Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada

Better government: with partners, for Canadians

GC Enterprise Security Architecture (ESA) Program Charter

Chief Information Officer Branch
Security Division

Version 1.4

GCDOCS #1111371(EN)
GCDocs nº 5728389(FR)

Canada

Document Revision History

Version	Description of Change	Author(s)	Date
1.0	Version 1.0 for Endorsement	P. Tea-Duncan, TBS-CIOB	05 June 2013
1.1	Updated based on comments from ADM ITST Meeting held 12 June 2013 - Updated Figure 2 on pg. 7 - Removed “service” under TBS description on pg. 16 - Removed “as applicable” under depts. description on pg. 18 - Updated Figure 7 on pg. 20 - Replaced Program ConOps with Program Implementation Plan	P. Tea-Duncan, TBS-CIOB	17 June 2013
1.2	Minor edits on page 1 driven by a requirement to generalize some terminology	C. Daoust, TBS-CIOB	24 June 2013
1.3	Updated based on comments received 2 July 2013 - Removed reference to ConOps in Section 2.3 and Section 5 - Replaced Program Implementation Plan with Program Implementation Framework	P. Tea-Duncan, TBS-CIOB	4 July 2013
1.4	- Version 1.3 endorsed by ADM IT Security Tripartite at August 23, 2013 meeting. - Minor updates - Added GC to heading and added CSIS to Section 2.3.4.2.	P. Tea-Duncan, TBS-CIOB	6 September 2013

Table of Contents

List of Figures

Authorization

This Program Charter formally authorizes the existence of the Enterprise Security Architecture (ESA) program.

Endorsed by ADMs as the August 23, 2013
ADM IT Security Tripartite meeting.

_____ _____

Corinne Charette Date
GC Chief Information Officer
Chief Information Officer Branch (CIOB),
Treasury Board of Canada Secretariat (TBS)

_____ _____

Benoît Long Date
Senior Assistant Deputy Minister
Transformation, Service Strategy and Design
Shared Services Canada (SSC)

_____ _____

Toni Moffa Date
Deputy Chief, IT Security
Communications Security Establishment Canada (CSEC)

1. Introduction

In 2012, the Government of Canada launched an initiative (hereinafter, “GC cyber security initiative”) recognizing the need to improve the security of its information and IT assets. As a result, funding was received by Treasury Board of Canada Secretariat (TBS), Shared Services Canada (SSC) and Communications Security Establishment Canada (CSEC) to strengthen the security of federal cyber systems in support of Pillar 1 of Canada’s Cyber Security Strategy. The funding received will help to enhance security of government networks and systems to protect against malicious cyber threats and to provide a secure, reliable and uninterrupted service to Canadians as they become more interactive with government online, while protecting the private information of Canadians, Canadian businesses and government information as it is processed through Government of Canada (GC) systems.

The GC cyber security initiative is divided into three (3) approaches: Prevent, Defend & Detect, and Respond & Recover. Under the Prevent approach, TBS will lead the establishment of a security architecture for the GC Information Technology (IT) infrastructure. The focus of the Enterprise Security Architecture (ESA) initiative is the development and maintenance of an enterprise IT security architecture vision, strategy and designs, led by TBS in collaboration with SSC, and supported by CSEC.

An enterprise IT security architecture will ensure that risk is adequately managed, security controls are applied in a consistent manner, and the total cost of ownership to the GC is minimized. With the creation of SSC in August 2011, there is an opportunity to build-in security from the outset as systems are being designed, which results in better security and is much less expensive that adding security after the fact. Cyber threat exposure will be reduced by taking advantage of consolidation of data centers and reduction in the number of networks that connect to data centers to improve the security of the IT infrastructure through standardization and reengineering initiatives. Incorporating an array of security features and designs into the consolidated network will strengthen the security posture of individual departments.

This program charter document describes the ESA initiative and provides a framework to support the delivery of the program and its objectives. The program charter will guide the execution and control of the program and documents its definition and characteristics as well as an overview of the program governance, roles and responsibilities, and high level plans.

1.1 Business Issue Overview and Problem Statement

The Government of Canada (GC) relies heavily on information technology (IT) to conduct its day to day business activities. The information processed and stored on GC networks and systems varies in importance and in sensitivity, including private information about Canadian citizens, sensitive information dealing with Canada’s economic and political interests and classified information related to national security.

Threats to GC systems and networks continue to evolve in level of sophistication and in stealth. It is extremely important to recognize that GC networks and systems are lucrative targets and have already proven to be vulnerable to exploitation. There was considerable coverage of unauthorized attempts to access several Government of Canada networks in January 2011 which raised questions about the Government’s ability to safeguard the personal information of Canadians. These cyber security incidents against GC systems and networks have clearly demonstrated that this information is of great interest to a variety of threat actors, including nation states that are devoted to obtaining this information using a variety of techniques. Consequences could include significant loss of sensitive and/or classified information leading to threats to national security, economic losses for Canada, direct costs to departments to recover from cyber incidents, and loss of credibility for the GC.

1.2 Current Situation and Applicable History

1.2.1 Canada Cyber Security Strategy

Canada's Cyber Security Strategy (CCSS), published in October 2010, demonstrates the GC's commitment to protecting Canada's cyberspace. CCSS is national in scope and is comprised of three fundamental pillars:

1. Securing Government Systems - Canadians trust Government with their personal and corporate information, and also trust Government to deliver services to them. They also trust that the Government will act to defend Canada's cyber sovereignty and protect and advance our national security and economic interests. The Government will put in place the necessary structures, tools and personnel to meet its obligations for cyber security.

