Deloitte.

BCeID Operational Governance and Management Control Framework
Advisory Services
Report

BCeID
Workplace Applications Services
Workplace Technology Services
Ministry of Labour and Citizens' Services

Table of Contents

Definitions

Definitions -

These definitions are working definitions for the purpose of this project. The primary source is BCeID Operational Documentation. In addition. other terms were agreed to, by the project sponsors, as working definitions during the course of this project.

Deloitte.

Definitions	
Authentication	The provision of assurance of a person's identity through a process of confirming or verifying information.
Authentication Credential	Evidence used to prove identity and evidence of authority. Used to determine access rights to government ICT resources (e.g., user ID and password, keys, digital certificates, biometrics).
Authorization	Establishes what actions or information the person is permitted to access or what goods and services the person can receive. The process of giving someone permission to do or have something.
BCeID Control Framework	A formalized and documented logical organization of the governance components along with the supporting methodology for the ongoing management of the business and support for the overall governance of an organization's control elements.
BCeID Operational Model	The logical representation and illustration of the relationships and interactions between the various entities within BCeID responsible for operation of the functions supporting the business.
Confidentiality	Assurance that information is not viewed, stored or disclosed to unauthorized persons, processes or devices.
Credential	*Digital document used to bind an identity or an attribute to a token.* Data that is transferred or presented to establish either a claimed identity or the authorizations allocated to an entity.
Digital Identity (Persona)	The set of data elements (and their values) by which a person wishes to be known and thus identified in a transaction.

Definitions

Deloitte.

Definitions	
Eligibility	The set of data elements (and their values) used to determine if a person qualifies for goods or services. For example, a person may be eligible to participate in a program or may be eligible for benefits.
E-service	A transactional application, which delivers a business function for a government program. One program may have many e-services. One application may deliver one or many e-services.
Governance Model	Information Governance is defined as specifying the decision rights, principles and accountability framework to encourage desirable behaviour in the use of information. The Governance Model is the logical representation and illustration of the relationships and interactions between the various entities responsible for components of Information Governance.
Identity	The unique set of characteristics (data elements) by which a person is known.
Identity Proofing	The process by which a Registration Authority validates sufficient information to uniquely identify a person.
Integrity	Assurance that information has been maintained in a way that can only be accessed or modified by those authorized to do so. Implies that an audit trail is maintained to confirm "who did what, when and how".
Multi-Factor Authentication	Authentication accomplished using at least two factors (something you know plus something you have). This is sometimes also referred to a strong authentication.
Non-repudiation	The ability to confirm the origin, transmission, receipt or processing of a transaction.

Definitions

Deloitte.

Definitions	
Personal information	Means recorded information about an identifiable individual.
Policy	Means a course or principle of action adopted or proposed by a government, party, business or individual. Policies are usually, but do not have to be, formally recorded and relate directly to the mandate and functions of the public body.
Principle	A statement of value, operation or belief that defines the organization's approach to security. The principles define the philosophy of the organization that influences the definition of the policies.
Registration	The process of establishing a verified identity and creating a digital identity and authentication credential.
Registration Authority	A trusted entity that establishes and vouches for the identity of an entity in order to perform registration.
Relying Party	An entity that relies upon the subscribers credentials, typically to process a transaction or grant access to information or a system.
Repudiation	The ability to deny the origin, transmission, receipt or processing of a transaction.
Standard	A requirement for compliance for a particular means of executing a function resulting from a policy. The standard defines what methods and mechanisms will be used to enforce the policy.

Executive Summary

Executive Summary

Move towards a Program defined Governance and Management Control Framework

Drivers for Stronger Governance

Following significant private and public sector failures, there is increasing public expectation that corporations and governments provide management assurances on controls. As a result, there are increased requirements for stronger governance, risk management, controls and control activities.

