities, hospitals, other levels of government).
Platforms	Identifies the underlying hardware and software that determine an information system's operations, functions, and specialization.
Security	Describes a set of standards to follow and products that have been shown to work well when developing security solutions, with the objective of maintaining the confidentiality, integrity, and availability of information and information systems such that the level of protection is commensurate with risk.
Systems Management	Identifies technical tools for monitoring and collecting data on system performance to enable better availability, performance, and reliability from the IT environment.

5. Security Architecture

Security Architecture describes the organization's existing and planned controls that ensure that information is available and can continue to be used for the purposes it is collected for while maintaining its confidentiality, and integrity. These controls can be technical, physical or administrative in nature and at GNB are broken into the following specific domains.

Domain	Description
Data Security	The protection of data and information throughout its lifecycle; from creation, processing, storage and eventual destruction. Controls such as encryption, backups, & data sanitization are examples found in this domain.
Server & Storage Security	Controls implemented at the point where data is stored and processed. Operating System Hardening, patch management, and authentication can be found in this domain.
Application Security	Controls implemented during an application's life-cycle to prevent compromise of the application, the data it serves and the platform(s) it is hosted on. Coding standards, input and output checking, patch and change management are all found within this domain.
Network Security	The protection of data as it is transferred via network technologies and protocols. Controls implemented here deter, deny and detect unauthorized logical access to data resources. Firewalls, VPNs and Intrusion Detection Systems are examples found in this domain.
Client Security	Controls implemented to protect the systems end-users access data from. This includes PCs, smartphones and thin clients. Items such as Anti-virus, password management and patch management can be found in this domain.
Identity & Access Management	Identifying individuals in a system and controlling access to the resources in that system by placing restrictions on the established identities of the individuals. Background checks, access control technology and tokens are found in this domain.
Physical Security	Controls implemented to deter, deny and detect unauthorized physical access to a data center, or office facility wherein data resources are housed. Examples in this domain are proximity cards, cameras and security guards.

Governance	The set of processes, policies, and laws affecting the way GNB directs, administers or controls information security. The Government Information System Security Policy (GISSP), the supporting standards, threat risk assessments, and the metrics collected all are part of this domain.

An absolute security, where all risk is eliminated, is neither reasonable nor cost-effective. The government security program is not designed to eliminate cyber risks, but rather to minimize risk to government operations to ensure compliance with legislative requirements and to ensure information is used for its intended purpose.

Appendix B: EA Governance Bodies' Terms of References

Executive Steering Committee (ESC) Terms of Reference

MISSION STATEMENT

The Executive Steering Committee (ESC) provides the governance that is essential to make "Enterprise" Architecture work for GNB (including Parts I, II, III, and IV). The focus of the ESC is on the holistic aspects of Information Management (IM) and Information and Communications Technology (ICT), including understanding and directing the linkage among GNB strategy, business transformations, information governance transformations, and technology directions and investments at the enterprise-wide level.

EXECUTIVE STRUCTURE

- The Executive is composed of a Chair, a Vice-Chair, and a Secretary.
- The OCIO Enterprise Architecture Program Office (EAPO) Support Team provides administrative support.

MEMBERSHIP

- Including the Executive, there are eleven (11) permanent and four (4) rotating members.
- The rotating members are appointed for a two-year term and may not serve more than three consecutive terms.
- The Executive Sub-committee will appoint new members, as required.
- With advance notification and approval by the Chair, alternates may replace regular members when necessary. Approved alternates will have the same voting power as a regular member.

Table below provides the list of the committee's membership at launch:

Role	Organization	Title	Name
Committee Executive			
Chair	ECO	The Clerk of the Executive Council Office	Byron James
Vice-Chair	ECO – OCIO	Government Chief Information Officer (GCIO)	Christian Couturier
Secretary	FacilicorpNB	President & CEO	Gordon Gilman
Permanent Members			
	ECO	The Clerk of the Executive Council Office	Byron James
	ECO – OCIO	Government Chief Information Officer (GCIO)	Christian Couturier
	FacilicorpNB	President & CEO	Gordon Gilman
	DGS, SNB, NBISA	Deputy Minister of DGS and President of SNB and NBISA	Sylvie Levesque-Finn
	HorizonNB	CEO	John McGarry
	VitaliteNB	CEO	Rino Volpé
	ASD-E	Superintendent	Gregg Ingersoll

	DSF-NO	Direction Générale	Bertrand Beaulieu
	NB Power	President & CEO	Gaëtan Thomas
	ECO	Assistant Secretary to Cabinet for Government Renewal	Judy Wagner
	ECO	Chief of Strategy Management	Jane Washburn
Rotating Members			
	DTI	Deputy Minister	Jean-Marc Dupuis
	SD	Deputy Minister	Edith Doucet
	DPS	Deputy Minister	Dale Wilson
	ANBL	President & CEO	Daniel Allain

ROLES AND RESPONSIBILITIES

Chair:

- Chairs the meeting - facilitates the discussion of issues.
- Prepares ESC agendas using input gathered from committee representatives.
- Reviews prepared minutes prior to distribution.

Vice-Chair:

- Provides assistance to the Chair, as requested.
- Hosts and chairs ESC meetings in the event that the Chair is unavailable.

Secretary:

Ensures that:

- Meeting minutes are taken.
- The agenda and minutes of the previous meeting are distributed to all members.
- Arrangements are made for any guest speakers.
- Meeting locations are secured.

All ESC members:

Advocacy & Leadership:

- Enhance and endorse the GNB Enterprise Architecture (EA) Roadmap;
- Influence all GNB IM & ICT stakeholders to align to and buy into the EA Roadmap;
- Support the GCIO in engaging stakeholders towards delivering the EA Roadmap;
- Ensure the alignment of GNB strategy and business transformation with IM & ICT priorities;
- Recognize and promote the value of EA and its accomplishments;
- Foster understanding of GNB business drivers, direction, strategy, trends and how they impact the future of GNB;
- Provide strategic direction for EA;
- Provide sponsorship and support cross-GNB commitment to EA;
- Ensure that GNB EA is part of strategic decision-making processes;
- Promote the use of Business Capability Modeling (a top-down planning technique that focuses on business outcomes) for effective IM & ICT planning.
- Provide insight into how to identify and address foreseeable areas of conflict;
- Provide insight into the EA long-term vision and the requirements and constraints of the environment under which public bodies operate;

- Promote an enterprise wide IM & ICT planning framework;
- Where appropriate, support funding requests through Memorandums to the Executive Council (MEC) presented to the Board of Management (BoM).

MODE OF OPERATION

- ESC will meet *semi-annually*.
- The meetings will be held around mid-year (June) and close to the end of the calendar year (December), unless otherwise agreed by the members.
- Members or non-members may request that items be placed on the agenda. Final approval for the agenda lies with the Chair.
- The Committee Executive (Chair, Vice-Chair, and Secretary) will meet in between regularly set ESC meetings, to prepare for the next ESC meeting.
- Recommendations from the committee shall be recorded in the minutes and a formal memorandum from the Chair will be issued to appropriate stakeholders as required.
- ESC will generally operate on a consensus basis; however, the Chair will be the ultimate decision maker. A vote may be requested by a committee member. A quorum, defined as 60% of the members, must be in attendance for a vote to take place. Each member shall have one vote.
- For agenda items with a formal presentation, the presenter(s) must supply, if possible, an electronic copy of their material to the Secretary to be shared with the committee members.
- The agenda and minutes of the previous meeting will be posted to all members in advance of each meeting. Agendas & minutes, information items, and presentations will be posted on the ESC site under the Governance sub-repository of the GNB EA Repository located at *http://gnbsp.gnb.ca/sites/EARep-RepAE/GNBGR/GNBESC/SitePages/Home.aspx*.
- Non-members will attend the meetings only for the duration of their agenda item.
- At the request of the committee, the Chair or Vice-Chair following a collaborative structured process will represent the collective views of the committee to other government groups/committees, etc.
- The Committee may form sub-committees, through EAPO to address and make recommendations on issues that have been brought to, or identified by the Committee. Sub-committees will comprise of OCIO chief strategists for each architecture domain (or an equivalent role), public bodies' chiefs of architecture domains, IT managers, and/or business owners. Sub-committees report to the Vice-Chair or the designate responsible for each particular initiative, who in turn will report back to the Committee. The Vice-Chair or the designate will be responsible for establishing sub-committees and agendas. The administrative support responsibilities of sub-committees will be facilitated by the EA Program Office.
- The Committee will form a permanent Executive Sub-committee comprised of the Committee Executive (Chair, Vice-chair, and Secretary) and no more than two committee members.
- The Committee may delegate decisions or tasks to this Executive sub-committee to expedite the business of the ESC.
- Language of Work: The committee's language of work is determined annually as the membership changes. Members are to advise alternates of the committee language of work, and if bilingual accommodations are required for a particular meeting, the Chair is to be advised in advance of the meeting.
- There will be an annual review of the membership composition and the Terms of Reference during the *December* meeting. Any revisions to the Terms of Reference take effect immediately.

Architecture Review Board (ARB) Terms of Reference

MISSION STATEMENT

The Architecture Review Board (ARB) ensures appropriateness, consistency, and completeness of the holistic GNB Enterprise Architecture (EA), evaluates compliance, assesses the impacts of the "next big project" of the "Enterprise" Architecture, and promotes EA within the public bodies.

The ARB:

- Reviews and provides recommendations on architectures (EA Development Process);
- Evaluates compliance to recommend to GCIO (Compliance Assessment Process);
- Evaluates Requests for Exception to recommend to GCIO (Dispensation Process); and
- Provides guidance to EA sub-committees and working groups.

EXECUTIVE STRUCTURE

- The Board Executive is composed of the Chair, a Vice-Chair, and a Secretary.
- The Chief Solutions Strategist of the Office of the CIO serves as the Chair.
- The Vice-Chair and Secretary are elected by the board members for a one-year term and may not serve more than two consecutive terms.
- The one-year term is defined as *January to January*. Nominations occur at the *November* meeting with elections taking place at the *December* meeting. New appointments take effect in *January*.
- The EA Program Office (EAPO) Support Team provides administrative support.

MEMBERSHIP

- 8 to 10 permanent members at CIO and CTO levels.
- 3 rotating members elected from ADM level.
- OCIO EAPO chief strategists (information, application, technology, and security architecture domains) represent the EAPO as non-voting members.
- The rotating members are elected by the board members for a one-year term and may not serve more than two consecutive terms.
- The one-year term is defined as *January to January*. Nominations occur at the *November* meeting with elections taking place at the *December* meeting. New appointments take effect in *January*.
- With advance notification and approval by the Chair, alternates may replace regular members when necessary. Approved alternates will have the same voting power as a regular member.

Table below provides the ARB's membership:

Role	Name	Title	Organization
Board Executive			
Chair	Christian Couturier	Acting Chief Solutions Strategist	OCIO – EAPO
Vice-Chair	Derrick Jardine	CIO	FacilicorpNB
Secretary	Ken Fitzpatrick	VP of IT Infrastructure and Applications	NBISA
Permanent Members			
	Christian Couturier	Government CIO, Chair of ITMAC	ECO, OCIO
	Derrick Jardine	CIO	FacilicorpNB
	Ken Fitzpatrick	VP of IT Infrastructure and Applications	NBISA
	Laurie Robichaud	Director of Information and Technology Management, Vice Chair of ITMAC	ELG
	Gary Beattie	CIO	NBCC
	Luc Bourgoin	Directeur des TIC	CCNB
	Carol Macdonald	VP of Technology and Business Development	SNB
	Louise Ouellette	Director of Information Systems Services	EECD
	Dwayne Chase	Director of Information Technology	ANBL
	Huguette Pothier	Director of Information Systems - Shared Services	NBPower
Rotating Members			
	Jerome Connors	Executive Director	DPS
	Judy Ross	Vice President	SNB
	Cheryl Hansen for Tom Maston	Assistant Deputy Minister, Corporate Services	DoH
Non-Voting Members			
	Robert Arsenault	Chief Solutions Strategist	OCIO – EAPO
	Diane Nadeau	Chief Information Strategist	OCIO – EAPO
	George Papageorgiou	Chief Application Strategist	OCIO – EAPO
	Robert Loughlin	Chief Technology Strategist	OCIO – EAPO
	Jamie Rees	Chief Information Security Strategist	OCIO – EAPO

ROLES AND RESPONSIBILITIES

Chair (Chief Solutions Strategist):

- Chairs the meeting – facilitates the discussion of issues.
- Prepares ARB agendas using input gathered from board representatives.
- Reviews prepared minutes prior to distribution.

Vice-Chair:

- Provides assistance to the Chair, as requested.
- Hosts and chairs ARB meetings in the event that the Chair is unavailable.

Secretary:

- Review of the meeting notes to assist in the preparation of formal minutes.
- Assist in coordinating guest speakers for the meetings and securing meeting locations.

All ARB members:

EA Development

- Review and provide recommendations on the EA Program Charter including the EA processes, EA principles, architecture visions and plans, and the EA Governance Framework;
- Review and provide recommendations on the conceptual (high level) and detailed domain architectures, including recommended products, technologies and standards;
- Discuss and reach consensus on why and how an architecture will benefit GNB, the level of effort involved, and commitment to comply with the guidelines; and
- Establish working groups or sub-committees, as described under the Mode of Operation.

EA Compliance

- Consider architecture compliance issues from a horizontal, cross-cutting perspective, in the process of identifying the preferred technical solutions;
- Provide guidance on issues related to technical compliance with the architecture; and
- Provide guidance on GNB-wide IT initiatives that have an EA-related perspective

Exception Requests (Dispensation)

- Review and recommend exceptions to the enterprise standards and architectures, and
- Review and provide recommendation on dispensation request for major projects

Security and Information Assurance

- Review applications escalated by the Corporate Information Security Officer (CISO) for exception to the Government Information Systems Security Policy (GISSP). Exceptions shall be based upon input from the CISO, the System Owner and industry experts, enabling the ARB to make recommendations based upon a full understanding of the benefits and risks associate with the request.
- The ARB Executive will be an advisor to the CISO when modifications to the GISSP and supporting security documentation are being considered. In the case of major modifications a meeting of the ARB may be convened by the CISO to solicit advice. Input around minor modifications may be collected via email.

Service-Oriented Architecture (SOA)

- Serve as an advisor to the SOA Competency Centre (SOACC);
- Review all architectures for SOACC projects; and
- Review future SOA strategic direction and roadmap.