2. Partnering to secure vital cyber systems outside the federal Government - Canada's economic prosperity and Canadians' security depend on the smooth functioning of systems outside the Government. In cooperation with provincial and territorial governments and the private sector, the Government will support initiatives and take steps to strengthen Canada's cyber resiliency, including that of its critical infrastructure sectors.

3. Helping Canadians to be secure on-line - The Government will assist Canadians in getting the information they need to protect themselves and their families online, and strengthen the ability of law enforcement agencies to combat cybercrime.

CCSS identified several areas that need to be addressed in terms of securing government systems, including keeping pace with evolving cyber threats, enhancing the security of the GC cyber architecture, addressing global supply chain issues and improving cyber security education and awareness. The ESA initiative will focus on Pillar 1 activities.

1.2.2 Strengthening the Security of Federal Cyber Systems: A Backgrounder

As outlined in the *Strengthening the Security of Federal Cyber Systems: A Backgrounder* paper, enhancing the security posture of GC systems and networks requires a comprehensive IT security strategy that includes developing IT security architecture designs, implementing defence-in-depth IT security capabilities based on these designs, and detecting and effectively responding to cyber threats. It also means ensuring that GC users understand and adhere to applicable security policies and know how to identify and respond to cyber threats directed at end users. Finally, enhancing the security posture of GC systems requires that the GC understand how the IT landscape is evolving and that it continues to align its IT security strategy with its overall IT strategy.

The paper describes three fundamental themes:

1. *Improve our understanding of the cyber threat landscape*. The cyber security threat landscape is broad and complex and there is evidence that we are only scratching the surface when it comes to our understanding of this topic. The GC needs to devote more resources to analyze both potential and existing cyber threats and design security measures that guard against them. The more informed the GC is regarding the cyber threat landscape, the more effective its security designs and capabilities will be.

2. *Strengthen defensive capabilities*. The GC needs to improve its security posture by continuing its ongoing consolidation activities and implementing more comprehensive and robust defence-in-depth security measures. This includes enhancing our ability to detect and respond to cyber threats. The design and implementation of these security measures will be informed by cyber threat intelligence.

3. *Establish incident recovery capabilities*. Cyber incidents are bound to occur despite protective and defensive measures being implemented. The exploited vulnerability must be addressed as quickly as possible and the amount of downtime and lost productivity must be minimized. To that end, the GC must establish a comprehensive incident response and recovery capability in order to provide more rapid response to serious incidents affecting GC systems.

Over the next several years, the GC will focus on the following areas:

- Identity, Credential and Access Management (ICAM);
- End User Device Security;
- Data Security;
- Application Security;
- Network and Communications Security;
- Compute and Storage Security; and
- Security Operations.

The following figure provides a visual representation of the focus areas.

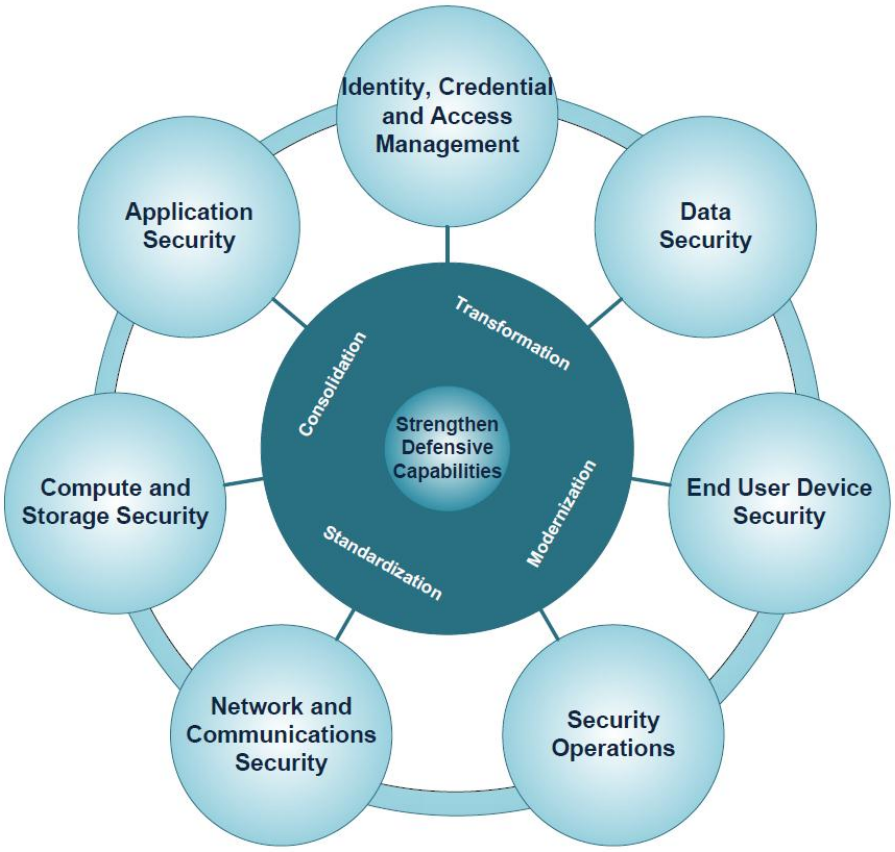


Figure 1 – ESA Focus Areas

1.3 Vision, Mission and Program Purpose

The ESA program has been established as a government-wide initiative to provide a standardized approach to developing IT security architectures, ensuring basic security building blocks are implemented across the enterprise as the infrastructure is being renewed. ESA will provide support to the broader IT transformation initiatives using a proactive approach of building an infrastructure that will address threats, technologies, and business requirements as they change over time and developing flexible and dynamic architectures that enable faster adoption of new use models and capabilities, while providing security across an increasingly complex environment and changing threat landscape.