In the BC government, some of these requirements and responsibilities are outlined in various pieces of legislation and policy. Legislative requirements are principally contained in the Financial Administration Act, Budget Transparency and Accountability, and Public Service Acts. The legislation is expanded upon in Core Policy, Human Resource Policy and IM/IT Policy. Currently, the BC Government does not have a predefined (such as COSO (US) and CoCo (Canadian)) control framework to assist its management in working towards management assurances on controls. However, there are a number of known frameworks that incorporate broad concepts or standards for good management control.

Deloitte.

Move towards a Program defined Governance and Management Control Framework

Purpose of a Control Framework

A control framework is intended to provide a common language for discussing and understanding the relationship between objectives, risks, controls and performance. Further the control framework defines standards against which management, or auditors on management's behalf, can evaluate an organization's ability to deliver its business objectives, to clearly assign responsibilities and to identify its risks and controls.

Purpose of this Engagement

This engagement is to assist the program management in conducting preliminary planning and analysis toward a defined BCeID operational governance and management control framework that will enable the program to provide assurance to its stakeholders (including the public) that it is a well governed and managed operation.

Project Purpose, Scope, and Objectives

Executive Overview - Purpose, Scope & Objectives

Deloitte.

Purpose
The purpose of this engagement was to provide the BCeID program management assistance in defining a high-level BCeID operational governance and management control framework based on leading governance practices, frameworks and objectives.

Scope and Objectives

The review scope and objectives considered the following:

1. Identification of the relevant IT management control frameworks that apply to BCeID;

2. In relation to the control framework, define some of the categories of control objectives and provide illustrative examples of service and control objectives;

3. Design of the structure of the BCeID - IT Management Control framework and provide advise and tools for managing the framework;

4. Identification of potential vendor products that can be used to manage, in the long term, the control framework structure and the related content; and

5. Presentation of the final high-level framework design to appropriate members of ministry management.

Project Intent and Approach

Executive Overview - Intent

Intent of the Engagement and Report

The intent of the engagement and report was to:

1. Assist the BCeID program management in working towards a structure and process as a means to demonstrate accountabilities and compliance with legislation, policy, procedures and strategies/business requirements as well as to meet the auditor assurance process.

2. Assist IAAS with providing management a better understanding of existing frameworks, management's responsibilities for controls and incorporating these controls into their processes.

   This engagement was not intended to develop a detailed control framework or a comprehensive set of control objectives. Rather to support program management in the analysis of control frameworks and related concepts, and illustrate the use of control frameworks and control objectives, within the context of BCeID.

Engagement Approach

The engagement followed the approach outlined in this diagram from initiation to completion