MODE OF OPERATION

- ARB will meet monthly or as required, depending on the workload.
- The monthly meetings will be held on the *second Wednesday* of each month, unless otherwise agreed by the members.
- Members or non-members may request that items be placed on the agenda. Final approval for the agenda lies with the Chair.
- The Board Executive (Chair, Vice-Chair, and Secretary) will meet in between regularly set ARB meetings, to prepare for the next ARB meeting.
- The agenda items typically include minutes of previous meeting, requests for change, requests for exception (dispensation), architecture compliance results review, and dispute resolution.
- Recommendations from the Board will be recorded in the minutes and a formal memorandum from the Chair issued to appropriate stakeholders.
- ARB will generally operate on a consensus basis. A vote may be taken upon request by a board member. The vote will not take place until the following meeting allowing time for the formal recommendation to be recorded in the minutes. A quorum, defined as 60% of the members, must be in attendance for a vote to take place. Each member will have one vote.
- For agenda items with a formal presentation, the presenter(s) must supply, if possible, an electronic copy of their material to the secretary to be shared with the board members.
- The agenda and minutes of the previous meeting will be posted to all members in advance of the meeting. Agendas & minutes, information items, and presentations will be posted on the ARB site under the Governance sub-repository of the GNB EA Repository located at *http://gnbsp.gnb.ca/sites/EARep-RepAE/GNBGR/GNBARB/SitePages/Home.aspx*.
- Non-members will attend the meetings only for the duration of their agenda item.
- At the request of the board, the Chair or designate(s) shall, following a collaborative structured process, represent the collective views of the board to other government groups/boards, etc.
- The Board may form EA Sub-committees, through EAPO to address and make recommendations on issues that have been brought to, or identified by, the ARB or the ESC. EA Sub-committees will be composed of OCIO chief strategists for each architecture domain (or an equivalent role), public body chiefs of architecture domains, IT managers, and/or business owners. Sub-committees will report to the Vice-Chair or the designate responsible for each particular initiative, who in turn will report back to the board. The Vice-Chair or the designate will be responsible for establishing sub-committees and agendas. The administrative support responsibilities of sub-committees will be facilitated by the EA Program Office.
- The Board will form a permanent Executive Sub-committee comprised of the Board Executive (Chair, Vice-chair, and Secretary) and two board members.
- The Board may delegate decisions or tasks to this Executive sub-committee to expedite the business of ARB.
- Language of Work: The board's language of work will be determined annually as the membership changes. Members are to advise alternates of the board's language of work, and if bilingual accommodations are required for a particular meeting, the Chair is to be advised in advance of the meeting.
- There will be an annual review of the membership composition and the Terms of Reference during the *September* meeting. Any revision to the Terms of Reference will take effect by the *October* meeting.

Enterprise Architecture Program Office (EAPO) Terms of Reference

MISSION

The Enterprise Architecture Program Office (EAPO) is located within the Office of the Chief Information Officer (OCIO) of the Executive Council Office. It is a permanent Enterprise Architecture (EA) Program management office whose purpose is to cultivate EA throughout GNB. One of the primary responsibilities of the office is to promote and support the Government of New Brunswick (GNB) through the application of EA.

The EAPO coordinates and manages the EA Program, EA Standing Committees, the governance framework and processes, and the EA Repository and its content. It is responsible to ensure that EA projects are carried out consistently and successfully in compliance with GNB recommended methods, standards, and strategies. The EAPO provides:

- A central repository for architecture standards, methods, processes and policies;
- The authority to enforce architecture governance; and
- A forum to cultivate EA throughout the organization.

OBJECTIVES

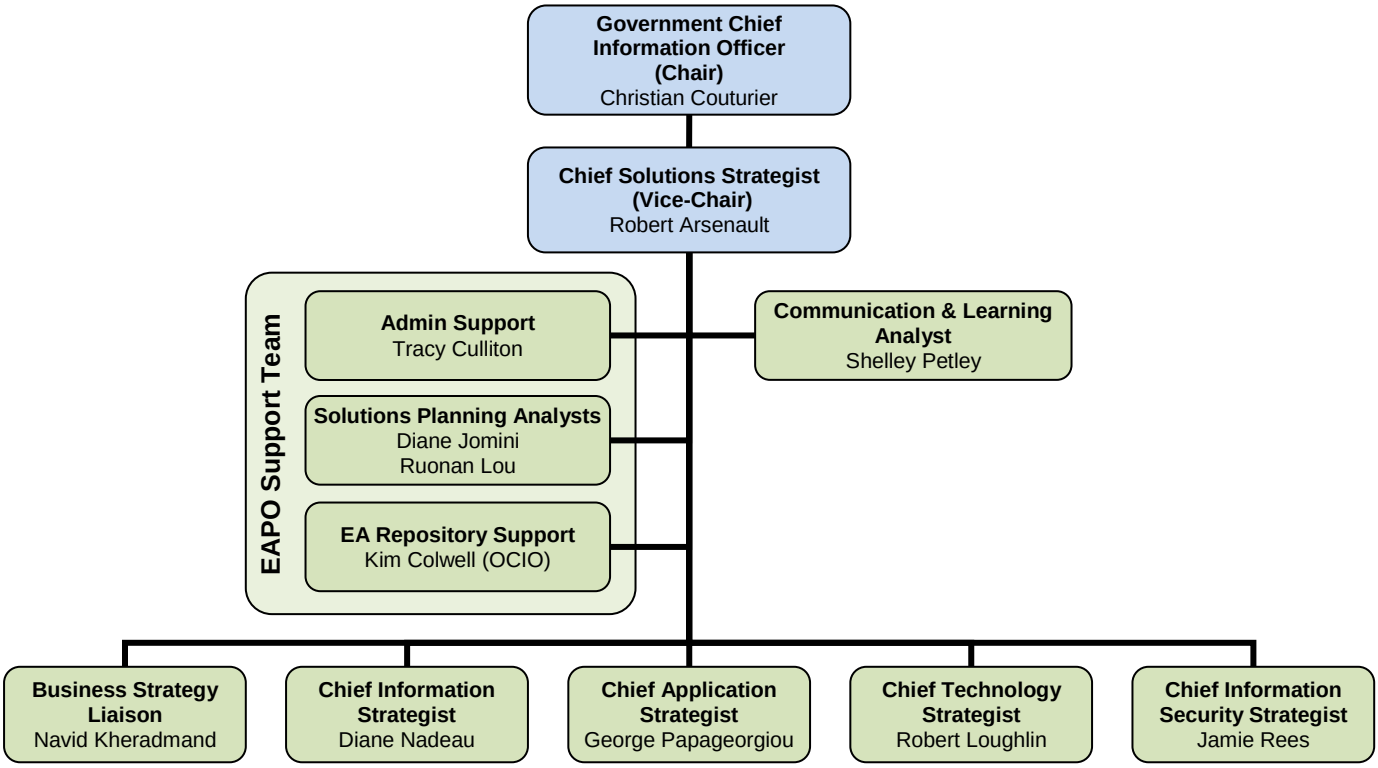
- Develop a core conceptual model and methodologies to support public bodies in the development of their EA. The model will promote public body-specific tailoring while maintaining a common conceptual structure;
- Develop consistent, GNB-wide business, information, application, and technology architecture standards (these will likely progress from the establishment of methods, guidelines, and best practices);
- Develop reusable guidelines which address business asset reuse, information reuse, technology asset reuse, and Service Oriented Architecture (SOA) guidelines for reuse; and
- Prioritize, review, and establish GNB-wide and/or shared applications that address common business problems.
- Provide primary support to senior and line business managers on current and proposed business process improvement;
- Serve in an advisory capacity on, Information, Application, Technology and Security architectures;
- Consult on the design and development of EA components related to specific projects;
- Make recommendations and provide advice on policy, procedures, standards, and benefits relating to the development, maintenance and evolution of the EA;
- Serve as a “working group” for architectural priorities specifically set by the EA governance bodies, namely Executive Steering Committee (ESC) and Architecture Review Board (ARB), or architecture stakeholders;
- Promote standard architectural practices throughout the organization;
- Communicate best practices, ideas, and evolutionary architectural elements to stakeholders.

STRUCTURE

The EAPO will be composed of a Chair (Government Chief Information Officer), a Vice-Chair (Chief Solutions Strategist), a domain subject matter expert (SME) for each domain, the EA Support Team, and an OCIO Communications and Learning Analyst. Deputy Chief Information Officer (Deputy CIO) is an ex-officio member of the EAPO.

The domain SMEs could be any or all of:

- **Business Strategy Liaison** – ensures that EAPO is working tightly with public bodies and the Office of Strategy Management;
- **Chief Information Strategist** – provides input concerning the elements necessary to support and integrate the business and key business information;
- **Chief Application Strategist** – translates the other elements into design and/or configuration specifications that can be supported by the Technology Architecture.
- **Chief Technology Strategist** – provides input concerning the requirements necessary to support the application, infrastructure, and/or the service being developed;
- **Chief Information Security Strategist** – provides input and direction on which Security Controls are required to support service or product delivery; whether the controls are process or technology oriented, or the asset or information in question is physical or logical.



EAPO Organizational Structure

ROLES AND RESPONSIBILITIES

The EAPO is comprised of the following roles:

- Government Chief Information Officer (GCIO), as the Chair
- Chief Solutions Strategist (CSS), as the Vice-Chair
- Chief Strategists (Domain Subject Matter Experts)
- EA Support Team
- Communication and Learning Analyst

The EAPO's central responsibility is the daily execution and management of the GNB EA Program and associated activities and initiatives. In this capacity, the EAPO's primary responsibilities are to:

- Lead in the creation and renewal of architecture and standards;
- Lead and facilitate the architecture domain team processes;
- Manage domain team memberships;
- Design GNB mission and architecture alignment;
- Lead assessments of evolving technologies for the purpose of standards adoption or renewal;
- Plan and recommend architectural migration;
- Assess the current environment in specific technical areas;
- Publish the architecture in the chosen format;
- Conduct awareness/education sessions;
- Advise on business and IT planning;
- Interpret and communicate architecture issues and choices;
- Advise project teams on the best use of architecture;
- Support projects on assessing compliance when requested;
- Evaluate project requests for exceptions to architecture; Develop recommendations for the Architecture Review Board (ARB) as the basis for decision-making;
- Represent GNB EA architecture to the public bodies; and
- Provide EA reviews in support of GNB capital planning and investment processes.

Responsibilities of the Government Chief Information Officer (Chair)

- Chair the meetings - facilitate the discussion of issues.
- Prepare EAPO meeting agendas using input from EAPO members.
- Review minutes prior to distribution.

Responsibilities of the Chief Solutions Strategist (Vice-Chair)
As the Vice-Chair:

- Provide assistance to the Chair, as requested;
- Host and chair EAPO meetings in the event that the Chair is unavailable;
- Establish working groups and their agendas.

As the Chief Solutions Strategist (CSS):

The CSS manages and supports the EA and reviews proposed projects for EA compliance. The CSS is responsible for leading the development of GNB's EA, ensuring the integrity of the architectural development processes, and the content of the EA products. The CSS role can also act as the ombudsman to the information technology and program/business line units in the public bodies, and ensure that program/business unit processes are addressed in the public body EA. In addition, the CSS will:

- Ensure that the EA provides the best possible information and guidance for information technology projects and stakeholders;
- Manage the development of the EA (i.e., managing the production of EA content by program/business, IM and IT experts that form the EA team;
- Undertake the authority, responsibility, and accountability for the overall EA effort, planning and staffing. This includes liaising with the ARB for sustained funding, negotiating schedules for development and publishing of EA content, and the timely and accurate delivery of the EA products (or "artifacts"); and
- Advise the GNB EA governance entities on EA policy, communications requirements, exception handling, and technology direction.

In the future:

- Continue to refine the schedule and enhance the requirements for more comprehensive reporting, and in collaboration with the public body members of domains architecture, define the category of the system and the expected impact on GNB;
- Consult with public bodies to ensure appropriate EA tools, processes, and best practices are used and leveraged;
- Define and manage the change management process, including EA products, processes, and technologies.

Responsibilities of the Chief Strategists

Each domain of the GNB EA reference model is led by a subject matter expert (SME)., a senior resource with extensive experience in the domain. Typical activities would include:

- Develop the reference model (i.e. sub-architecture) for their domain as an integral portion of the overall GNB EA reference model. The model will typically include enterprise-level technical and information standards that can be used by GNB agencies and public bodies when they design solutions/systems, refresh technology, etc.;
- Review public body-proposed changes or enhancements to the reference model (sub-architectures) to ensure they are consistent with the GNB EA;
- Conduct spot checks of public bodies for compliance and review the components of existing systems when necessary;
- Work with public body EA project teams early in the development life cycle to achieve compliance with GNB EA;
- Consult with stakeholders across GNB on issues in their specific domain; and
- Recommend policies, standard operating procedures and manuals to support the above functions or activities.

Responsibilities of the EA Support Team

Admin Support:
Acts as the single point of contact for EAPO and provide secretarial support to EAPO, ARB, Executive Steering Committee (ESC), and EA working groups and sub-committees:

- Notify members when minutes are available;
- Take minutes of meetings;
- Distribute the agenda and minutes of the previous meeting to all members, prior to the next meeting;
- Coordinate guest speakers for the meetings; and
- Secure meeting locations.

Solutions Planning Analysts:
These are subject matter experts in:

- Architecture domains,
- enterprise strategies,
- program/service/business,
- information management,
- data scientist,
- standards,
- information systems, and
- information technology

who will provide support to the chief strategists in the areas of:

- Research,
- Development of artifacts including policies, standards, request for information and proposals,
- Development of business cases,

EA Repository Support:

- Develop and maintain services to support EA Repository technologies;
- Provide data and information stewardship services to manage and assure quality of the information (along with departmental representatives);
- Provide information management services for the EA Repository (architecture tools);
- Provide information management services for EA artifacts such as Acts and Regulations, Policies, etc.

Responsibilities of the Communication and Learning Analyst

- Provide strategic communication and learning advice to the EAPO team;
- Develop and maintain communication and learning plans;
- Design and deliver Education, Training, and Awareness (ETA) materials, such as presentations and learning modules;
- Oversee and manage EA Program online presence;
- Ensure stakeholder engagement;
- Ensure continuous improvement of communication processes and practices.

MODE OF OPERATION

- EAPO will meet bi-weekly on Thursdays unless otherwise agreed by the members.
- Members or non-members may request that items be placed on the agenda. Final approval for the agenda lies with the Chair.
- Recommendations from the EAPO members shall be recorded in the minutes and a formal memorandum from the Chair will be issued to appropriate stakeholders as required.
- Formal presenter(s) must supply, if possible, an electronic copy of their material to the secretary to be shared with the members.
- The agenda and minutes of the previous meeting will be posted and all members notified in advance of the meeting. Agenda and minutes will be posted on ***http://gnbsp.gnb.ca/sites/EARep-RepAE/GNBGR/GNBEAPO/SitePages/Home.aspx;*** Information items and presentations will be posted on the same location.
- Non-members will attend the meetings only for the duration of their agenda item.
- Based on the items on the agenda, Strategic Alignment and/or Strategic Sourcing staff may participate in the meetings.
- As directed by the Chair or designated Vice-Chair, a member or members of the EAPO will, following a collaborative process, represent the collective views of the EAPO to other government groups/boards as required.
- EAPO may form working groups, to address and make recommendations on issues that have been brought to, or identified by, EAPO, ARB, or ESC. Working groups can also be established to manage Architecture Compliance reviews and/or Architecture Creation process and to handle proposals for adoption, development, or amendment of EA artifacts. Working groups will be composed of OCIO chief strategists, members of EAPO Support Team, business owners, public bodies' architecture domains SMEs. Working groups will report to the Vice-Chair or designate responsible for each particular initiative, who in turn will report back to the EAPO. The Vice-Chair will be responsible for establishing working groups and agendas. The EAPO Support Team will facilitate secretarial responsibilities for the working groups.
- EAPO may form standing committees focused on specific domains of EA to foster the proper development and evolution of the domains. Standing committees will meet monthly.
- An annual review of the Terms of Reference will occur during the first meeting in October. Any revision to the Terms of Reference will take effect the second meeting in October.