The ESA program will define:

> ***A sustainable, secure and resilient GC enterprise infrastructure enabling the trusted delivery of internal and external GC programs and services.***

GC assets including data, devices/tools and the IT infrastructure must be protected to minimize the risk of compromise, loss and non-availability. The ESA program must adopt a more data-centric and attribute-centric approach. An attribute-centric architecture will facilitate the adoptions of new technology, the centralization of IT, and the evolution towards shared services for all of GC. The attribute centric-architecture will assign attributes to all assets and people, hence ensuring the assets are accessible by those who are authorized, using the appropriate technology and infrastructure.

The ESA program's purpose is to achieve the following results:

- Ensure more cost-effective, interoperable, resilient and secure IT solutions in support of GC objectives;
- Maintain availability of GC systems and services while complying with relevant GC legislation and policy instruments;
- Adoption of an architecture methodology and approach to ensure common understanding, alignment, and reduce duplication of effort amongst interdepartmental stakeholders;
- Security of information, IT infrastructure and applications with the implementation of consistent security controls which result in lower total cost of ownership; and
- Keep risk at acceptable levels.

2. Program Scope and Objectives

The overall objective of the ESA program is to ensure that security is built into the designs of the IT infrastructure as it undergoes its transformation. The GC must, on an ongoing basis, identify threats to GC networks and systems, prioritize and counter identified and potential threats, and continually improve the robustness and security of the GC IT infrastructure.

2.1 Program goals, objectives, and business outcomes

The ESA program will offer secure IT architectures for the GC. The following identifies the goals, objectives and expected business outcomes for the program:

No.	Goals	Objectives	Business Outcomes
1.	Define and establish security architecture governance.	• Establish a GC-wide IT security architecture governance structure including roles and responsibilities for the delivery of the program and its objectives. • Define and establish sustainable governance, processes and methodologies that will support the development, implementation and maintenance of IT security architectures.	• Horizontal approach to IT security • Unity of effort and effective interdepartmental cooperation • Accountability and ownership is understood • Clear roles and responsibilities (with handoffs) • Improved information sharing and ongoing collaboration • Resources are utilized cost-effectively and efficiently
2.	Define and establish a common IT security architecture framework and methodology.	• Develop a framework that will provide a common understanding for the development of security architectures for the GC IT infrastructure. • Adopt an architecture approach that includes the development of security patterns that will provide guidance on how to implement the minimum baseline security controls in target architectures for a particular context. • Develop appropriate tools to help ensure that requirements are effectively managed and traceable between business requirements and the design and an integrated architecture repository that can be used to enable re-use efficiencies across the GC.	• Translation of abstract policy requirements into measurable security controls • Effective introduction, implementation, and evolution of architectures • Consistent security posture across the GC • Information security solutions are implemented and operated consistently throughout the GC • Architecture alignment and compliance

No.	Goals	Objectives	Business Outcomes
3.	Define and establish security architectures for the GC IT infrastructure.	• Develop an overall vision and strategy for the enterprise IT security architecture. • Develop risk-managed target architectures that are designed to meet GC business needs and align with the overall enterprise IT architecture and enterprise IT security architecture. • Develop a strategic roadmap and integrated work plan that identifies the scope, priorities, resources, and activities necessary for meeting overall program objectives and business requirements that meet ESA focus areas and support high-priority initiatives. • Develop a generic threat assessment for the GC to guide the selection of enterprise security controls and to provide a starting point for Department Security Control Profile development. • Complete the Risk Spectrum in ITSG-33 in order to provide support on risk mitigation strategies for IT security architectures for Secret and below.	• Application of timely and consistent enterprise security controls across the environment • Resilient and secure IT systems in support of government objectives • Reduced cost through standardization and risk reduction • Appropriate and up-to-date domain and/or federated architectures exist that provide reliable architecture information. • Systems that are securely designed and built to provide cost-effective systems on which business can rely

2.2 Program Scope

2.2.1 Scope Definition

Architecture views are representations of the overall architecture that are meaningful to one or more stakeholders. Architecture views are leveraged to simplify the scoping, development, management and alignment between different architecture levels. Each architecture view focuses on a subset of the overall environment in order to deal with a specific business or technological issue, and includes an appropriate level of detail based on its target audience.

For any given focus area, the GC may develop three distinct IT security architecture views of increasing level of detail:

- High-level View. Artefacts developed at this layer are high level documents that are GC/Enterprise in scope and have a strategic impact.
- Context Specific View. Artefacts developed at this layer provide supplementary details; their scope is on common, shared or departmental services and they have a business impact.
- Solution View. Artefacts developed at this layer include significant detail, are system in scope and have an operational impact.

The ESA views are depicted in the figure below.