The BCeID Control Framework provides structure and context to the governing and operating policies and processes used to deliver the business services. The framework also provides an anchor point or measuring and reporting on compliance to various legislative and regulatory requirements as well as providing a method for responding to formal assurance measurement and reporting requirements. The framework provides a method and anchor point for the business practices and processes of BCeID.
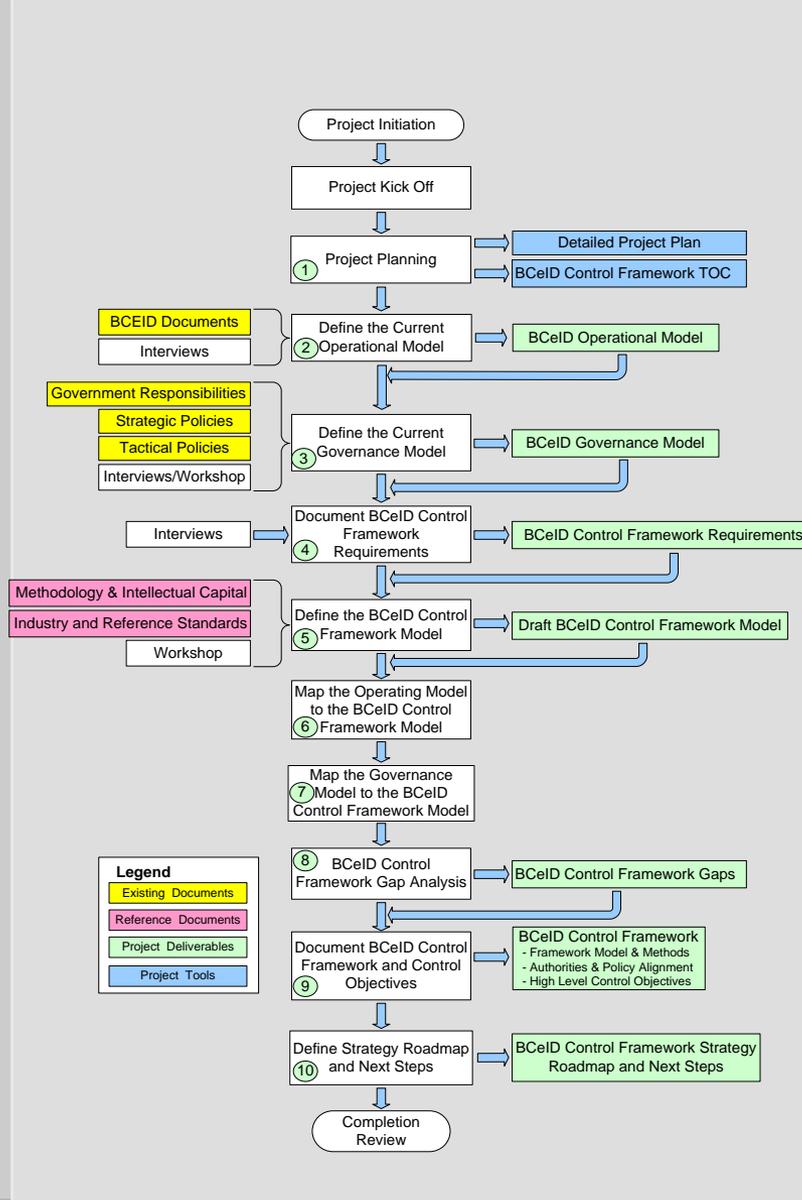
The project followed the approach outlined in following figure from project initiation to completion. This diagram outlines the specific set of project tasks and the associated inputs and outputs for each task. The boxes in the middle part of the diagram outline the high level tasks that were executed to complete the project. The items on the left side of the diagram indicate the areas that provided input into the project tasks. The items on the right side of the diagram indicate the outputs or deliverables that resulted from the project tasks.

Objectives and Findings

Objective #1:
Identify relevant IT management control frameworks that apply to BCeID

Deloitte.

Findings

1. The relevant IT control frameworks were identified: COSO, COBIT, ISO17799 (via the Information Security Policy - ISP) and ITIL were confirmed as current industry practices that should be included in the framework design. ISO 17799 has been adopted by the BC Government.

2. The role of these frameworks was discussed during the project (see next slide for summary). There is a relationship between these frameworks (see next slide).

   a) COSO – Enterprise-wide controls framework focussed on effectiveness and efficiency of operations, reliability of financial reporting and compliance.

   b) ISO17799 – Code of practice for Information Security Management

   c) COBIT – A model for the control of IT Management

   d) ITIL – Best practices for IT service Management

3. The AUS/NZ methodology for risk assessment was also identified as an adopted government standard/tool that should be incorporated on a go forward basis.

4. These IT control frameworks are being used or being considered by many other private and public sector organizations.

Internal Control Framework Relationship Overview

COSO – for enterprise controls

COBIT

ISO

ITIL

What to do? (strategic)