EA Communities of Practice Terms of Reference

MISSION STATEMENT

EA Communities of Practice ensure the proper development and evolution of the architectural domains, namely information, application, technology, and security. These communities provide horizontal alignment, collaboration, and engagement of subject matter experts in the architectural domains throughout the government.

MEMBERSHIP

- The OCIO Chief Strategists act as the Lead of the communities.
- The membership should provide a fair presentation of the government public bodies, depending on the focus of the communities.
- Government CIO (GCIO) and Chief Solutions Strategist (Director of Solutions Planning) are considered ex-officio members of any of the communities.

ROLES AND RESPONSIBILITIES

- Collaborate in preparing next iterations of the GNB EA Roadmap;
- Influence the practice of EA by participating in the development of EA plans to align with the EA Roadmap;
- Participate in the EA strategic initiatives and action plans for each domain;
- Influence the development of public bodies' EA roadmaps and operational plans;
- Encourage the alignment of public bodies operational plans with the EA plans;
- Review domain architectures and enterprise directives, as needed;
- Promote active participation in the domain sub-committees and working groups;
- Raise awareness of EA successes in each domain;
- Support proper domains maturity and capabilities.

MODE OF OPERATION

- Communities will meet *2 or 3 times a year or as needed.*
- For agenda items with a formal presentation, the presenter(s) must supply, when possible, an electronic copy for distribution.
- Meeting documentation will be posted on each of the communities' sites under the Governance sub-repository of the GNB EA Repository located at:
    - Information Architecture: *http://gnbsp.gnb.ca/sites/EARep-RepAE/GNBGR/IACP/SitePages/Home.aspx*;
    - Application Architecture: *http://gnbsp.gnb.ca/sites/EARep-RepAE/GNBGR/AACP/SitePages/Home.aspx*;
    - Technology Architecture: *http://gnbsp.gnb.ca/sites/EARep-RepAE/GNBGR/TACP/SitePages/Home.aspx*; and
    - Security Architecture: *http://gnbsp.gnb.ca/sites/EARep-RepAE/GNBGR/SACP/SitePages/Home.aspx*.
- Non-members will attend the meetings only for the duration of their agenda item.
- The communities' language of work is determined annually as the membership changes.
- These Terms of Reference will be reviewed, as needed. Any revisions take effect immediately.

Appendix C: EA Governance Processes

To successfully implement the EA governance framework, key governance processes in the EA Program define the relationships among governance bodies and the decision making approaches. These governance processes ensure that the EA Program efficiently and effectively fulfills its vision and delivers value to its stakeholders through formal, clear, and well-defined procedures.

According to The Open Group Architecture Framework (TOGAF®), "Governance processes are required to identify, manage, audit, and disseminate all information related to architecture management, contracts, and implementation. These governance processes will be used to ensure that all architecture artifacts and contracts, principles, and operational-level agreements are monitored on an ongoing basis with clear auditability of all decisions made."[19]

EA Development

The EA development process includes adoption, development, amendment, and approval of EA capabilities and assets including artifacts, standards, guidelines, best practices, policies, etc.

The development process is triggered:

- as part of an EA initiative;
- at the request of the Chief Solutions Strategist (e.g. receiving recommendations or proposals from chiefs strategists);
- as part of a recommendation from one of the EA sub-committees or working groups;
- at the request of the Government Chief Information Officer (GCIO); and/or
- as part of an architecture lifecycle management procedure to review, revise, or retire existing EA artifacts.

The Architecture Review Board (ARB) reviews and makes recommendations on EA assets to the Government CIO (GCIO); however, the final approval for all EA assets is the responsibility of the GCIO. The EA Program Office (EAPO) facilitates and coordinates activities required to prioritize requests and adopt, develop, amend, and/or approve all EA assets.

All the requests for adoption, creation, and amendment of EA assets are received by EAPO. EAPO assesses these requests based on their significance and impact against the government IM & ICT priorities on the EA Roadmap. For EA assets of low significance or impact, such as operational and tactical assets (working guidelines or technical standards), EAPO provides the GCIO with a low priority request and the GCIO reviews and approves the request without ARB.

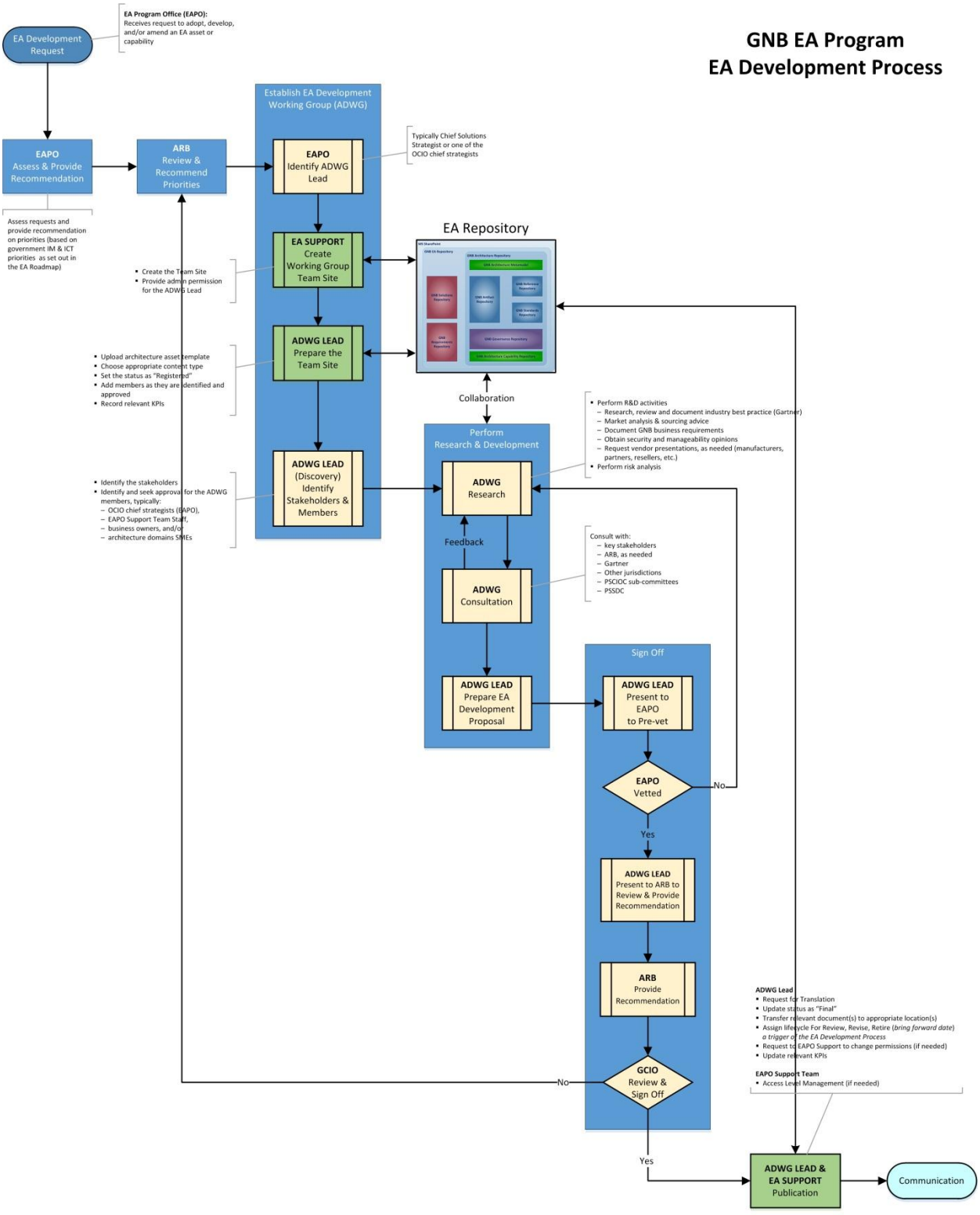
However, at the discretion of the GCIO, when the assets are of high significance or impact to the enterprise, such as high-level strategic assets, EAPO prepares an ARB priority request. The request is presented to ARB for review and their recommendations passed on to the GCIO, who retains final approval.

[19] TOGAF® 9.1 Online Guide, http://pubs.opengroup.org/architecture/togaf9-doc/arch/, Section 50.2.1.2

Once the priorities are set, EAPO establishes an architecture development working group composed of EAPO chief strategists, EAPO Support staff, business owners, and public bodies' architecture domains SMEs, and identifies the working group lead (typically the Chief Solutions Strategist or one of the EAPO chief strategists). The working group performs research and development on the asset or capability in consultation with key stakeholders including ARB.

The working group prepares the development proposal which is reviewed, recommended, and endorsed by EAPO before being presented to the ARB for endorsement and finally to the GCIO for sign off. Once the proposed architecture is approved, it follows the EA Repository Management workflows for registration, lifecycle management, access level management, and publication. The stakeholders are also informed of publications following an appropriate OCIO communication process.

The following diagram illustrates typical activities involved in the EA Development Process. The activities in green are part of the EA Repository Management and the communication activity in light blue is part of the OCIO communication procedure.



FINAL – 2013-02-13

Architecture Compliance

An essential aspect of architecture governance is ensuring the compliance of individual EA initiatives and assets with the approved enterprise architectures. An Architecture Compliance review is a scrutiny of the compliance of a specific initiative or asset against established architectural criteria and objectives.

The Architecture Compliance review process is triggered as part of the Strategic Alignment Process or ad hoc, at the request of the Chief Solutions Strategist or the GCIO. Depending on the scope of the initiative, EAPO may form a compliance review working group composed of EAPO chief strategists, EAPO Support Team, members of the project team, business owners, and public bodies' architecture domains SMEs. The ARB reviews and provides recommendations on the compliance assessments results presented by the working group. The GCIO has the final sign off on the assessment results.

In addition to the standard criteria set out in the Strategic Alignment process, EAPO also takes into consideration the TOGAF® Architecture Compliance Review Process and its requirements including the checklists provided in Chapter 48 of TOGAF® manual: http://pubs.opengroup.org/architecture/togaf9-doc/arch/. It is recommended that project owners and the public bodies' architecture teams become familiar with this process and its compliance criteria.

The Architecture Compliance Review Process encompasses the activities presented in the diagram next page. The activities inside the brown box are part of the Request for Exception (Dispensation) process, as described below.

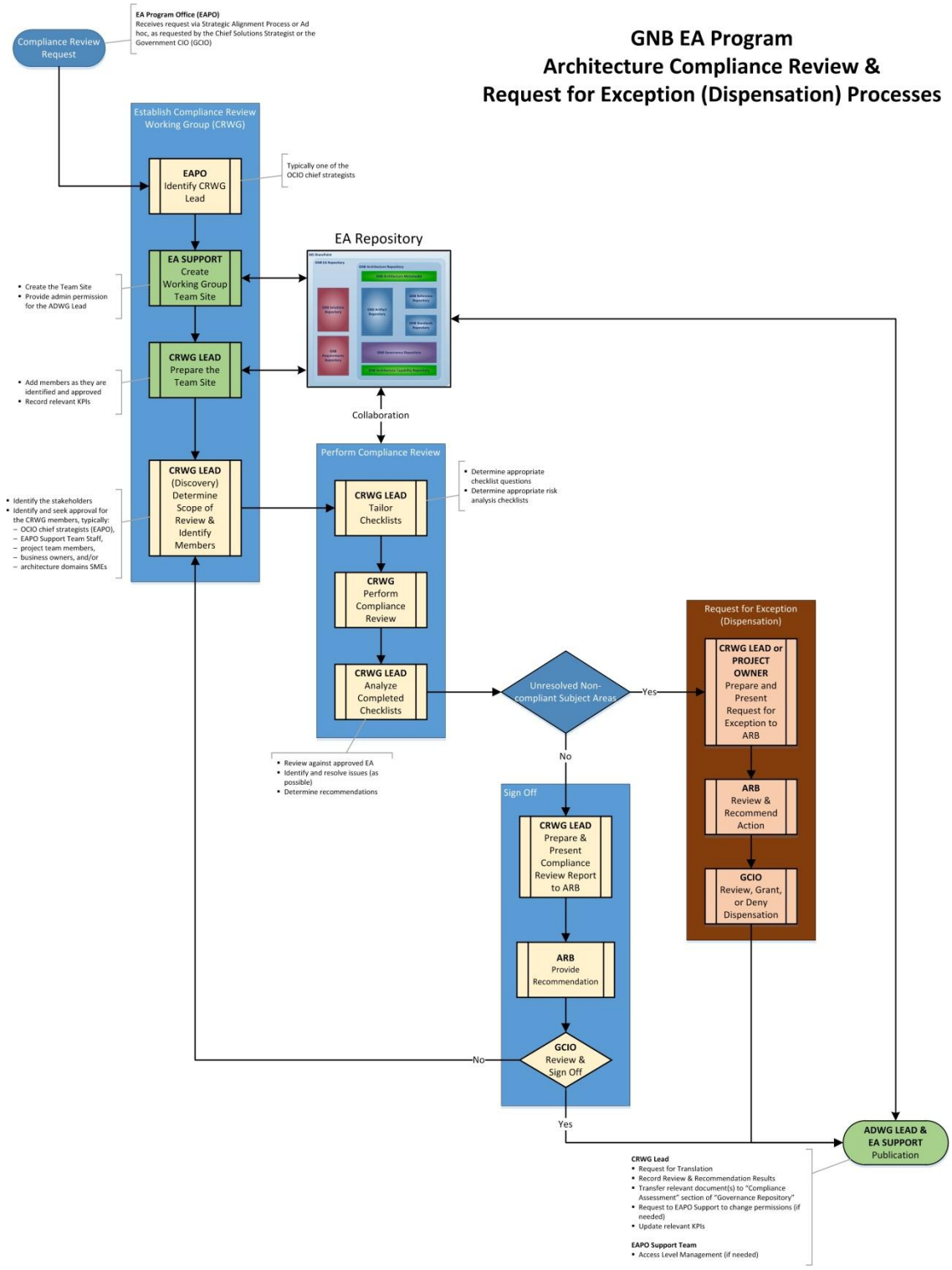
Request for Exception (Dispensation)

A request for exemption is required when an EA initiative or a subject area (design, operational, service level, or technology) does not comply with approved enterprise architectures. Non-compliance cases are identified at the initiation stage or are revealed through Architecture Compliance reviews.