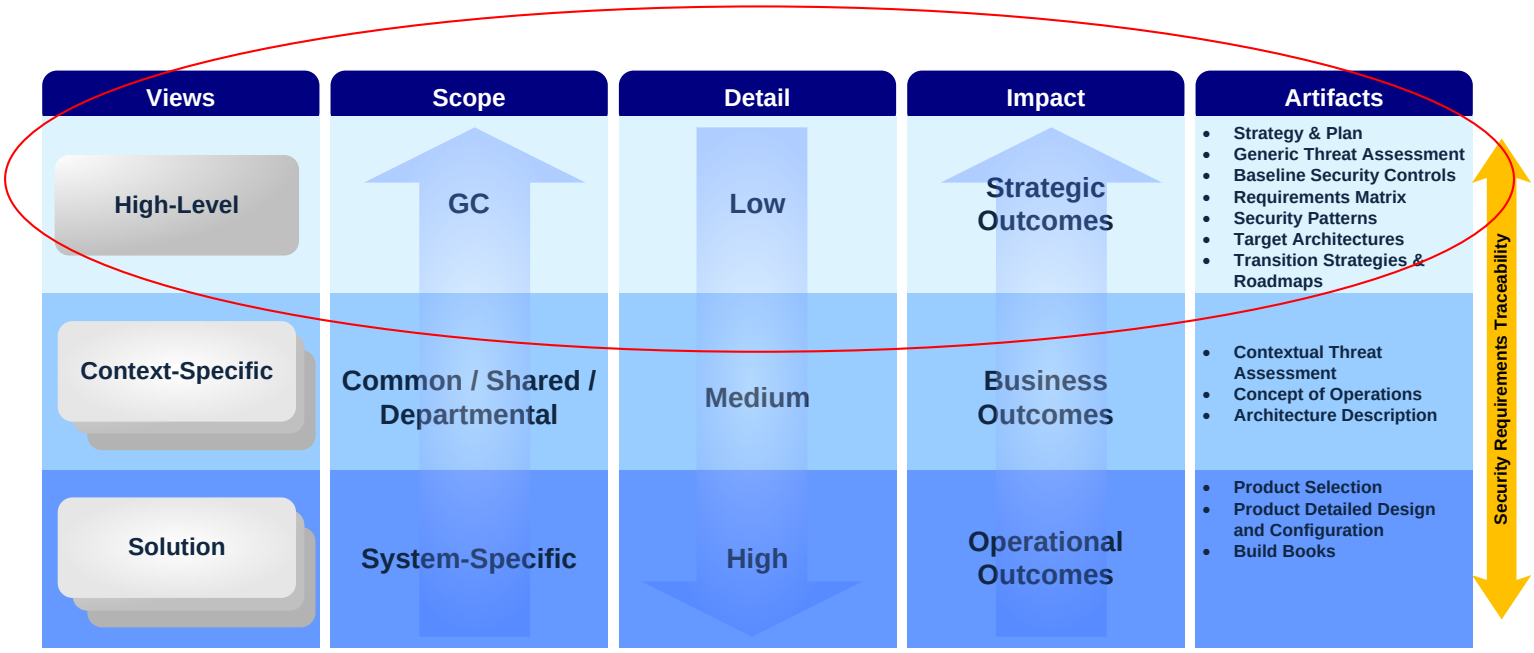


Figure 2 – ESA Architecture Views

The primary focus of the ESA program is the development of the high-level views however for common services or to provide support for GC priority initiatives, the ESA program may provide additional technology-agnostic guidance for the context-specific or solution views. The ESA program will develop architectures aligned with the ESA IT Security Focus areas described in Section 1.2.2.

2.2.2 Boundaries

Activities in Scope	Activities out of Scope
1. Development of the Program Management documentation such as the Program Charter.	1. Development of the Project Management deliverables such as the Project Charter, Project Plans, etc.
2. Development of the program methodology and operational model including processes for escalating issues, assigning authorities, engaging governance etc.	2. Development of the Service/System Concept of Operations on how the architecture will be implemented within a department.
3. Development of a framework that includes an architecture development methodology and processes to manage security requirements.	3. Development of a systems development lifecycle framework.
4. Develop security patterns that provide guidelines on how to implement enterprise level security controls.	4. Developing system-specific detailed design specifications.
5. Developing risk-managed target architectures that are aligned with GC strategies.	5. Developing the solution architectures including technology roadmaps and the implementation of the solution architectures in an operational environment.

2.3 Program Approach

The following sections provide an overview of the governance, risk, architecture conformity and monitoring and measurement strategies for the ESA program. More detailed operational processes will be outlined in the ESA Program Implementation Framework document.

The desired results can only be achieved through the collaboration of departments and agencies which each have a specific role in designing and implementing the GC enterprise IT security architecture. Security architecture expertise from other lead security agencies and key stakeholders will be leveraged in support of many of the activities identified within this GC IT security strategy. Industry will be engaged to provide support in ensuring that the enterprise architecture and associated designs will continue to evolve over time to keep pace with the ever-changing threat and technological environments.

2.3.1 Governance and Management

A clear governance model and management plan must be developed. The governance model should set the direction and objectives for ESA within the GC, and the management plan should execute the achievement of the objectives. Governance provides a systematic way for an organization to make decisions. It establishes decision-making rights, authorities, responsibilities and precepts, and it codifies those precepts as principles, policies, standards, processes, guidelines and consequences for noncompliance. A guiding principle in ISACA's COBIT 5 framework is the distinction made between governance and management which are defined as follows:

- Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives.

- Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.

These are different types of activities, with different responsibilities; however, given the role of governance—to evaluate, direct and monitor—a set of interactions is required between governance and management to result in an efficient and effective governance system. The following figure provides a reference model for the GC ESA governance and management key areas.