How to do it? (Operational/Tactical)
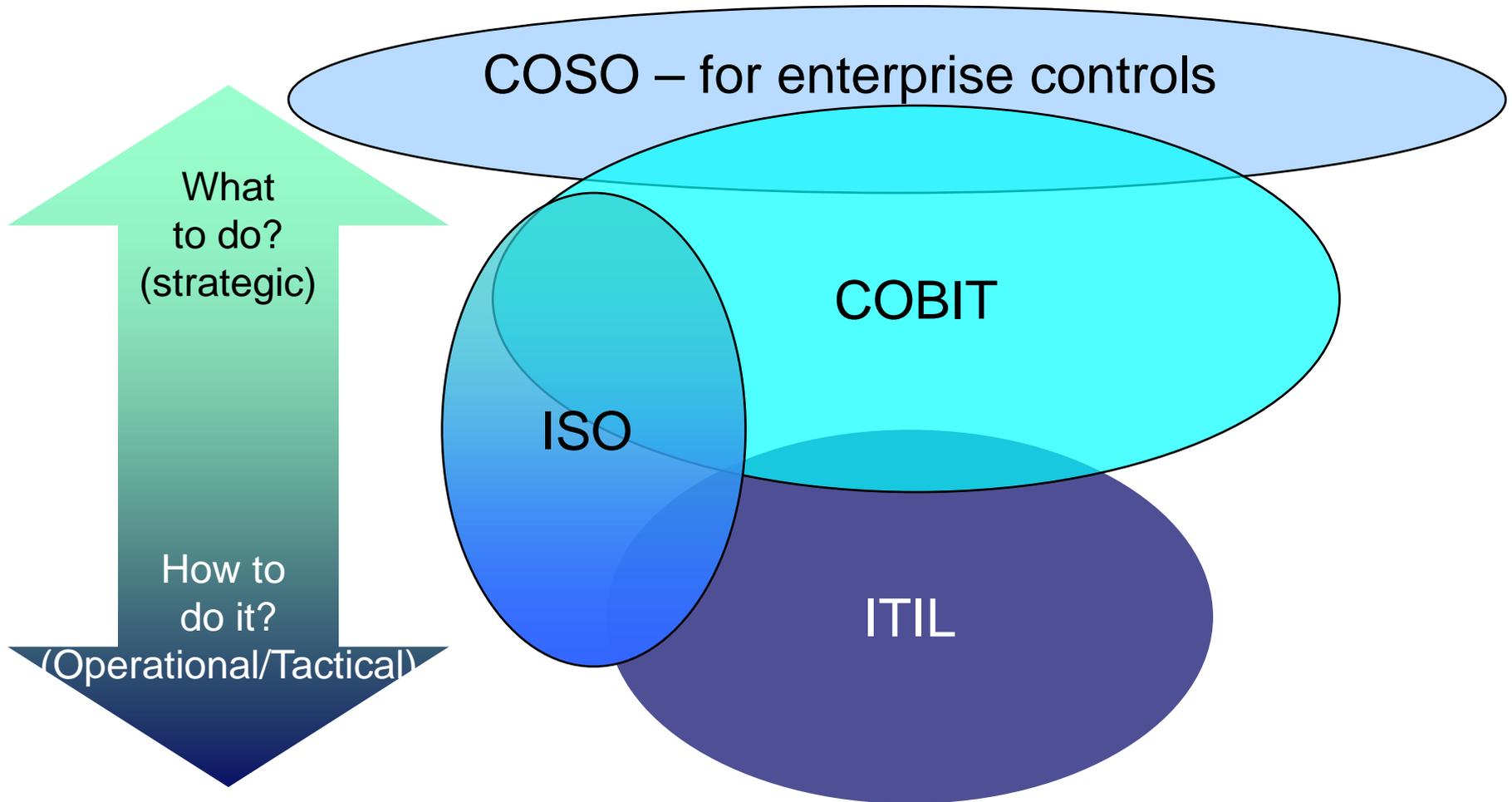
Source: ITGI – Implementing IT
Governance – Peter Davis & Associates

Objective #2:
Control Framework Objectives

Objective #2 - Categories of Control Objectives

COSO – Control Environment

▸ Internal Environment
▸ Objective Setting
▸ Event Management
▸ Risk Assessment
▸ Risk Response
▸ Control Activities
▸ Information and Communications
▸ Monitoring

ITIL - Service Objectives

▸ Service Desk
▸ Configuration Management
▸ Incident Management
▸ Problem Management
▸ Change Management
▸ Release Management
▸ Service Level Management
▸ Availability Management
▸ Capacity Management
▸ Financial Management
▸ IT Service Continuity Management