The non-compliant subject area can be adjusted or realigned to meet the compliance requirements. However, if the subject area, despite best efforts utilized, cannot comply with approved architectures and/or needs more time to become compliant, the project owner or the working group lead responsible for the Architecture Compliance review of the initiative, must prepare a request for exception describing:

- the reasons for non-compliance;
- the efforts taken to comply (if applicable);
- the timeframe for the exemption;
- benefits of exception being granted and the implications of the exception not being granted; as well as
- a plan to achieve compliance.

Exemption requests received by the EAPO will be included on the next ARB meeting agenda for their review. ARB's recommendation is passed on to the GCIO, who grants or denies the dispensation.



FINAL – 2013-02-13

EA Repository Management

All EA assets and supporting information must come under governance through a set of formal workflows in order to register, validate, ratify, manage, and publish new or updated content.

The EAPO Support Team is responsible for these workflows, as part of its responsibility to manage the EA Repository and its content. The content is managed through a registration workflow, a set of standard procedures for content lifecycle management (Review, Revise, and Retire), which may trigger the EA Development Process, and appropriate access level management. The publication of content also follows an appropriate publishing procedure.

These workflows are described in more detail in a separate documentation.

Processes External to the EA Program

The EA Assurance and Strategic Sourcing processes are external to the EA Program; however, they have touch points with the EA processes and therefore their existence and impact need to be recognized in the EA context.

EA Assurance

The EA Assurance process consists of Strategic Alignment and Portfolio Management processes.

The OCIO Strategic Alignment (SA) process is a government inward facing, screening, and endorsement process ensures that all government body Information Management (IM) & Information and Communications Technology (ICT) activity aligns with established IM & ICT architectural directions. The OCIO gathers all relevant and appropriate information relating to IM & ICT related procurement activities, projects and initiatives and assesses this information to assure alignment with GNB's enterprise IM & ICT strategies, laws, architectures, policies, standards, and/or guidelines, both established and evolving.

Potential opportunities for consolidation of infrastructure, business solutions, and government cost savings are identified by the OCIO Strategic Alignment. This process guides government at the initiative level and functions in concert with the OCIO Portfolio Management process, which guides government at the portfolio level. Together, these processes ensure that optimal value is received for the investments made in IM & ICT.

Portfolio Management is a continuous process of identifying, selecting, and managing a selection of important IM & ICT projects in alignment with key performance metrics and strategic objectives as defined by the GNB Strategy Map. This enables GNB in doing the right things and doing things right.

Review of the active projects and consideration of the prioritization of IM & ICT resources leads to a more in-depth analysis, and improved executive decisions. Monitoring and analyzing the delivery of IM & ICT projects in terms of time, quality, budget, and benefit realization form the basis for the OCIO's IM & ICT project portfolio recommendations to the government.

Strategic Sourcing

To align business requirements with business strategy, Strategic Sourcing establishes and manages strategic sourcing opportunities, supporting architecture standardization and associated enterprise cost reductions for common ICT products and services.

The OCIO Strategic Sourcing provides enterprise accountability for the development of ICT sourcing strategies. This strategy optimizes costs and drives on-going performance of the supply chain while increases value-for-money. In concert with the EA and Strategic Alignment (SA) processes, Strategic Sourcing actively participates in multi-department working groups and develops Strategic ICT Sourcing recommendations for proposed corporate architectures. In partnership with Government Services – Strategic Procurement, Strategic Sourcing monitors & analyses contract spend, benchmarking and demand forecasting.

Appendix D: EA Principles[20]

1. Application of Principles

These principles of EA apply to all the public bodies of the government and the whole of government must abide by these principles.

2. Enabling Business and Information Readiness

EA should enable business and information readiness and be continuously refined to support public bodies' business strategies and plans and to provide quality and value to the stakeholders.

3. Compliance

EA and Information Assurance initiatives and activities must comply with all relevant and established principles, laws, regulations, and policies.

4. Standardization, Harmonization, and Normalization

The EA environment is standardized, harmonized, and normalized with respect to processes, technological diversity, information, data definitions, security, and all other EA components and assets.

5. Sharing and Integrating EA assets*

EA assets must be shared, when appropriate, across public bodies and must have a clear ownership. EA assets, whether developed by public bodies or acquired from other sources, must be properly integrated to enable sharing.

6. Interoperability

EA assets must, where possible, leverage defined standards that promote interoperability for data, application, and technology.

7. Information Quality is Everybody's Business

GNB must adopt an information quality culture where clear definition, correct value(s), and understandable presentation matters. Public bodies require quality information to make decisions to accomplish business objectives which affect stakeholders.

8. Information is a Valuable Enterprise Asset

Information is an asset that has value to the enterprise and must be managed accordingly.

9. Discoverability and Accessibility of Information

Information is easily discoverable, accessible, and understood.

10. Service Orientation

All architectures are based on a design of services which mirror real-world business activities comprising the enterprise business processes.

11. Robust, Reliable, Accepted, Supported, and Sustainable Technology

GNB will adopt new technologies that are demonstrably robust and reliable, have broad industry acceptance, have committed available support, are appropriate for the business needs, and are sustainable.

12. Risk-based Mitigation

GNB will use a risk-based treatment approach to ensure consistent and effective mitigation programs while maintaining the capability to address the risk to any particular data using multiple complementary techniques.

[20] The content of this appendix provided by the OCIO-EAPO chief strategists.

	1. Application of Principles
Statement	These principles of EA apply to all the public bodies of the government and the whole of government must abide by these principles.
Rationale	– These EA principles must be followed in order to provide maximum value to the government and enable information readiness by delivering timely, relevant, and quality information to all stakeholders.
Implications	– Without this principle, exclusions, favoritism, and inconsistency would undermine the EA's capability to enable information readiness. – EA initiatives will not begin until they are in compliance with the EA Principles. – A conflict with a principle will be resolved by changing the framework of the initiative.

	2. Enabling Business and Information Readiness
Statement	EA should enable business and information readiness and be continuously refined to support public bodies' business strategies and plans and to provide quality and value to the stakeholders.
Rationale	– Continuous improvement in EA processes and technology implementations will lead to reduced costs, improved efficiency and effectiveness and increased confidence in public bodies to provide services securely. – Will align and optimize resources for Information Management and Information & Communication Technologies (IM & ICT) with the needs of the business. – Will increase the effectiveness, quality and value of deployed EA solutions by leveraging common EA assets.
Implications	– Technology must be selected and deployed for its business value, in support of business needs and priorities. – GNB must conduct ongoing assessments of its EA capabilities and offer improvement recommendations. – As technologies change and business requirements evolve, the processes and technologies put in place to protect them must also change to ensure appropriate protection and efficiencies. Without continuous review and management of solutions they become unwieldy, interruptive and costly. – Alignment between IM & ICT and business must be demonstrated through appropriate tools and processes (e.g. plans, architectures, business cases). – Must provide continuous improvement of tools and processes. – Business and IM & ICT alignment must begin at the planning stage. – EA must support GNB's business strategies and plans. – Public bodies may choose to extend the EA to support the unique aspects of their business. – As EA assets are business enablers, an "investment" view rather than a "cost" view must be taken in budgeting or funding. – Must provide an effective process for deployment and usage of EA Program Compliance.

	3. Compliance
Statement	EA and Information Assurance initiatives and activities must comply with all relevant and established principles, laws, regulations, and policies.
Rationale	– EA and Information Assurance initiatives and activities will enable public bodies to operate in a balance that meets their goals while maintaining an appropriately secure environment that complies with relevant legal, regulatory, and policy requirements. – Delivery of services to citizens and other entities in line with government strategies is imperative. Information Assurance enables such delivery while protecting both the citizen and the public body by ensuring that statutory obligations are met, and civil or criminal penalties are avoided.
Implications	– EA assets must comply with laws, regulations, and policies. This will not preclude business process improvements that lead to changes in policies and regulations, and which may lead to changes in processes or applications. – A foundational aspect of Information Assurance is availability of information when and where it is needed. EA's role must be to allow access to information for the intended audiences while not allowing data to become available in contravention to legal or contractual obligations. A balance between both these requirements must be maintained. – Government must meet both protection of privacy and access to information requirements established in legislation. – Education must be provided on the relevant laws, regulations, and policies.

	4. Standardization, Harmonization, and Normalization
Statement	The EA environment is standardized, harmonized, and normalized with respect to processes, technological diversity, information, data definitions, security, and all other EA components and assets.
Rationale	– This principle supports interoperability and quality information. – Common architectural assets across the enterprise bring the benefits of economies of scale to the government. – Standard processes are repeatable, predictable, scalable, and more efficient. – Process standardization will help GNB comply with certain legislation and quality standards. – It is easier to focus attention, resources, knowledge, and investments in a standardized environment. – Technical administration and support costs are better controlled when limited resources can focus on this shared set of technology. – Common vocabulary and definitions will enable clearer communication and understanding of issues. – Common components are easier to manage when they can be consolidated at fewer locations.
Implications	– IM & ICT solutions must be designed to minimize functionality overlaps. – IM & ICT solutions must be reused where possible. – Concessions may be needed in user requirements. – The government must establish an initial common vocabulary for business and EA and the definitions will be used uniformly throughout the government. – Must formally manage the common vocabulary as a registry function. – Standardization initiatives must have a clear governance model. – Development of enterprise-wide applications is preferred over the development of similar or duplicate applications which are only intended for a single organization. – The preferred decision-making sequence for IM & ICT capabilities delivery is reuse, buy, build.

	5. Sharing and Integrating EA assets*
Statement	EA assets must be shared, when appropriate, across public bodies and must have a clear ownership. EA artifacts, whether developed by public bodies or acquired from other sources, must be properly integrated to enable sharing.
Rationale	– In the long term, sharing leads to government information being made available on a timelier basis.
Implications	– This principle supports Interoperability, Standardization, Harmonization, and Normalization. – In acquiring or developing new EA artifacts, public bodies must weigh uniformity and ability to integrate versus individual 'best of breed' capabilities. – Reliable inventory of reusable EA artifacts must be managed formally and be available to all stakeholders. – Infrastructure to support reuse must be in place.

** Please refer to the Glossary section*

	6. Interoperability
Statement	EA assets must, where possible, leverage defined standards that promote interoperability for data, application, and technology.
Rationale	– Standards for interoperability help ensure support from multiple vendors for their products, and facilitate supply chain integration.
Implications	– Interoperability must facilitate information sharing and exchange. – Interoperability, open, and industry standards must be followed unless there is a compelling business reason to implement a non-standard solution. – Defined and approved standards must be selected, following the sequence of international, regional, national, and organizational standards. – Support for open standards is a necessary criterion in the acquisition of IM & ICT solutions. – Existing custom built Application interfaces must be wrapped as web service components and quickly be converted into standards-based re-usable SOA artifacts, where appropriate. – Applications must become independent of specific technology choices and operate on a variety of technology platforms.

	7. Information Quality is Everybody's Business
Statement	GNB must adopt an information quality* culture where clear definition, correct value(s), **and understandable presentation matters**. Public bodies require quality information to make decisions to accomplish business objectives which affect stakeholders.
Rationale	– **This principle enables information readiness (as described in Principle 2).** – Having quality information supports better decision making. Relevant, timely, and quality information is critical to accurate and timely decisions. – Having no defects in information conforms to lean six sigma best practice**.**
Implications	– Educate stakeholders to ensure that they understand the value of this cultural change. – Every stakeholder must be responsible for information quality. – Information must be captured and stored once electronically and validated as close to the source as possible. – Information standards must be developed and enforced. – Standards for controlled vocabularies must be developed and enforced. – Standards for presentation of information must be developed and enforced. – An enterprise metadata registry must be developed to communicate and facilitate reuse in all types of applications, and to improve the management of information quality. – Quality control measures must be implemented to ensure the integrity of the information. – An information quality environment must be established following a quality system (e.g. Total Information Quality Management (TIQM)).

** Please refer to the Glossary section*

	8. Information is a Valuable Enterprise Asset
Statement	Information is an asset that has value to the enterprise and must be managed accordingly.
Rationale	– Information is a valuable enterprise resource. It has real, measurable value. – Management of information is legislated. – Information management ensures that we know where the right information is and can obtain it when and where we need it. – This principle supports “Business and Information Readiness Enabler”, “Discoverability and Accessibility of Information”, and “Information Quality is Everybody's Business”. – There is a cost and risk associated to poor quality information.
Implications	– Most enterprise assets are carefully managed, and information is an enterprise asset. – Care must be taken to treat information like any other asset by ensuring adequate quality, security, integrity, protection, availability, understanding, effective use, and disposition. – Must educate the enterprise stakeholders to understand the relationship between management of information, value of information, sharing of information, and accessibility to information. – There must be a cultural transition from "data ownership" thinking to "information stewardship" thinking. – Information governance must be implemented under the directions of government senior executives as the top information governance body, in the same way that there is a top governance body for financial management, business performance management, and human resources management. – Information management should be simplified. Consistent processes must be developed, approved, and communicated. – An enterprise information governance policy as well as service-level agreements must be developed to support the appropriate quality and use of information in business and IM & ICT processes. – All information assets must be identified and categorized as core, enterprise or business assets. Their management must be mandated at the enterprise or organizational level and must also be assessed for value and prioritized accordingly. – Information stewards must be appointed to manage information assets. – There must be a mechanism to identify, document, and analyze information complaint issues including information quality. – There must be a reliable mechanism to impose sanctions for noncompliance with fair information management practices. – The format in which information is passed from one system to another must be consistent across the enterprise. – Information must be captured once and stored once, as an authoritative source. – Managed replication of information must be allowed when it is proven necessary for response time, availability, security, or ease-of-use. – Information must be encapsulated by application(s) or service(s) responsible for managing the data integrity. All updates to that information must be through the encapsulating application(s) or service(s). – Eventually, all shareable data must be stored in an appropriate repository or registry and managed by “Made-for-Purpose”* management systems, and must be standardized. – Emails, documents, and collaboration environments must use a master records repository

	and must be managed by a records management system. – Related metadata (e.g. workflow and audit information) must be stored with the relevant information in the appropriate repository via the appropriate system. – Web content applications (publishing on the Web and intranets) and “Open Government Data”* must use a published environment and not an operational environment. – Since many legacy systems are still in place: • mass changes to make data consistent is impractical and costly. Therefore, the inconsistency must be controlled centrally and actively reduced over time. • to prepare for the “Information Age”*, management of information must move to using the “Information-Centric”* and “Customer-Centric”* approaches.