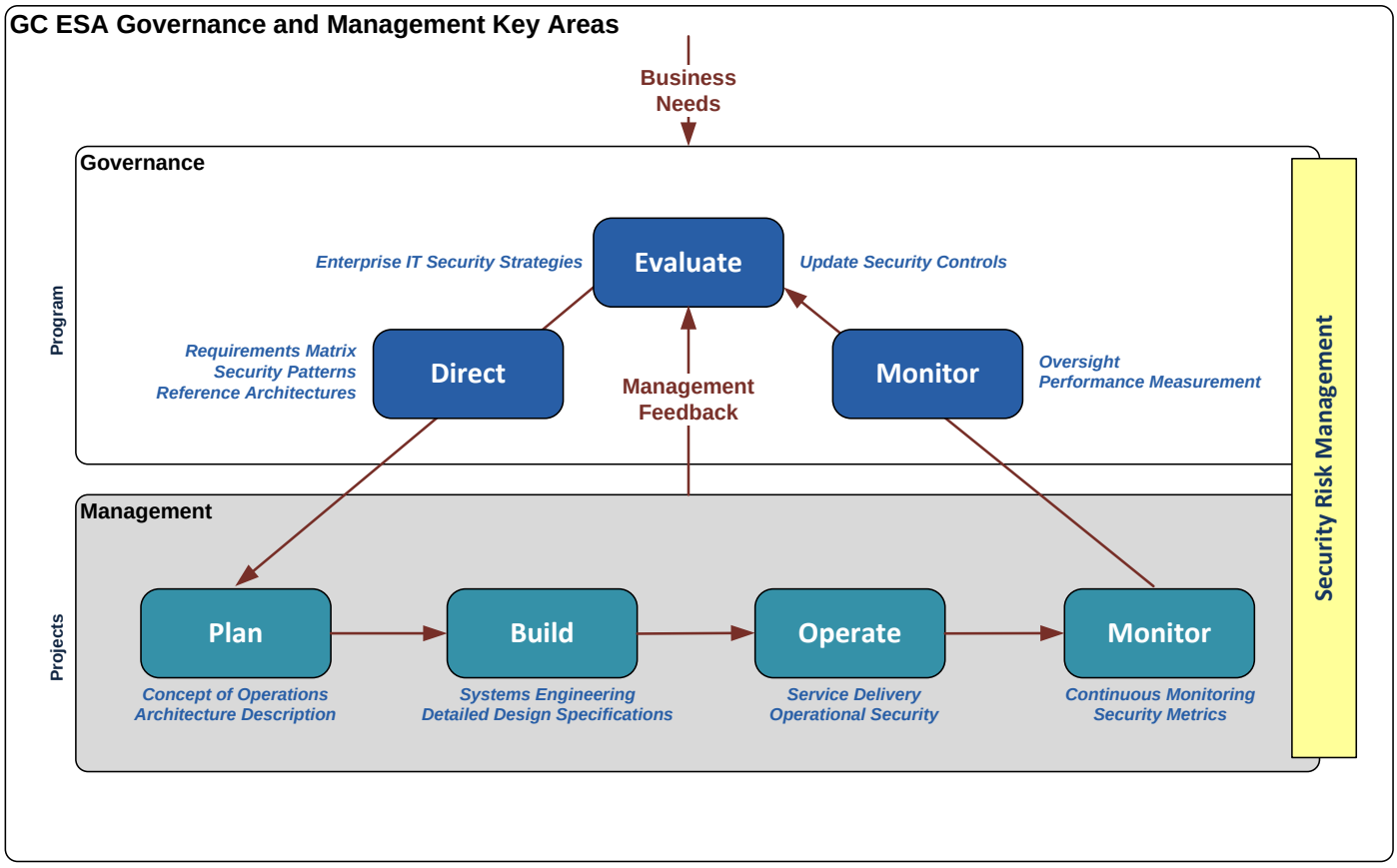


Figure 3 – ESA Governance and Management Key Areas

The description of the key areas for ESA Governance and Management are discussed below:

Governance

- Evaluate the business needs for security and assess risks to the GC. Identify the selection of security controls that align with GC IT security strategies.
- Direct and prioritise the implementation of the context-specific architectures and solution architectures using approved target architectures, security patterns and requirements matrices that help translate abstract policy and business requirements into measurable security controls and provide guidance on the implementation of enterprise security controls; and
- Monitor the performance of the information system in meeting agreed-on direction and objectives, and provide oversight to management.

Management

- Plan the solution for common, shared and departmental information systems and demonstrate alignment to the overall GC IT security architecture and ITSG-33 management activities for risk-managed decisions;
- Build the secure information system by following activities identified in ITSG-33 Information Systems Security Implementation Process (ISSIP) including security assessment and authorization activities;
- Operate the system securely and in accordance with system policies and procedures; and
- Monitor the effectiveness of security controls and ensure continuous monitoring of the information system as well as providing feedback to Governance.

2.3.2 Risk-Managed Approach

Risk management is the strategic discipline of assessing, prioritizing, monitoring and controlling the impact of uncertainty on objectives and is central to business decision making. The *Framework for the Management of Risk* states that "effective risk management equips federal government organizations to respond actively to change and uncertainty by using risk-based information to enable more effective decision-making. In turn, increased capacity and demonstrated ability to assess, communicate and manage risk builds trust and confidence, both within the government and with the public."[1] Risk management helps align IT security decisions with business strategy and supports the business in making better decisions. Risk management is a continual process or cycle in which risks are identified, measured and evaluated; mitigations are then designed, implemented and monitored to see how they perform, with a continual feedback loop for decision maker input to improve countermeasures and consider trade-offs between risk acceptance and avoidance. Managing risk as a system allows for greater situational awareness of how varied risks and mitigation efforts may impact other activities.