COBIT- Controls over IM/IT and related business processes

▸ Define a strategic IT plan
▸ Define the information architecture
▸ Determine the technological direction
▸ Define the IT processes, organization and relationships
▸ Manage the IT investment
▸ Manage Quality
▸ Manage projects
▸ Identify automated solutions
▸ Acquire and maintain application software
▸ Acquire and maintain technology infrastructure
▸ Ready operational solutions
▸ Procure IT resources
▸ Install and accredit systems

▸ Manage third-party services
▸ Ensure system security
▸ Identify and allocate cost
▸ Educate and train users
▸ Manage data
▸ Manage the physical environment
▸ Manage operations
▸ Monitor IT performance
▸ Monitor internal control
▸ Oversee IT governance
▸ Oversee regulatory requirements and issues

The control objectives based on COSO include the IT control objectives of the same category.

The service objectives based on ITIL include the IT control objectives of the same category.

ISO 17799 (or government ISP) provides guidance for security that are also included at high level in COBIT.

Objective #2 - Examples

Illustrative Examples of Control Objectives based on COSO

The control objective categories based on COSO include both the business and IT control objectives

- Internal Environment
  - Risk Management Philosophy and Tolerance
  - Assignment of Authority and Responsibilities
  - Organizational Structure
  - Manage Human Resources

- Objective Setting
  - Strategic Objectives
  - Risk Tolerance
  - Define a Strategic Plan

- Risk Assessment
  - Assess and Manage IT Risks
  - Methodologies and Techniques

- Specific Process Level Objectives
  - More specific control objectives could be defined for example to ensure the operations are effective at a business process level. For example "Identification is verified in accordance with policy".

Objective #3:
BCeID Operational Governance and Management Control Framework

Deloitte.

BCeID Business Direction and Governance Authority
(as provided in April 2007)

BCeID obtains business direction from a number of areas of government.

▸ An Office of the Chief Information Office management representative provided a draft working assumption on the IT governance organization based on a project currently underway.

▸ The Government Services Board of Directors provides input for shared services and other government or federal programs.

▸ IM/IT Direction comes from the Chief Information Officer.

▸ Business direction comes from Shared Service BC.

Scope and Objectives

Objective #3

Deloitte.

Identity Management Policy Owner – Office of the Chief Information Officer (GCIO)
- Owner of the Information Security Policy
- Identity Management Standards and Long-Range Planning
- IM/IT Standards and Legislation and Policy to adhere to privacy legislation

Program Owner – ADM, Workplace Technology Services
- Linkage to WTS Objectives
- Responsible for compliance to WTS policies and standards

Program Manager – Director BCeID Program
- Owner of BCeID Policies
- Authoritative Source Management

Risk and Compliance Auditors
- Measure compliance
- Governance issues

Service Delivery Partner - WTS Internal
- Delivery Units reporting to the Service Owner
- Hosting compliance with infrastructure

Service Delivery Partner - Government Internal
- Delivery Units reporting to other parts of government

Service Delivery Partner - External Suppliers
- Private sector organizations

Service Delivery Partners - Registration Authorities
- Establish and vouch for the identity of an entity
- Performs registration
- Defines the identity
- Provides policy content

Program Staff (Employees, Contractors)
- Execute operating procedures
- Maintain and deploy program standards

Program Clients – Online Service Owners
- Responsible for the security and integrity of the online services

Program Customers – Account Holding Businesses and Individuals
- Enter into agreements with BCeID

Document Disposal Act

Information Security Policy

Electronic Transaction Act

Core Policy Manual

Income Tax Act

Partnership Act

FIOPPA

Business Number Act (Bill 16 – 2005)

Business Corporation Act

BCeID Operating Policies

Operational Procedures

Program Activities

Legend:
- Government-CIO
- Workplace Technology Services
- BCeID
- Auditors
- Service Delivery Partners
- Program Customers
- Program Clients
- Governing Legislation

Objective #3: The High-Level BCeID Framework consists of a Service, Control and Operating Framework

Deloitte.