** Please refer to the Glossary section*

	9. Discoverability and Accessibility of Information
Statement	Information is easily discoverable, accessible, and understood.
Rationale	– Enterprise access to information leads to efficiency and effectiveness in decision-making, and affords timely response to information requests and service delivery. – Staff time is saved and consistency of information is improved. – If integrity of data is questionable, all conclusions reached on retrieved data is in question.
Implications	– Information must be considered from an enterprise perspective to allow access by a wide variety of users. – Discoverability and access to appropriate information must be simplified and consistent processes must be developed, approved, and communicated. – Discoverability and access to appropriate information must meet sharing and exchange of information requirements, such as customer service, reporting, analytics, and forecasting (business intelligence) requirements. – Will require a consistent mechanism(s) to discover, search, access, and present information using a “common look and feel”. For example, reporting, analytics and forecasting (business intelligence), enterprise search engine, enterprise discovery engine, enterprise taxonomy management engine, and auto-categorization engine (consistent tagging of information). Management of these mechanisms must be resourced accordingly. – Information access and information display must be sufficiently adaptable to meet a wide range of stakeholders (e.g. persons with disabilities) and their corresponding methods of access. – Educate the stakeholders on ending the prevailing culture of information ownership and accepting the new culture of information access and user access rights. – Access to information must be granted to users/programs, and systems at the lowest privilege level possible that allows completion of the workflow.

	10. Service Orientation
Statement	All architectures are based on a design of services which mirror real-world business activities comprising the enterprise business processes.
Rationale	– Service orientation delivers agility and Boundaryless Information Flow*.
Implications	– Service representation is defined by using business processes, rules, policies, service interfaces, and service components related to a specific common business function. – Services are implemented by using service orchestration. – Apply service-orientation results in units of software partitioned into operational capabilities, each designed to solve an individual need/problem. – Service orientation places unique requirements on the infrastructure, and implementations must use open standards to realize interoperability and location transparency.

** Please refer to the TOGAF® Glossary*

	11. Robust, Reliable, Accepted, Supported, and Sustainable Technology
Statement	GNB will adopt new technologies that: – are demonstrably robust and reliable; – have broad industry acceptance; – have committed available support; – are appropriate for the business needs; and – are sustainable.
Rationale	– Lower the risk of introducing new technologies. – Reduce time and cost to deliver and maintain IM & ICT solutions. – Reduce frequent changes to IT infrastructure. – Allows GNB to develop or acquire narrower and deeper technology skills (rather than broader and shallower).
Implications	– Criteria must be defined for robustness, reliability, industry acceptance, committed support, appropriate for the business needs, and sustainability. – Means of ensuring compliance to criteria must be defined. – This principle does not imply that GNB will not be innovative in its use of technology, but it does mean that GNB will be pragmatic.

	12. Risk-based Mitigation
Statement	GNB will use a risk-based treatment approach to ensure consistent and effective mitigation programs while maintaining the capability to address the risk to any particular data using multiple complementary techniques (Defence in Depth*).
Rationale	– Implementing assurance solutions via a standardized approach based on "Data Classification and Loss Expectancy"* ensures that risk is treated in an effective manner consistent with enterprise strategy and within budgetary goals. – Any given information assurance technique (people, process, technology) will encounter failure and allow for non-compliant use or access. By using multiple complementary techniques the risk of failure in one mitigates the impact to the data being protected. Such combination of techniques and the amount used shall be based on outcomes of a Threat and Risk Assessment (TRA)*.
Implications	– Implementing security controls or other assurance mechanisms without proper risk evaluation can lead to overprovisioning of the control, potentially exceeding project budgets and forcing overly onerous requirements on the end user or business. While it is sometimes more efficient to apply a control in a blanket fashion, it is generally better to assess the sensitivity of the data involved and protect it accordingly. – Reliance on one technique to protect data will inevitably lead to compromised data when the technique is corrupted.

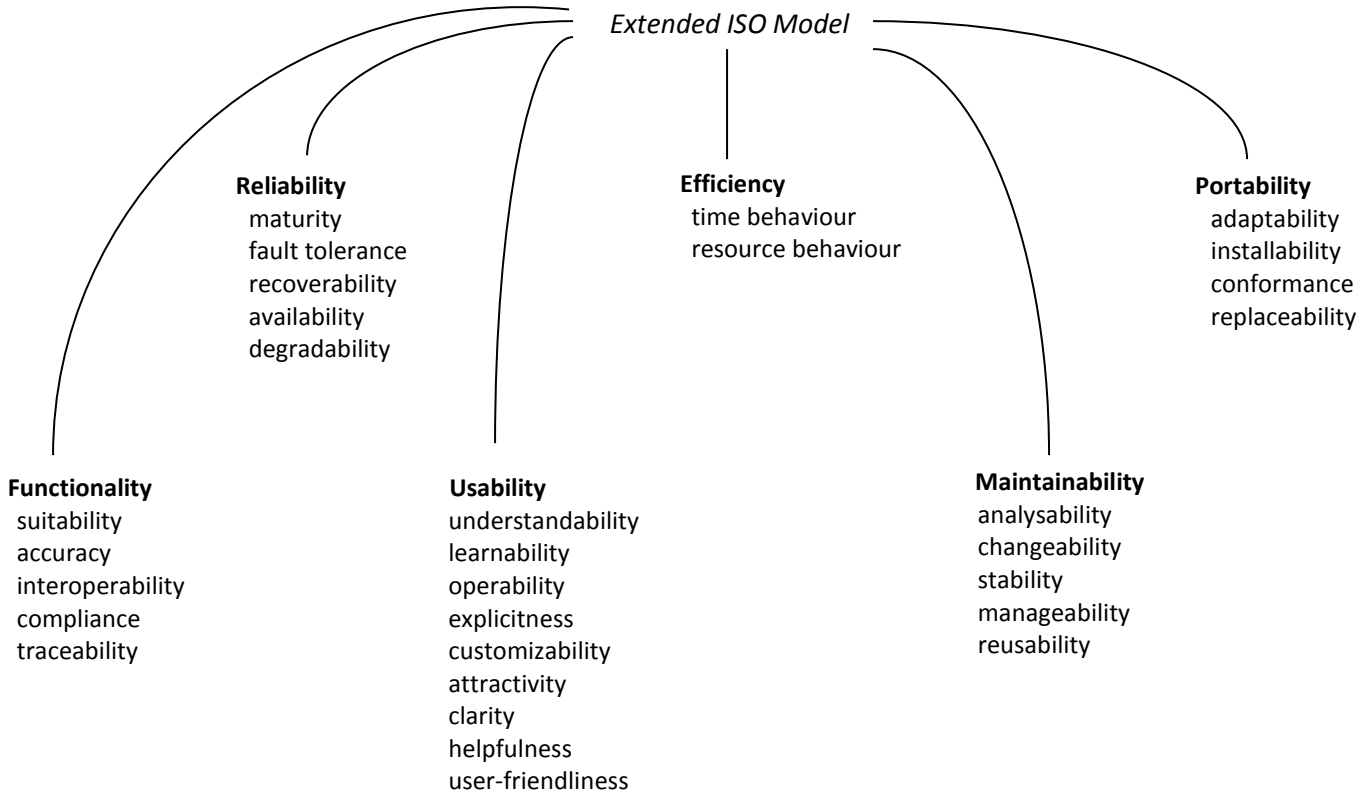
** Please refer to the Glossary section*

Quality Attributes, Extended ISO 9126 Model[21]

ISO 9126 provides a set of quality attributes. These quality attributes are originally focused on software quality; however, they are fairly applicable to other architecture domains, as explained below.

In the EA context, the business architecture revolves around organizational aspects such as products [or services], processes, and people.

Functionality can be seen as the extent to which useful functions are provided to the organization and its clients.
Reliability is the extent to which the functions are provided when needed.
Usability is the extent to which the functions are friendly to employees and customers.
Efficiency is the extent to which resources (people, money, and time) are used efficiently in providing the functions.
Maintainability is the extent to which changes can easily be made to the functions.
Portability is the extent to which the functions are independent of organizational changes, such as outsourcing.



[21] "Architecture Principles, The cornerstones of Enterprise Architecture", Danny Greeghorst & Erik Proper, 2011 (Sringer), p. 68

The following are the original definitions for these attributes:

Functionality: a set of attributes that bear on the existence of a set of functions and their specified properties. The functions are those that satisfy stated or implied needs.
Reliability: a set of attributes that bear on the capability of software to maintain its level of performance under stated conditions for a stated period of time.
Usability: a set of attributes that bear on the effort needed for use, and on the individual assessment of such use, by a stated or implied set of users.
Efficiency: a set of attributes that bear on the relationship between the level of performance of the software and the amount of resources used, under stated conditions.
Maintainability: a set of attributes that bear on the effort needed to make specified modifications.
Portability: a set of attributes that bear on the ability of software to be transferred from one environment to another.

Appendix E: EA Vision[22]

Information Readiness Enabler

Delivering relevant, timely, and quality information

As GNB matures its newly launched Enterprise Architecture Program, it will focus on creating technical efficiencies from the way it runs its IT. This will in turn start to affect business efficiencies by growing the amount of services IT can offer business users. As we continue to mature, GNB will begin to reap the benefits of efficiencies (time, cost, resources) and be able to reinvest in business transformative initiatives brought on by more effectiveness toward our desired end state.

All Architecture

Improving architecture foundation to enable information readiness

In order to deliver relevant, timely, and quality information, GNB is establishing its EA Program by putting in place an EA Governance Framework that encompasses all four parts of the government, an EA Repository accessible to all GNB and specifically to the EA community as a focal point for all enterprise architecture assets including business processes, and an EA Framework adopted from The Open Group Architecture Framework (TOGAF®).

[22] The content of this appendix provided by the OCIO-EAPO chief strategists.

Information Architecture

Enterprise information architecture (EIA) designs outcomes to drive the information-sharing strategy across the organization, leading to the development of the semantically interoperable, compliant, and trusted enterprise information infrastructure. EIA aims at removing the silos of information and integrating applications, while satisfying business requirements.

There are 5 levels of maturity for information "use":

1. Data to run the business (focus on data and reporting);
2. Information to manage the business (basic information interaction);
3. Information as a strategic asset (information in business context);
4. Information to enable innovation (information enabled business innovation);
5. Information as a competitive differentiator (adaptive business performance).

GNB public bodies can be assessed at level 1 or 2.

Improving access to information for decision making purposes

Business Intelligence (BI)

"Business Intelligence is the capability of the organization to explain, plan, predict, solve problems, think in an abstract way, understand, invent, and learn in order to increase organizational knowledge, provide information to the decision process, enable effective actions, and support establishing and achieving business goals." [23]

In government, the need for better BI is evident. The Government Renewal (GR) Plan refers to three urgent needs:

- Financial Accountability;
- Corporate Human Resource Planning; and
- ODH-1236 Health Analytics.

Forty business applications with BI capabilities have been identified in Part I alone and could leverage a common platform. The use of MS Excel and MS SharePoint has exploded in GNB public bodies to fill the gap of producing required reports.

Business Intelligence (BI) Strategy and Framework

GNB enterprise and public bodies have a wide variety of requirements. Therefore there is a need for a BI strategy and framework for using a portfolio of BI solutions. Examples of such solutions are:

[23] Overview of Business Intelligence Maturity Models, Irena Hribar Rajterič, 2010

- traditional reporting, self-service BI and dashboards;
- discovery solutions and best-of-breed tools for such needs as financials, human resources; and
- analytical and forecasting tools for special analysis.

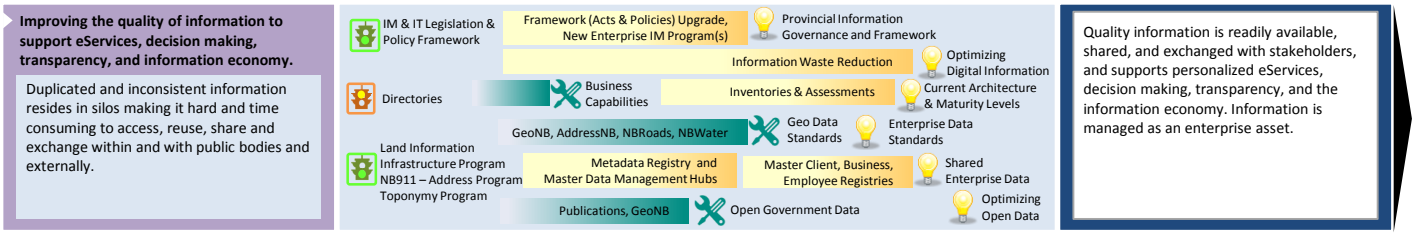
BI Competency Centre

GNB public bodies could use a BI competency centre to evaluate which BI solution will meet their requirements and perform tests with real program data.

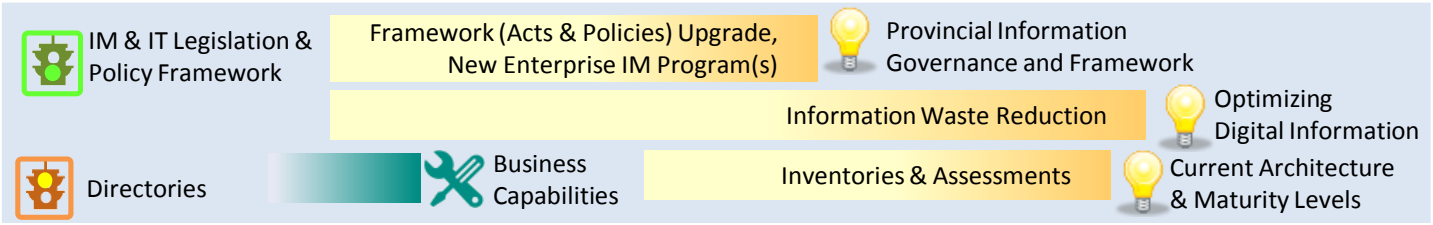
Optimizing BI, Analytics & Forecasting

Once the enterprise information is standardized, high performance enterprise data warehouses and matured BI can be achieved to provide quality, relevant, and timely information to the decision making processes. This will enable effective actions and support establishing and achieving business goals as repetitive processes.

Improving the quality of information to support eServices, decision making, transparency, and information economy



Information Management



Provincial Information Governance and Framework

There is a need to upgrade the existing framework of acts and policies, to support Information Readiness, data sharing, data quality, and to prepare for the Information Age. The governance needs simplification and the rules need to be demystified. Today, there are about fifteen (15) acts that affect the management of information, from privacy, official languages, health information, electronic transaction, evidence, and archives and many policies including security, privacy, records management, email.