In a shared environment, risk management is even more important. An enterprise security risk management approach is necessary to view how risks from one organization can affect other parts of the organization or to see the cumulative risks the organization faces and to subsequently provide senior management with an organization-wide view of its risks so as to promote better trade-off decisions and enhance application of foresight. A risk assessment strategy will help in decision making and helping the business to go forward with its plans while accepting or mitigating associated IT risks and should include an evaluation of current and future information threats so that informed, timely action to mitigate risk can be taken.

The ESA program will leverage terminology and concepts from CSEC's *IT Security Risk Management: A Lifecycle Approach (*ITSG-33). The IT security risk management process documented in ITSG-33 defines a set of activities to ensure key steps are performed on an ongoing basis during the lifetime of the information systems, and to ensure risk management is applied from an enterprise perspective. Continuous improvement is a key aspect of the recommended process to ensure that as the threat environment evolves, so do the controls that have been put into place.

2.3.2.1 Security Assessment and Authorization

ITSG-33 describes an information system security implementation process (ISSIP) to help government departments ensure security is considered right from the start of a project lifecycle. The ISSIP includes activities related to Security Assessment and Authorization (SA&A) which is the independent verification and validation of the security controls of a system to determine if it was properly implemented, and if it is working correctly. The SA&A activities will help ensure that solutions are designed securely with enterprise security requirements and necessary security controls integrated into the GC enterprise architecture and systems development life-cycle (SDLC) processes. ESA architectures and patterns will provide security assessors and authorizers with a reference point when assessing the implementation of the security requirements in a solution and help to ensure that information systems are designed and implemented in alignment with agreed-on objectives.

An enterprise SA&A approach is required to provide a more holistic approach which engages the project, internal service providers and representatives from key departments and stakeholders. This process must be simple, easily understood and allow for quick (reasonable) turnaround times.

[1] TBS Framework for the Management of Risk, http://publiservice.tbs-sct.gc.ca/pol/doc-eng.aspx?id=19422&section=text.

2.3.3 Architecture Compliance

To ensure that a consistent security posture of the IT architecture is maintained, security controls are appropriately implemented and the total cost of ownership to the GC is minimized, an architecture compliance review process is required. An architecture compliance review is a scrutiny of the compliance of a specific project against established GC objectives and architectural criteria such as the ESA target architectures and security patterns.

As a separate initiative led by TBS, a GC IT Architecture Review Board (GC ITARB) is being proposed that will include an architecture compliance review process. The vision for the IT Architecture Review Boards (ITARB) as outlined in the *ITARB Concept of Operations Guidelines* is depicted in the following figure.

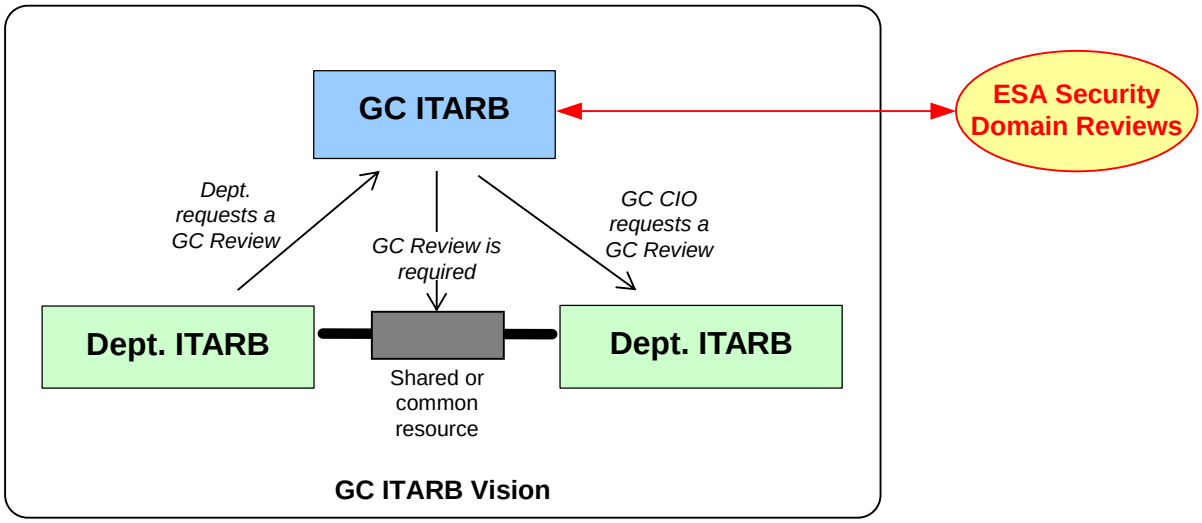


Figure 4 – GC ITARB and ESA

Architecture reviews will be requested by Departments or by the GC CIO at various points in an IT-enabled project lifecycle (namely at Gates 2 and 5 as per the TBS *Guide to Project Gating for IT-Enabled Projects*). Subsequently, the GC ITARB will convene architecture review meetings with domain experts including Security. An architecture artifact is approved or a decision made by the ITARB that allows the project to move forward. Subject matter experts (SMEs) from the ESA program will participate in the security domain architecture reviews to ensure that proposed solutions are aligned with GC IT security strategies and objectives.