The BCeID Framework is represented by three individual framework areas:

- The **Service Framework** identifies the services that BCeID provides (slide 27);
- The **Control Framework** identifies the controls in place to manage BCeID business (slide 28); and
- The **Operating Framework** identifies the BCeID operational responsibilities, policies and process (slide 29).

The BCeID Framework illustrates the orientation of the three framework areas and the drivers and requirements and leverages the existing BCeID Operating Policy Framework.

Objective #3 : BCeID Framework Assumptions

Deloitte.

1. The BCeID Operating Policies will be the anchor point for the framework contents.

    – The industry framework structures will assist with the framework contents.

    – All industry frameworks will be mapped according to the BCeID Operating Policies.

2. The framework contents will be populated with any areas currently missing from the BCeID Operating Policies.

    – The industry frameworks (COBIT, ITIL, COSO) will be used to provide additional framework content for those areas not currently addressed by the BCeID Operating Policies.

3. The Operating Framework represents the current responsibilities, policies and procedures.

    – The BCeID Operating Policies are already mapped to the BC Government Information Security Policy which is organized according to ISO 17799.

Objective #3: BCeID Service Framework

The Service Framework;

- Is based on the business need and expected services provided by BCeID.

- Defines the **Service Requirements** based on the **Business Requirements**.

- Derives the **Service Objectives** from the service requirements.

- Defines or links to a **Program Activity** to support the **Service Objective**.

- Should be aligned with ITIL where the services involve Service delivery or Service Management components of ITIL.

- Can be aligned with components of COBIT.

- Can be assessed against ISO 20000 for ITIL-based services.

Objective #3: BCeID Control Framework

Deloitte.

The Control Framework;

- Is based on the business need and risk tolerance of the organization.

- Defines the **Control Requirements** based on the **Business Requirements**.

- Derives the **Control Objectives** from the **Control Requirements**.

- Defines or links to a **Program Activity** to support the **Control Objective**.

- Can be assessed against ISO 17799 for information security controls and COBIT for IT controls.

Objective #3: BCeID Governance Framework

Deloitte.

The Governance Framework;

- Is based on the **Organizational Responsibilities** and culture of the organization.

- Defines the **Operating Policies** that support the execution of BCeID's mandate.

- Defines the **Operational Procedures** that direct how the BCeID responsibilities should be carried out.

- Defines the **Technical Controls** implemented by supporting technologies and configurations.

- Aligns with the **Information Security Policy** from the Office of the Chief Information Office.

- Can be assessed against ISO 17799 for information security controls and COBIT for IT controls.

- Can be assessed against ISO 27001 for certification.

High-Level BCeID Framework Illustrative Relationships

Business Goals
- Set by Government
- Deputy Ministry Council
- Defines business priorities

Financial Priorities
- Set by Shared Services Board of Directors
- Defines investment priorities and constraints

Results in

Prioritizes

Electronic ID Requirements
- Set by the G-CIO
- Defines government-wide requirements

Core Policy Manual
- Set by the G-CIO
- Chapter 12

Business Objectives
- Set by the WTS
- Reviewed on a regular basis

defines

Risk Assessment
-

IM/IT Policies
- Set by the G-CIO

Electronic ID Requirements
- Set by the G-CIO
- Defines government-wide requirements

Business Requirements
- Defined by BCeID
- Identifies what needs to be in place to support the Business Objectives

Defines control needs

provides input into

provides input into

contributes to

Provides input into

contributes to

defines service needs

Service Requirements
- Defined by BCeID
- Defines the scope and services BCeID is required to provide

Information Security Policy
- Set by the G-CIO

Control Requirements
- Defined by BCeID
- Defines the scope and controls that BCeID is required to implement

provides input into

BCeID Operating Policies
- Governs the operation of BCeID

Ensures compliance with

Ensures compliance with

Is achieved by

Is achieved by

Service Objectives
- Set by BCeID
- The desired result or purpose to be achieved by implementing services