Information today is not managed as an enterprise asset. An Enterprise Information Management (EIM) program is non-existent. Such a program would establish itself as a core, invaluable enabler and provider of

corporate/shared services for information and business needs for government public bodies to operate as one enterprise more effectively internally and globally.[24]

Currently, GNB has programs to manage the information lifecycle, privacy, security, data centre, web content and information architecture. However, there are few programs at the enterprise level, and no corporate/shared program(s) currently exist(s) to manage business intelligence, portals, search, mobile apps, workflow, metadata and taxonomy, governance, data warehousing, master data, data quality improvement, enterprise collaboration, etc.

Optimizing Digital Information

There is a need to reduce the volume of information in all GNB public bodies. Such an exercise is called Information Waste Reduction, Information Governance or Defensible Disposal in the industry.

- Gartner reported that 90% of data is either stale or of non-business value.[25]
- Cisco saved $12M by eliminating information waste in eighteen (18) months.[26]
- After a large legal case, DuPont estimated that it cost $12M to have attorneys review all additional documents that were kept past their established retention period.[27]
- US Government Accountability Office (GAO) achieved 92% accuracy in automatic tagging/categorization effectiveness. Information is now more easily discoverable.

The challenge clearly lies with utilizing effective tools for intelligent information management[28]. The following activities could be done:

- deletion of content: emails, collaboration, business applications, and records based on retention schedules;
- deletion of duplicate information;
- deletion of business applications and data with no value;
- move the 90 business applications performing correspondence tracking, invoice tracking, etc. and associated information to an enterprise repository and retire these applications; and
- implementation of intelligent tools.

An Information Waste Reduction initiative could also manage all “Request for Information” in public bodies. This means that “Information requests from the public, Auditor General and/or Comptroller” as mentioned in the Government Renewal Plan could be addressed by this initiative.

GNB public bodies would then be able to make their significant digital information semantically organized, trusted, legally compliant, standards compliant, exchangeable and re-useable.

[24] Gartner Research Inc.
[25] KM World, September 2011
[26] Gartner Research Inc., 2012
[27] KM World, September 2011
[28] Intelligent information management tools such as taxonomy management, document and records management, auto-classification, enterprise search

Business Capabilities

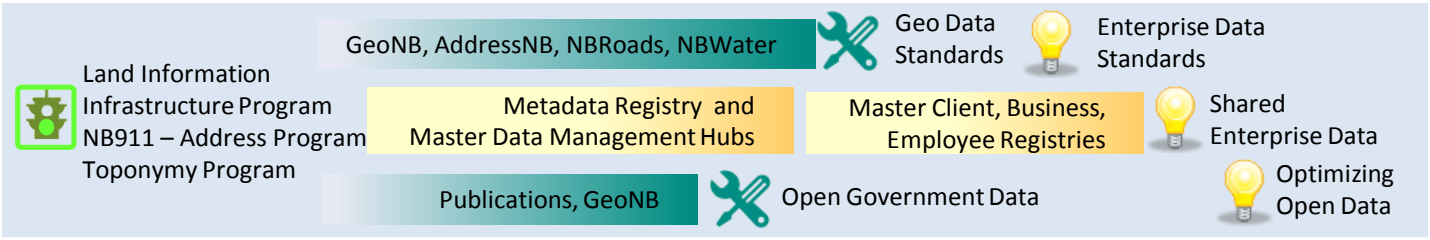
All GNB public bodies' business functions, information and services should be categorized according to the appropriate business capabilities. This way, the business capability can be analyzed and appropriate metrics can be established and monitored. Similar capabilities (throughout all GNB public bodies) can then be transformed as a whole to be more effective and efficient. Appropriate enterprise information requirements, reporting and analytics for the capability can then be achieved.

Current Architecture & Maturity Levels

Inventories are necessary to gain knowledge of business information and applications that currently exist in public bodies is necessary in order to develop strategies. Assessments would be done to identify:

- business applications that have no value;
- business applications that could be replaced by implementing an EDRMS[29]. Ninety (90) were previously identified for Part I alone. Likely higher since MS SharePoint is widely used;
- reporting tools that could be replaced by implementing a business intelligence framework. Forty (40) were previously identified;
- duplicate information that should be managed as "enterprise information assets", and assessment of business applications that perform registration process. There were 125 previously identified.
- information that could be shared externally, to communities of interest, to the public, etc. as "Open Government Data";
- the status of using data standards based on international and national standards.

Enterprise Data Sharing and Information Economy



New Brunswick citizens and businesses must be able to use GNB information to become smarter, healthier, unified, and world leaders in both the economic and political fronts. GNB must make its information available in multiple languages to support investors and immigrants.

Geo Data Standards

Currently Service New Brunswick is leading the GeoNB project with major stakeholders the departments of Natural Resources and Public Safety. These standards are international and national. New Brunswick geo

[29] EDRMS = Enterprise document and records management solution

data is open for the private sector to reuse in the InfoEconomy. Eventually more geographic data layers will be made available.

Enterprise Data Standards

Lack of adoption of semantic interoperability means higher costs and higher errors in data meanings and exchange, and less opportunities. Over US$100 billion per year is lost because of the lack of a widely used semantic interoperability standard in the US alone.

Every discipline has standards: transportation, construction, health, etc. Over 700 data standards from over 40 authoritative bodies have been found for business, information and data. GNB needs to start now to work towards establishing semantic interoperability standards. A standards program must be established and resourced[30], and enterprise registries are required to ease the reusability of components in business applications.

Shared Enterprise Data

Shared and trusted enterprise data is accomplished with the implementation of an enterprise metadata registry and of master data for such things as clients, businesses, employees, locations, products, etc.

According to the MDM institute, master data management is “the authoritative, reliable foundation for data used across many applications and constituencies with the goal to provide a single view of the truth no matter where it lies.” An MDM hub promotes standardization and harmonization of applications and information assets in order to maximize reuse, efficiency, effectiveness, and value to the organization.

There should be mechanisms by which government reduces the service delivery inefficiencies to customers (including business and employees). These registries are candidates for the master data management (MDM) hub. For instance, customer profiles would be accessible from a client registry for reuse in electronic forms and for accessing eServices. It would allow for viewing all interactions with a customer.

Open Government Data

Open Government Data[31] is defined as “public data which is complete, primary, timely, accessible, machine processable, non-discriminatory, non-proprietary, license-free, and when compliance is reviewable.”

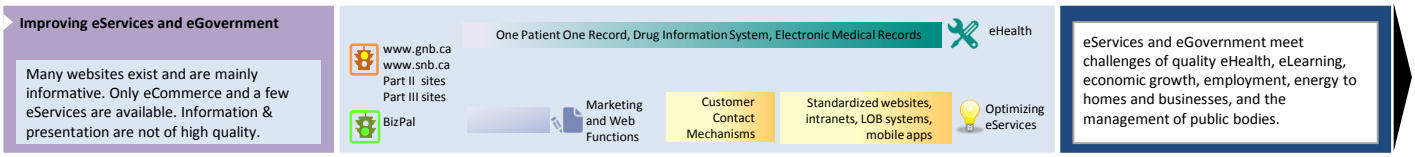
Currently, GNB’s websites offer publications, reports, audios, videos, etc. This can be assessed at maturity level 1-2. Even when more is added to the collection, it will remain at maturity 1-2, since the data does not meet the above definition. In European Union (EU), re-use of Public Sector Information (PSI) is expected to bring more than $100 billion economic value to the EU.

[30] GNB’s Apprenticeship and Occupational Certification (Branch) of the department PETL has seven (7) employees.
[31] http://www.opengovdata.org/

Optimizing Open Data

It is difficult to imagine what the Information Age and the Information Economy will be in 10 to 20 years. Currently, Canada is still working towards objectives from 1999[32], such as customs and taxation, global uniform commercial code, privacy and consumer protection, security and encryption, technical standards and interoperability and electronic payment systems and financial institutions. In 2009, new directions and principles were developed[33].

Improving eServices and eGovernment



Raise the Standard of eServices to the Home, Businesses and Public Bodies

eHealth

The implementation of Electronic Medical Records (EMR) integrated with One Patient, One Record (OPOR) and Drug Information System (DIS) will create unprecedented accuracy, relevancy, availability and therefore quality information to all stakeholders of the health care system. OPOR uses a master data management technology from IBM (Initiate) to manage patient information from their various sources of information.

Marketing and Web Functions

The Government Renewal Plan has identified that policies are to be written to describe the functions requirements for marketing and web[34].

Customer Contact Mechanism

The Government Renewal Plan has identified the fact that the mechanisms by which customers are contacted should be standardized with the same quality, whether by phone, SNB TeleServices, or the Web throughout all public bodies.

[32] Working paper for the *African Development Forum '99,* 24-28 October 1999, United Nations Conference Centre
[33] Building the Global Information Society, Nomura Research Institute (2009)
[34] ECO, Corporate Communications

Standardized Websites, Intranets, LOB Systems, Mobile Apps

There is an opportunity to reuse the current web content management (WCM) platform across GNB public bodies (www.gnb.ca, www.snb.ca, Part II websites, Part III websites, all intranets, all line of business (LOB) systems, and mobile apps). Standards for the Web, accessibility, branding, presentation, metadata, taxonomies, search engine, navigation, etc. should be adopted, developed, and reused. The WCM platform can be extended for eCommerce, eForms, Client Registry, etc.

Optimizing eServices

GNB is aiming to raise the standard of its eServices to meet the challenges of quality eHealth, eLearning, economic growth, employment and energy to the home and businesses, and also to meet the challenges for the management of GNB public bodies.

Application Architecture

The Roadmap defines the critical application architecture evolution that needs to take place in order to transform our existing silo and disjointed application environment into one that:

- guides Government Renewal Program;
- enables development of more agile and cost efficient business processes;
- improves secure information sharing;
- increases return on assets from past it investments;
- supports shared services initiatives; and
- reuses and only develops functionality that the enterprise does not have (PwC 2011 report).

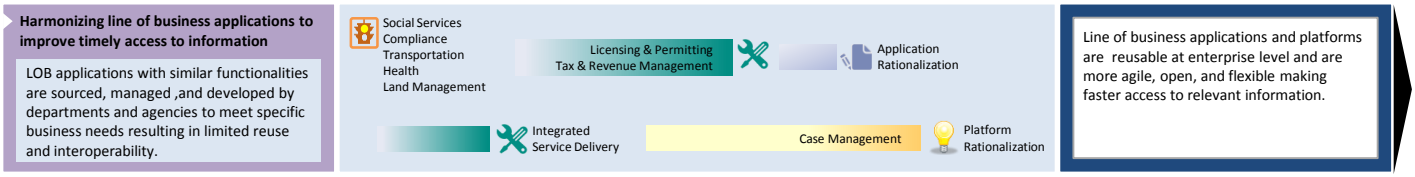
Adoption of Service Oriented Architecture and stakeholder engagement are crucial success factors for this transformational journey.

The Government of New Brunswick recognizes that it must continually evolve its business services to respond to the changing needs of its citizenry. However, as with most organizations, GNB's large and diverse embedded technology base is acting as an impediment to business transformation. The existing GNB application environment cannot meet government's renewal and transformation demands. The uncoordinated IT spending that is required to keep the environment running is also placing GNB in a deteriorating position, both technically and financially.

Application rationalization, standardization, modernization and simplification are necessary steps for overhauling the application portfolio and getting Government back on the right technology path.

An overall Government application strategy and portfolio management practice will assist Government in determining its investment posture with regard to particular applications. Based on the technical state and business fit of an application, a decision can then be made on whether to tolerate, invest in, migrate, or eliminate a given application.

Harmonizing line of business applications to improve timely access to information



Business Improvement scenario

Clients can get all their building permits and associated information from a single point of entry as a package service that it provides a well-coordinated fulfillment process from point of entry to completion.

Application Rationalization

Application rationalization reduces costs, redundancies and complexities of GNB's IT landscape via application rationalization activities.

In the current environment, multiple applications and technologies exists for similar business functions. This application sprawl and redundancy of applications has a cascading effect on cost and IT landscape complexity. For instance, Part I currently has:

- 125 separate systems performing a registry functions;
- 39 systems performing HR functions;
- 42 systems for reporting tools;
- 90 systems for document/correspondence management;
- 42 applications that have Accounts Payable functionality; and
- 50 systems that perform some type of Inventory management.

Rationalization will assist government identify, upgrade and eliminate IT assets that deliver low value to the business.

Integrated Service Delivery

Integrated Service Delivery (ISD) is a new approach to the delivery of services and programs to New Brunswick children and youth with emotional-behavioural and mental health issues within the school, family and community context.

Platform Rationalization

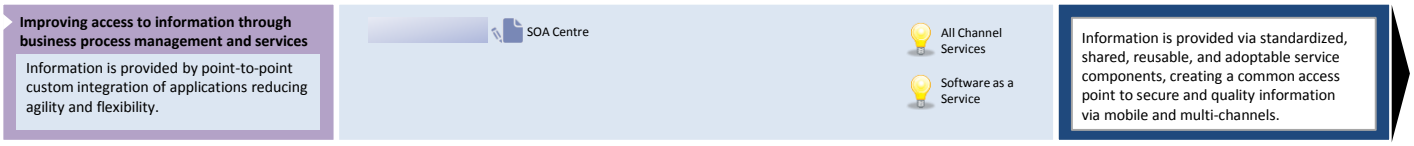
Platform rationalization reduces the total number of assets by consolidating best of breed components, features, and functionalities from multiple existing systems into either a single existing or new system. For

instance, case management workloads currently spread out across many applications can be consolidated into a single case management configurable platform that all clients can use.

Past government IT silo project practices has led GNB to an IT environment of maze of applications and platforms of different ages, sizes, types resulting in an ongoing high maintenance costs.

Industry best practices and recent government reviews indicate that significant savings and efficiencies can be achieved by platform rationalization. (i.e. running existing IT process and functionality on fewer platforms will result in significant reductions of software and hardware licensing and operating costs).

Improving access to information through business process management and services



Business Improvement scenario

Citizens can receive government services via their choice of access channel and with equivalent client experience and satisfaction. A citizen can renew his Motor Vehicle registration over the counter, via the web or mobile devices etc. with equal service quality.

Service Oriented Architecture

The target application architecture is based on Service Oriented Architecture (SOA). SOA is a design paradigm used to construct business driven information systems composed of independent, reusable, and reconfigurable IT components. The use of an SOA approach can lead to more agile and cost efficient business processes and thus can help guide the government renewal initiative. Other benefits of SOA include improved information sharing, increased return on assets from past IT investments, and better support for the shared services initiative.

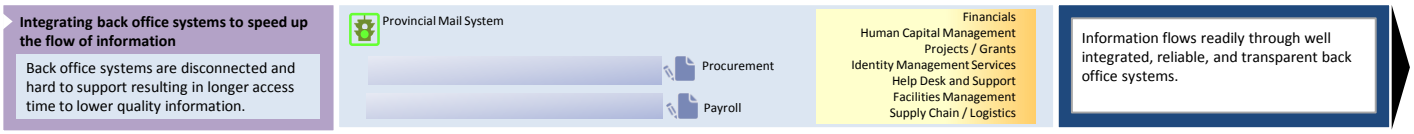
Software as a Service

SOA can assist GNB in implementing a secure cloud computing environment where Software as a Service (SaaS) can be hosted and provided externally by private sector and internally by a specific agency.