The GC ITARB will provide the following benefits:

- Ensure the application of best practices to architecture work.
- Provide an overview of the compliance of an architecture to mandated enterprise standards.
- Provide a way of deciding between architectural alternatives, since the business decision-makers typically involved in the review can guide decisions in terms of what is best for the business, as opposed to what is technically more pleasing or elegant.
- Provide measurable deliverables to the GC CIO to assist in decision-making.
- Architecture reviews can serve as a way for the architecture organization to engage with development projects that might otherwise proceed without involvement of the architecture function.

ESA processes will be aligned with the GC ITARB as it is further developed.

2.3.4 Monitoring

2.3.4.1 Security Measurement and Monitoring Strategy

ESA target architectures and security patterns will help translate abstract policy and business requirements into more tangible security controls within an information system and provides a mechanism for security measurement. Security measurement is important for assessing the current security status and help to identify specific security controls that are implemented incorrectly, are not implemented, or are ineffective. Security measurement can enable the GC to quantify improvements in securing information systems and demonstrate quantifiable progress in accomplishing GC strategic goals and objectives. A strategy will be developed to ensure that controls are monitored on an ongoing basis, remain effective and are updated as required.

2.3.4.2 Horizontal Performance Measurement Strategy (HPMS)

At the ESA program level, monitoring of performance using metrics enables management to ensure that goals are achieved. The Horizontal Performance Measurement Strategy (HPMS) is a Public Safety led initiative to monitor performance of initiatives identified under Pillar 1. For ministerial reporting, TBS is the lead to collect the data from Pillar 1 departments and provide the consolidated data to PS for inclusion in the ministerial report. TBS will collaborate with SSC and CSEC, as well as the Canadian Security Intelligence Service (CSIS) to ensure that the evaluation reporting reflects the intent of the funding allocated for Pillar 1 activities.

2.4 Program Deliverables

This section describes a non-exhaustive list of deliverables that will be developed to meet program objectives. In some cases, the deliverables are living documents that are refreshed on a periodic cycle and may include multiple instantiations depending on the specific scope of the work stream or priority.

Deliverable	Description
1. Program Charter	An overview of the program vision, mission, objectives, governance, and roles and responsibilities that make up the program.
2. Program Implementation Framework	A document that provides an overview of the ESA operational model including key processes for escalating issues, assigning authorities, engaging governance, architecture compliance, architecture change management, etc.
3. Communications Plan	A document to create awareness and understanding of the ESA objectives, through communication to appropriate stakeholders and users throughout the GC. It will cover required messages, target audiences, and communication mechanisms/channels and will help to communicate the business value of the program including how deliverables of the program will be shared with the community.
4. Architecture Framework	A collection of tools, techniques, taxonomy, principles, artifact descriptions, process models, reference models and guidance used by architects in the production of enterprise-level IT security architectural artifacts.
5. Requirements Matrix	A tool to enable traceability from various sources of high-level requirements to the selection of security controls. The tool will help to track the status of individual requirements (including all rejected requirements) during the design, development and implementation of an information system.
6. Requirements Management Tool & Architecture Repository	A tool to manage and store the architectural artifacts including requirements matrices, security patterns, and target architectures. The tool must support artifacts developed for IT security architectures designs for Protected B and Secret environment.

Deliverable	Description
7. Work Plan	An integrated work plan that includes high-level summaries of the projects that make up the program and identifies activities and interdependencies within each work package so that resources can be effectively utilized.
8. Backgrounder Paper	An overview of the GC IT Security Strategy that will support the delivery of a secure GC IT architecture.
9. Target Architectures	A collection of architecture descriptions, models, use cases, etc. that enable the creation of building blocks that form the foundation and meet the vision and strategy of the program. It will include security patterns for the “target” or “to-be” architecture, describing the desired, future state and incorporates the minimum enterprise security controls.
10. Transition Strategies & Roadmaps	A document that defines a transition strategy and plan that documents the incremental approach for meeting target architectures. It outlines the priorities, scope, work packages and milestones and all relevant transition states of the architecture that are necessary for effective realization of the target architecture.
11. Threat Assessment	Development of a GC threat assessment that is continuously updated to provide departments with direction on what threats they should be concerned about.
12. Risk Spectrum Definition	Completion of the risk spectrum definition in ITSG-33 that will cover all the classification levels and is required for Secret, Confidential and Top Secret information. These definitions will provide support for CSEC Commercial Solutions for Classified (CSFC) Program and to meet vision for ESA.
13. Security Measurement and Monitoring Strategy	A document that outlines a strategy to ensure that security controls are implemented correctly, monitored on an ongoing basis to ensure effectiveness, and updated as required.

2.5 Preliminary Risks

This section outlines the initial risk assessment for the program. Early identification of risks and on-going strategic management of those risks will be performed on a regular basis.

No.	Risk Description	Probability (H/M/L)	Impact (H/M/L)	Planned Mitigation
1.	There is a risk that there will be a lack of resources (funding, people, etc.) to support the delivery of the desired initiatives.	High	High	• Develop strategies to obtain resources with the appropriate skillsets • Engage with private sector contractor resources on an as-needed basis