Operational Procedures
- Directs program execution

defines

Control Objectives
- Set by BCeID
- The desired result or purpose to be achieved by implementing controls

Implemented with

Provides direction to

Program Activities
- Set by BCeID
- Defines the required services and controls to carry out BCeID business

Provides direction to

Deputy Minister Council

Shared Services Board of Directors

Government-CIO

Workplace Technology Services-Exec

BCeID

directs

Technical Controls
- The collection of technologies and configurations required to effectively manage the ongoing business

* Related to slide 25 – presented to illustrate relationships

Deloitte.

Findings

1. The control frameworks (COBIT, COSO) and disciplines (ISO 17799, ITIL, Aus/NZ) are appropriate. These have been embraced or proposed for use within the BC Government standards (adopted for government --ISO17799, ITIL, Aus/NZ).

2. The outcomes of this project are likely to be applicable to other IT shared services in government, and for IM/IT governance overall. Other services and IT governance in general have the same issues as BCeID.

3. The documentation developed to date by the BCeID program was also reviewed to determine its consistency with an IT Management Control Framework based on the selected frameworks. It was determined that it is consistent with the defined information model, particularly in reference to ISO17799. It does not incorporate COBIT, COSO or Risk Assessment, but can be enhanced to do so.

4. There are tools available that assist with the set up of the framework within a database and support the adoption of a more comprehensive framework.

Objective #4:
Automation Considerations and Vendor Products

Objective #4

Deloitte.

Automation Considerations

1. Products are available that will take existing documents in many different forms and be able to establish a database of policies and procedures.

2. Many of these products can support multiple frameworks such as ITIL, COBIT and ISO 17799.

3. The existing BCeID Operating policy can be electronically "parsed" to produce an initial or partial electronic database of policies to ease the process.

4. These can then be crossed referenced with the existing frameworks such as ISO, ITIL and COBIT to provide multiple views.

5. Establish the ISO view from the BCeID Operating Policies using the ISP mappings.

6. Map COBIT to the BCeID Operating Policies using the ISO mapping as a reference.

7. Map ITIL to the BCeID Operating Policies using the COBIT and ISO mapping for reference.

8. Map any additional required control or service areas not covered by using the ISO mapping.

9. COSO ERM can provide overall guidance for organizing the resulting framework for business processes outside of IT.

10. One consideration is the risk that the standards will evolve or change at a different pace potentially causing them to be out of sync if they are used to cross reference each other in the automated.

Deloitte.

Findings

1. The effort to develop and populate the BCeID IT Management Control Framework will be significant. Maintenance effort is also significant.

2. Software tools would help, but complete automation is not feasible and there will be a mix of products, and a mix of automated and manual components required to hold the framework information.

3. This software area is immature, there is a wide variety of software tools providing partial coverage, and there will likely be consolidation and failures in the market.

4. Further definition of requirements and a better understanding of the range of products will be required before selecting a standard tool for government, although it might be possible to select a product that would support an IT Management Control Framework for a specific IT service.

Next Steps

Next Steps

1. Develop Control Framework:

    a) Conduct high level risk assessment to identify inherent risk and guide the development of control objectives.

    b) Identify reporting requirements and ensure the framework supports these requirements. These would include for example, internal control self-assessment or external service auditor assurance reports.

    c) Identify control objectives and their relevance based on risk and business requirements. Map the Service, Control and Governance Frameworks to the generally accepted industry frameworks. The Control and Service Objectives should align with objectives under ITIL, ISO 17799 and/or COBIT.

2. Select and implement appropriate tools to support the efficient implementation and sustainment of the framework.

3. Implement framework with considerations for sustainment. Ensure linkages between the framework components are well documented and maintained.

4. Perform BCeID program risk and control gap assessment to ensure control objectives are met.

5. Assess the potential to leverage this framework for other government IT services.