All channel services

Government services can be made available and easily accessible via all delivery channels, such as Web, over the counter, mobile, etc.

Integrating back office systems to speed up the flow of information



Business Improvement scenario

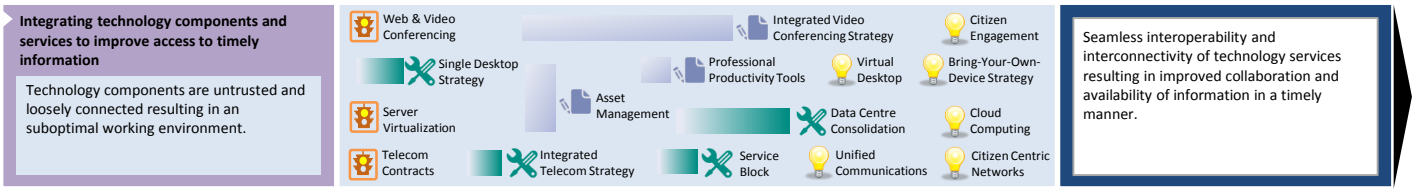
Improved self-service and personalization of services to internal government employees which equates to more efficient work force and therefore more time spend on government front line of business that results to improvements of citizen and business services. Doing more with less.

Back office enterprise systems

Back office processes and functions can be provided via enterprise systems that are architected to meet all client needs and are run by a single shared services agency. The Procurement and Payroll initiatives that are presently under way are two good examples of those opportunities. The SOA infrastructure will assist in providing dynamically and on demand necessary information or functionality to other government LOB applications that might require such services in order to complete or fulfill line of business transactions. (e.g. Oracle Financials can become the master database for all financial information and its data and financial processing can be accessed and re-used by other LOB applications via exposed Oracle Financials web services. The same design principles can be applied to all required back office corporate application processing needs).

Technology Architecture

Integrating technology components and services to improve access to timely information



As depicted above, four major infrastructure areas need to be matured across Government to help the business get access to information in a timely manner. Todays “ad-hoc” (Level 1) approach to technology procurement, planning and use represents a low level of maturity. By implementing an Enterprise Architecture (EA) program that can touch all public bodies, the appropriate level of governance, process improvement, and planning can be applied to help GNB mature towards an “optimized” (Level 5) infrastructure. In doing this GNB’s infrastructure will evolve to better enable communication, collaboration and efficiencies between all public bodies.

A matured approach that is used across GNB will facilitate the use of industry best practices such as: having access to the right tools, virtualization, data centre consolidation, and integrated telecommunications. All of which will enable GNB to build on efficiencies and gain cost savings.

Longer term goals such as cloud computing and possibly a Bring-Your-Own-Device (BYOD) strategy can be considered, evaluated, planned, and potentially implemented as to gain even more flexibly, efficiencies, and cost savings.

Connectivity: The contracts, networks, and devices to manage and connect the different parts of GNB

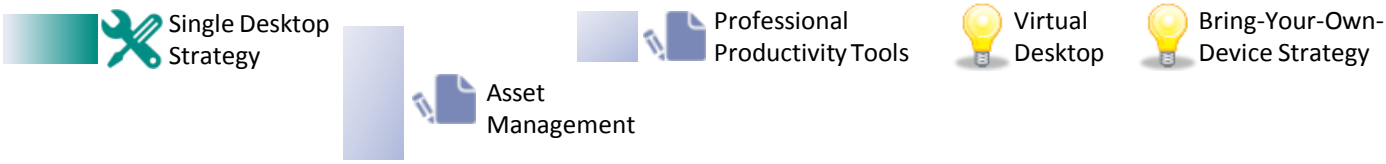
This area represents the migration of network connectivity from the decentralized approach of today towards an integrated telecom strategy that can be used by all public bodies. Progressing along this maturity scale will allow immediate cost savings from procurement efficiencies and would help to eliminate duplication, but also build a foundation level of connectivity that furthers many other GNB initiatives. A mature connectivity infrastructure can be used to further work in Unified Communication, and can be the foundation for Citizen Centric Networks to be used in education, healthcare and Smart Grid initiatives.
“Leverage our investments in the future for high value services such as education, health care and Smart Grid”

Backend: The servers, storage, process and tools to manage a backend infrastructure

Once a mature robust foundation connectivity layer exists, the backend server and data centre infrastructure can be considered. Mature approaches around server virtualization can be applied and the associated cost savings realized. This virtualization capability is the catalyst that enables enterprise-wide data centre consolidation and can allow GNB to realize potential savings. The next logical extension to this is to look to the concept of cloud computing for savings. Using the "cloud", in essence off site private data centres, removes the burden of managing and operating large amounts of infrastructure and its associated costs. Cloud computing not only relies on GNB having its own robust network infrastructure for connectivity, but requires highly robust interconnections with service providers and mature SLA management before the true value of the "cloud" can be realized.

"A well architected environment that can be leveraged for future potential cost savings approaches such as *cloud*"

Endpoints: Client devices such as laptops, desktops, tablets and the associated tools and management process



New end user devices continue to enter the consumer and professional market. This graphic shows a maturing of procurement and policy where GNB employees get access to the right end user devices, but in a controlled, managed and cost effective way. A mature approach to this area will logically include proper planning for, and procurement of the foundation technologies such as: tablet computers, and investments in desktop virtualization technologies that act as a layer of abstraction thereby possibly allowing GNB to gain flexibility and cost savings in evolving strategies such as Bring-Your-Own-Device (BYOD).

"A well architected environment that can be virtualized to facilitate future potential cost savings approaches such as Bring-Your-Own-Devices (BYOD)"

Collaboration: Enabling electronic collaboration

As mentioned before, once Connectivity has been matured and a robust foundation network layer exists between all public bodies, value add services such as web and video conferencing can be considered, better planned and rolled out as an integrated video conferencing strategy.

"A well architected environment can be leveraged for future high value services such as electronic citizen engagement"

Capability Maturity Model

Determine Technological Direction

Management of the process of *Determine Technological Direction* that satisfies the business requirements for IT of *having stable, cost-effective, integrated and standard application systems, resources and capabilities that meet current and future business requirements* is

0 Non-existent when
There is no awareness of the importance of technology infrastructure planning for the entity. The knowledge and expertise necessary to develop such a technology infrastructure plan do not exist. There is a lack of understanding that planning for technological change is critical to effectively allocate resources.

1 Initial/Ad Hoc when
Management recognises the need for technology infrastructure planning. Technology component developments and emerging technology implementations are ad hoc and isolated. There is a reactive and operationally focused approach to infrastructure planning. Technology directions are driven by the often contradictory product evolution plans of hardware, systems software and applications software vendors. Communication of the potential impact of changes in technology is inconsistent.

2 Repeatable but Intuitive when
The need for and importance of technology planning are communicated. Planning is tactical and focused on generating solutions to technical problems, rather than on the use of technology to meet business needs. Evaluation of technological changes is left to different individuals who follow intuitive, but similar, processes. People obtain their skills in technology planning through hands-on learning and repeated application of techniques. Common techniques and standards are emerging for the development of infrastructure components.

3 Defined when
Management is aware of the importance of the technology infrastructure plan. The technology infrastructure plan development process is reasonably sound and aligned with the IT strategic plan. There is a defined, documented and well-communicated technology infrastructure plan, but it is inconsistently applied. The technology infrastructure direction includes an understanding of where the organisation wants to lead or lag in the use of technology, based on risks and alignment with the organisation's strategy. Key vendors are selected based on the understanding of their long-term technology and product development plans, consistent with the organisation's direction. Formal training and communication of roles and responsibilities exist.

4 Managed and Measurable when
Management ensures the development and maintenance of the technology infrastructure plan. IT staff members have the expertise and skills necessary to develop a technology infrastructure plan. The potential impact of changing and emerging technologies is taken into account. Management can identify deviations from the plan and anticipate problems. Responsibility for the development and maintenance of a technology infrastructure plan has been assigned. The process of developing the technology infrastructure plan is sophisticated and responsive to change. Internal good practices have been introduced into the process. The human resources strategy is aligned with the technology direction, to ensure that IT staff members can manage technology changes. Migration plans for introducing new technologies are defined. Outsourcing and partnering are being leveraged to access necessary expertise and skills. Management has analysed the acceptance of risk regarding the lead or lag use of technology in developing new business opportunities or operational efficiencies.

5 Optimised when
A research function exists to review emerging and evolving technologies and benchmark the organisation against industry norms. The direction of the technology infrastructure plan is guided by industry and international standards and developments, rather than driven by technology vendors. The potential business impact of technological change is reviewed at senior management levels. There is formal executive approval of new and changed technological directions. The entity has a robust technology infrastructure plan that reflects the business requirements, is responsive and can be modified to reflect changes in the business environment. There is a continuous and enforced process in place to improve the technology infrastructure plan. Industry good practices are extensively used in determining the technological direction.

Security Architecture

Ensuring secure access to government information

Throughout public bodies threats against infrastructure can range through telecommunications, energy, electronic health records, authorization logics, distributed access in the cloud, location privacy, secure network location and design, etc.

As an interconnected member of the Canadian Infrastructure with public and private routes to various partners, our systems are simultaneously at risk from compromise via our partners and at risk of being used as a pathway to attack them.

The Security Architecture strategy is to identify the threats to these various lines of work, measure the risk impact and produce proactive mitigation plans; enabling secure transactions while aligning with budgetary targets.

Cyber Security Strategy

The New Brunswick Cyber Security Strategy will outline the top level issues we face and the steps government is taking to mitigate or aid in mitigation. Several national cyber security strategies, including Canada's have identified Organized Crime, State sanctioned espionage/sabotage and terrorist use of cyberspace as top level threats. To mitigate these issues New Brunswick's strategy will focus on three main areas; internal security of government systems, working co-operatively with FPT partners to ensure open communication and resolution of issues, helping NB citizens and business operate safely in cyberspace.

Information Assurance & Operational Security Standards

The vision is to provide a suite of Information Assurance and Operational Security documentation that provides guidance to public bodies; aiding decision makers to produce consistent, rational outcomes. This is achieved by collaborative work with Federal, Provincial, and Territorial jurisdictions as well as other partners to determine best approaches for Information Assurance and Operational Security Standards creation and review.

Identity & Access Management

Identity validation and administration must take place in an agreed upon and trusted method via a broker or other trusted evaluator such that services allocation processes can be built and used consistently. This is the foundation of the security aspect that follows and provides:

- a lower total cost of ownership through the increased efficiency and consolidation of identification and authorization procedures;
- security improvements that reduce the risk of internal and external attacks;
- greater access to information by partners, employees, and customers, thus leading to increased productivity, satisfaction, and revenue;
- higher levels of regulatory compliance through the implementation of comprehensive security, audit, and access policies; and
- greater business agility during events such as mergers and acquisitions.

Based on the evaluation conducted on the identity, roles can be assigned that allow or disallow access to relevant data as well as manage the ability to Read/Add/Remove/Change that data based on need. This can include time constraints on such access via expiry dates.

When an identity changes status from one group to another it must be tracked and assigned roles must change appropriately. Examples can be transfer of departments internally or a citizen moving to another province within Canada. Further an identity retirement/archive process must exist to handle life events.

Governance, Risk, and Compliance

The vision is to establish a regulatory or internal framework for satisfying governance requirements, evaluate risk across the enterprise and track how the organization complies with the established governance requirements. Then use this information to aid in prioritizing, funding and initiating any corrective actions or new systems required and as input to other management decisions as needed.

This is achieved via threat risk assessment processes of new or significantly changed systems and general IM&ICT policy & standards compliance checks to ensure that GNB is meeting its obligations in regards to legislation, regulations, contracts, strategies and policies.

Security Event Management Center (SEMC)

The vision is to enable public bodies to conduct business in a secure manner by offering consistent overview of threat trends, their impacts and producing mitigation strategies.

This is accomplished by managing the Security Event lifecycle process, through identification, investigation, prioritization, and containment via necessary services and guidance to solve them or support their resolution. To mitigate risks and minimize the number of responses required SEMC also provides preventive services; issuing advisories on vulnerabilities in various systems and on viruses and similar threats. The SEMC also acts as a liaison with Federal, Provincial, Territorial partners and the Intelligence community to ensure that near real-time threat and risk information is available.

Glossary

For the definitions of terms, please refer to the following sources:

- TGOAF® 9.1 Online Manual, Part 1, Chapter 3: Definitions, http://pubs.opengroup.org/architecture/togaf9-doc/arch/
- TGOAF® 9.1 Online Manual, Appendix A: Supplementary Definitions, http://pubs.opengroup.org/architecture/togaf9-doc/arch/
- TOGAF® 9.1 Online Glossary, http://www.opengroup.org/public/arch/p4/glossary/glossary.htm
- TOGAF® 9.1 Translation Glossary: English – French, https://www2.opengroup.org/ogsys/catalog/C127

Supplementary definitions are provided below:

Annual Loss Expectancy (ALE)
The ALE is the total amount of money that the organization will lose in one year if nothing is done to mitigate the risk. This is calculated by multiplying the SLE by the ARO. The ALE provides a value that the organization can work with to budget what it will cost to establish controls or safeguards to prevent this type of damage

Annual Rate of Occurrence (ARO)
The ARO is the number of times that one may reasonably expect the risk to occur during one year.

Business Capability
A Business Capability is a particular ability of a business to achieve a specific purpose or outcome. It describes what the business does that creates value for customers without consideration of who does it or how it is carried out. Capabilities are based on business outcomes, unique in terms of business intent, and unique in terms of information requirements.

Business Capability Model
The Business Capability Model is a hierarchical catalog of capabilities that, taken together, describe what the organization does. Capability Models provide a stable “anchor model” of the business because the fundamental capabilities are less likely to change over time than the processes and applications that implement them.

Business Process
A Business Process represents a sequence of activities that together delivers a specified output. They describe how the business performs, or implements, a particular capability, and how capabilities connect to deliver a desired outcome.

Business Service
A Business Service implements the activities of one or more business processes through a defined service interface. It may, in turn, be implemented by other, more granular services.

Customer-Centric
Customer-Centric, which influences how we create, manage, and present data through websites, mobile applications, raw data sets, and other modes of delivery, and allows us to shape, share and consume information, whenever and however they want it.

Data
Data is the raw material from which information is derived and is the basis for intelligent actions and decisions.

Data Classification (security)
The segregation of data into several levels which each detail how the data must be handle throughout its lifecycle; creation, storage, transmission and destruction.

Directive
Refer to Policy, Directive, Standard

Enterprise Metadata Registry
An enterprise metadata registry is a central location in an organization where metadata definitions are stored and maintained in a controlled method.

Information
Information is data in context. Information is usable data. Information is the meaning of data, so facts become understandable.

Information Age[35]
The Information Age began in the last quarter of the 20th century. The Information Age is a period that is characterized by the ability of individuals to transfer information freely, and to have instant access to information that would have been difficult or impossible to find previously. The idea is linked to the concept of a digital age or digital revolution. The Digital Revolution, also sometimes called the third industrial revolution, is the change from analog mechanical and electronic technology to digital technology. Implicitly, the term also refers to the sweeping changes brought about by digital computing and communication technology. Analogous to the Agricultural Revolution and Industrial Revolution, the Digital Revolution marked the beginning of the Information Age.

Information-Centric
Information-Centric is where “documents” are no longer managed but there are discrete pieces of open data and content that can be tagged, shared, secured, mashed up and presented in the way that is most useful for the consumer of that information.

[35] Wikipedia

Information Quality
Information quality requires quality of three components: clear definition or meaning of data, correct value(s), and understandable presentation (the format represented to a knowledge worker). Lack of quality of any of these three components can cause a business process to fail or a wrong decision to be made. Information is applied data and may be represented as a formula:

Information = f(Data + Definition + Presentation)

From a business perspective, information may be well defined, the values may be accurate, and it may be presented meaningfully, but it still may not be a valuable enterprise resource. Quality information, in and of itself, is useless. But quality information understood by people can lead to value.
Total Quality Management defines Information Quality as "Consistently meeting or exceeding all knowledge workers and end-customer expectations with information, so that knowledge workers can perform their work effectively and contribute to the enterprise mission, and so that customers are successful in conducting business with you and are delighted with the products, services and communications [information] they receive.

Information Security[36]
Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved

Information Security Event[37]
An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant

Information Security Incident[38]
A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

Information Stewardship[39]
Information Stewardship is an information-centric function that is primarily concerned with information delivery, meta-data management, information quality, information timeliness, information redundancy, etc.; in other words, the BI and dashboard side of the fence.
In many ways, Information Stewardship is more challenging than Data Stewardship because of the fluid and rapid pace of changing customer needs and demands driving BI application development and information delivery. Without proper governance - information inaccuracies, information inconsistencies, and information redundancy can quickly grow out of control like a wildfire.
Information Stewardship oversees and governs information visibility, accessibility, usability, consistency, accuracy, integrity, meaningfulness, actionability, timeliness, audit-ability, certification, and overall information quality.
Information Stewardship is primarily concerned with ensuring the integrity of information produced from authoritative data sources and delivered via authoritative BI and dashboard systems, tools,

[36] ISO/IEC 17799:2005
[37] ISO/IEC TR 18044:2004
[38] ISO/IEC TR 18044:2004
[39] http://www.dashboardinsight.com/articles/new-concepts-in-business-intelligence/bi-stewardship-part-one.aspx

applications, and processes. Conversely, information that is derived and disseminated via casual, non-authoritative means (such as spreadsheets and personal data stashes) frequently bypass the "command and control" of the Information Steward, thus creating information chaos within the organization – an all too common occurrence.

Additionally, Information Stewardship is responsible for monitoring usage of reporting, analytical and dashboard applications, and taking positive actions to retire obsolete or unused content, applications and metrics. Keeping information clutter to a minimum is also a core Information Stewardship function.

Please refer to the following white paper for more details on information stewardship:
http://iaidq.org/publications/doc2/english-2006-11-information-stewardship-white-paper-v3.pdf

"Made-for-Purpose" Management Systems
"Made-for-Purpose" Management Systems are Records Management, Master Data Management, Metadata Data Registry, Taxonomy Management, Digital Assets Management, Content Management, Geographic Information System, e-commerce.

Metadata
The term metadata is ambiguous, as it is used for two fundamentally different concepts. Although the expression "data about data" is often used, it does not apply to both in the same way. Structural metadata, the design and specification of data structures, cannot be about data, because at design time the application contains no data. In this case the correct description would be "data about the containers of data". Descriptive metadata, on the other hand, is about individual instances of application data, the data content. In this case, a useful description would be "data about data content" or "content about content" thus meta-content. Descriptive, Guide and the National Information Standards Organization concept of administrative metadata are all subtypes of meta-content. (Wikipedia)

Open Data Protocol[40]
The Open Data Protocol (OData) is a Web protocol for querying and updating data that provides a way to unlock your data and free it from silos that exist in applications today. OData does this by applying and building upon Web technologies such as HTTP, Atom Publishing Protocol (AtomPub) and JSON to provide access to information from a variety of applications, services, and stores.
OData is consistent with the way the Web works - it makes a deep commitment to URIs for resource identification and commits to an HTTP-based, uniform interface for interacting with those resources (just like the Web). This commitment to core Web principles allows OData to enable a new level of data integration and interoperability across a broad range of clients, servers, services, and tools.
OData enables the creation of REST-based data services, which allow resources, identified using Uniform Resource Identifiers (URIs) and defined in a data model, to be published and edited by Web clients using simple HTTP messages. This specification defines a set of recommended (but not required) rules for constructing URIs to identify the data and metadata exposed by an OData server as well as a set of reserved URI query string operators, which if accepted by an OData server, MUST be implemented.

[40] http://www.odata.org/

Open Government Data[41]
The principles define open government data as public data which is complete, primary, timely, accessible, machine processable, non-discriminatory, non-proprietary, and license-free, and when compliance is reviewable.

The 8 Principles of Open Government Data:

Government data shall be considered open if the data are made public in a way that complies with the principles below:

1. Data Must Be Complete
   All public data are made available. Data are electronically stored information or recordings, including but not limited to documents, databases, transcripts, and audio/visual recordings. Public data are data that are not subject to valid privacy, security or privilege limitations, as governed by other statutes.

2. Data Must Be Primary
   Data are published as collected at the source, with the finest possible level of granularity, not in aggregate or modified forms.

3. Data Must Be Timely
   Data are made available as quickly as necessary to preserve the value of the data.

4. Data Must Be Accessible
   Data are available to the widest range of users for the widest range of purposes.

5. Data Must Be Machine processable
   Data are reasonably structured to allow automated processing of it.

6. Access Must Be Non-Discriminatory
   Data are available to anyone, with no requirement of registration.

7. Data Formats Must Be Non-Proprietary
   Data are available in a format over which no entity has exclusive control.

8. Data Must Be License-free
   Data are not subject to any copyright, patent, trademark or trade secret regulation. Reasonable privacy, security and privilege restrictions may be allowed as governed by other statutes.

Finally, compliance must be reviewable.
A contact person must be designated to respond to people trying to use the data.

[41] http://www.opengovdata.org/

A contact person must be designated to respond to complaints about violations of the principles.
An administrative or judicial court must have the jurisdiction to review whether the agency has applied these principles appropriately.

Policy, Directive, Standard[42]
Policy is "a high-level overall plan embracing the general goals and acceptable procedures especially of a governmental body". OR "a definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions".

Directive is "something that serves to direct, guide, and usually impel toward an action or goal; especially: an authoritative instrument issued by a high-level body or official".

Standard is "something set up and established by authority as a rule for the measure of quantity, weight, extent, value, or quality".

Policies, directives, and standards all provide directions; however, in the context of GNB they have different direction characteristics, as described in the table below:

	Policy	**Directive**	**Standard or Process**
Authoritative	Strongest – Issued by BoM	In between – issued by CIO	Weakest – agreed upon by standards setting / standards approving body(s)
Update flexibility	Slowest – normally months	As per priority defined by OCIO directors	As new or updated standards or processes are approved by the appropriate standards setting body.
Granularity	Coarsest – high-level	Granularity – should be grouped on common themes	Finest granularity – detail level
Volume of items	Minimal number	Potential for zero to many Directives per Policy is expected	Potential for zero to many standards or processes per directive
Content includes	What, Why	Who, what, When, why	when, Where, How

Public body
Any entity from any parts of the government, including departments, agencies, crown corporations, etc.

Risk[43]
Combination of the probability of an event and its consequence

[42] Merriam Webster Dictionary
[43] ISO/IEC Guide 73:2002

Risk Evaluation[44]
Process of comparing the estimated risk against given risk criteria to determine the significance of the Risk.

Single Loss Expectancy (SLE)
The SLE is the total amount of revenue that is lost from a single occurrence of the risk. It is a monetary amount that is assigned to a single event that represents the organization's potential loss amount if a specific threat exploits a vulnerability.

Standard
Refer to Policy, Directive, Standard

Threat[45]
A potential cause of an unwanted incident, which may result in harm to a system or organization

Threat Risk Assessment (TRA)[46]
Overall process of analyzing applicable threats and risks and producing a risk evaluation

Vulnerability[47]
A weakness of an asset or group of assets that can be exploited by one or more threats

[44] ISO/IEC Guide 73:2002
[45] ISO/IEC 13335-1:2004
[46] ISO/IEC Guide 73:2002
[47] ISO/IEC 13335-1:2004

Abbreviations[48]

OCIO	Office of the Chief Information Officer	BCSI	Bureau du chef du service de l'information
ESC	Executive Steering Committee	CDE	Comité directeur exécutif
ARB	Architecture Review Board	CEA	Conseil d'examen de l'architecture
EAPO	Enterprise Architecture Program Office	BPAE	Bureau du programme d'architecture d'entreprise
CIOC	Chief Information Officers' Council	CCI	Conseil des chefs de l'information
ITMAC	IT Managers Advisory Committee	CCGIT	Comité consultatif sur la gestion de l'information et de la technologie
IM&ICT	Information Management and Information Communications Technology	GI et TIC	gestion de l'information et en technologie de l'information et des communications
GRC	Governance, Risk, & Compliance	GRC	Gouvernance, risque et conformité
IA	Information Architecture	AI	Architecture de l'information
AA	Application Architecture	AA	Architecture des applications
TA	Technology Architecture	AT	Architecture de la technologie
SA	Security Architecture	AS	Architecture sécurisée

[48] For the list of TOGAF® abbreviations, please refer to TOGAF® 9.1 Online Guide, http://pubs.opengroup.org/architecture/togaf9-doc/arch/, Appendix B

TOGAF® 9.1 Licence Agreement

(signed agreement available upon request)

TOGAF® Version 9.1 Corporate License (Non-Commercial)

BY SIGNING AND RETURNING THIS LICENSE, YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL THE TERMS OF THIS AGREEMENT, DO NOT INSTALL THE TOGAF DOCUMENTATION, AND DESTROY ANY COPY OF IT THAT YOU MAY HAVE.

1. **LICENSE**
   The Open Group grants the Licensee Organization named below a non-exclusive license to use the documentation suite known as TOGAF® Version 9.1 ("the Documentation") **in perpetuity**, and **free of charge**, subject to the following conditions.

   A. NON-COMMERCIAL USE: The Licensee Organization may use the Documentation internally for any purpose not involving commercial exploitation of the Documentation. In particular, the Licensee Organization may use it to develop an information system architecture for use within that organization, or to develop derivative works (subject to the conditions listed below) to support the Licensee Organization's work in the field of IT Architecture.

   B. DERIVATIVE WORK: For the purpose of this Agreement, "derivative work" shall mean any change to the Documentation or any new document that contains any portion of the Documentation. Licensee Organization shall retain all right, title and interest in the changes or additions it makes to the Documentation, but nothing herein shall be deemed to transfer any right, title or interest in the Documentation to the Licensee Organization. Furthermore, in any derivative work, Licensee Organization shall always fully acknowledge the right, title and interest of The Open Group in the original Documentation, and shall not claim or imply that any derivative work of the Documentation is the official TOGAF Documentation.

2. **REDISTRIBUTION PERMITTED WITHIN THE ORGANIZATION**
   Redistribution of the Documentation, in part or in whole, to any permanent employee of the Licensee Organization is permitted provided:
   A. All existing trademarks and copyright notices are retained in all copies of the Documentation;
   B. In any derivative works, TOGAF Version 9.1 is acknowledged as the source; and,
   C. All existing trademarks and copyright notices and this License appear in all derived supporting documentation.

   For the avoidance of doubt and purposes of this license, individual contractors, who do not represent themselves or offer their services commercially as architecture practitioners, shall be regarded as "permanent employees" of the Licensee Organization.

3. **REDISTRIBUTION OUTSIDE THE LICENSEE ORGANIZATION**
   Redistribution of the Documentation, in part or in whole, is not permitted to anyone who is not a permanent employee of the Licensee Organization, **except that**:

   A. The Licensee Organization may reproduce parts of the Documentation in its external literature for the purpose of furthering its work in the architecture field (for example, in Requests for Product, or in other information communicated to potential service providers or product suppliers); **provided that**:
      i. The literature does not in itself constitute a commercial product, or a part of a commercial product; and,
      ii. The above copyright notice appears in all such external uses of the Documentation.

   In particular, contracting companies and individuals needing to use the Documentation in order to perform work on the Licensee Organization's behalf must obtain their own licenses.

4. **PROTECTION OF THE OPEN GROUP'S INTELLECTUAL PROPERTY RIGHTS**
   If the Licensee Organization wishes to contract architecture services organizations or individuals other than permanent employees to undertake work on its behalf using the Documentation, the Licensee

Organization must use all reasonable efforts to ensure that such companies or individuals have a current commercial license for TOGAF Version 9.1 (which they are legally required to have, in order to undertake such work). Notwithstanding the foregoing, in the event that there is a use by a non-licensed architecture services company or individual, then Licensee Organization has no liability.

The Open Group operates a TOGAF certification program that enables companies offering products or services associated with TOGAF to make a legally binding warranty of conformance with Product Standards relating to TOGAF. The use of such certified products or services is **not** a condition of this license. However, The Open Group strongly recommends that such certification be required by the procurer of such products or services, if deemed appropriate. Details of this and other certification programs of The Open Group can be found at: http://www.opengroup.org/certification/.

5. **INCLUSION IN LISTING OF LICENSEES**
The Open Group reserves the right to include the Licensee Organization's name in a published list of organizations that have taken out this License.

6. **DISCLAIMER OF WARRANTY**
This Documentation is provided on an "AS IS" basis, without warranty of any kind.

THE OPEN GROUP DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS DOCUMENTATION, INCLUDING ALL IMPLIED WARRANTIES OF SUITABILITY AND FITNESS FOR ANY PARTICULAR PURPOSE. IN NO EVENT SHALL THE OPEN GROUP BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS DOCUMENTATION.

FOR AND ON BEHALF OF	FOR AND ON BEHALF OF
_____	THE OPEN GROUP
Licensee Organization	
Signature: _____	Signature: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

PRIMARY CONTACT FOR THE LICENSEE ORGANIZATION

Name: _____ Title: _____

Address: _____

Mobile : _____ Fax: _____

Email address: _____

Please complete the above information on behalf of the Licensee, and FAX the completed form to: +44 870-134-8146.

 ISBN 978-1-4605-0311-9