No.	Risk Description	Probability (H/M/L)	Impact (H/M/L)	Planned Mitigation
2.	There is a risk that decisions will be made without considering potential enterprise-wide impacts across the GC.	High	High	• Identify and communicate evidence of real issues, risks that need to be avoided and benefits to be gained (in business terms) relating to proposed improvements • Formalise ESA governance roles and responsibilities so that accountability for decisions is clear • Develop a generic threat assessment (TA) for the GC that can be leveraged for departmental TAs and information-specific TAs • Develop a communications plan to promote the ESA program and artifacts that can be leveraged by departments
3.	There is a risk that the architecture methodology used for developing the IT security architectures will be difficult to apply in a practical manner or will not be adopted across the GC.	High	High	• Security architectures must be focused on specific business objectives to minimize this risk • Develop security patterns and tools to guide implementation • Leverage and communicate with the ESA Interdepartmental Working Group for peer review of architecture artifacts • Engage industry to leverage private sector experience and support for architecture development and forecasts
4.	There is a risk that there will be no alignment between business requirements and IT security architectures.	Medium	High	• Integrated project team to ensure collaborative approach amongst key stakeholders. • Representation from each of these communities is required to minimize this risk • Develop an integrated work plan based on GC priorities • Align with GC ITARB processes • Develop strategy for managing security requirements and ensuring architecture compliance

No.	Risk Description	Probability (H/M/L)	Impact (H/M/L)	Planned Mitigation
5.	There is a risk that long-term commitment to the program will diminish over time.	Medium	Medium	• Foster open and transparent communication about performance, with links to PSC-led Horizontal Performance Management Strategy (as part of CCSS performance measurement) • Identify a combination of short-term, quick hits, projects that emphasize value and longer term infrastructural and cultural change projects will provide incremental increases in program quality • Publish positive outcomes and lessons learned to help establish and maintain credibility
6.	There is a risk that policies will not be updated in a timely fashion to address new work models and technology impacts.	Medium	Medium	• A feedback mechanism must be developed to trigger updates outside of the policy lifecycle and must consider changes to the environment that necessitate the review and update of existing policies, or the need for new policies. • Develop a security measurement and monitoring strategy to ensure that security controls are implemented correctly, monitored on an ongoing basis to ensure effectiveness, and updated as required.

2.6 Key Success Factors

This section defines the success factors for this program. These include, but are not limited to, the following:

- The delivery of an Enterprise Security Architecture Program that is understood, accepted, communicated, and used to make informed planning decisions including a common understanding of the alignment between business, information, and technology in the current GC environment;
- A clear understanding of the benefits, effort, risks, and feasibility of taking action on the Enterprise Security Architecture Program;
- Visible leadership and commitment from senior management by active participation;
- A governance structure that is understood, accepted, and used to make informed planning decisions;
- Organizational responsibilities and structures to support the architecture governance processes and reporting requirements; and
- Adequate funding, skilled human resources, and resource commitment.

3. Business Sponsorship and Program Stakeholders

3.1 Key Stakeholders

The Policy on Government Security describes the roles and responsibilities of departments and Lead Security Agencies. Lead security agencies are mandated to provide advice, guidance and services to other departments to support the day-to-day security operations of departments and enable government as a whole to effectively manage security activities, coordinate response to security incidents, and achieve and maintain an acceptable state of security and readiness.

- **Treasury Board of Canada Secretariat (TBS)** establishes and oversees a whole-of-government approach to security management and monitors the adequacy of services to support these activities and practices across government. TBS exercises strategic oversight of government security, provides leadership, sets government-wide direction, establishes priorities, and defines and formalizes security management requirements. This includes activities such as setting policies, establishment of service standards and providing direction on measures for managing security incidents.

- **Communications Security Establishment Canada (CSEC)** provides leadership and coordination for departmental activities that help ensure the protection of electronic information and information systems of importance and serves as the government's national authority for SIGINT and COMSEC. CSEC provides services to departments for predicting, preventing and defending against sophisticated IT security incidents, threats and vulnerabilities and for providing support services for security architecture design for GC shared, common or federated initiatives, and tailored engineering and operational support for information infrastructure projects of importance to the GC.

- **Shared Services Canada (SSC)**[2] is responsible for ensuring the confidentiality, integrity and availability of shared IT services provided to departments. This includes incident management, response and recovery activities, as well as a suite of information security services and their respective interfaces to departmental IT infrastructures.

The desired results for the enterprise IT security architecture can only be achieved through the collaboration of departments and agencies that each have specific roles in designing and implementing the GC enterprise IT security architecture as depicted in the figure below.

[2] SSC is not currently defined as a Lead Security Agency in the Policy on Government Security as it predates the creation of the department.

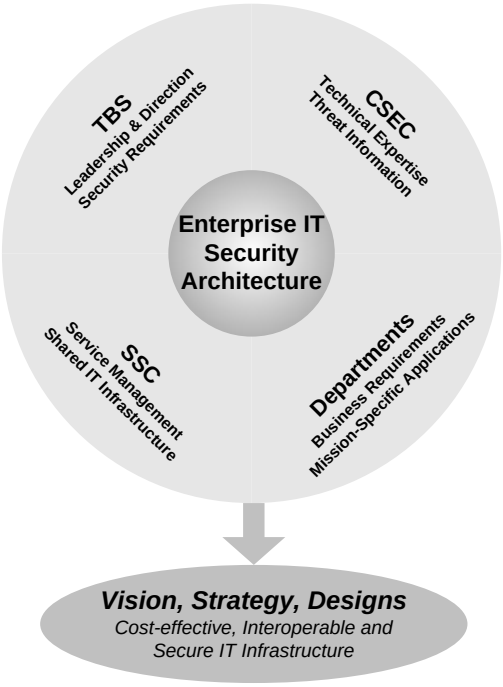


Figure 5 – ESA Key Stakeholders

For the enterprise IT security architecture initiative, as outlined in the 2012 *cyber security initiative,* responsibilities are as follows:

TBS will lead the establishment of the enterprise security architecture for the GC IT infrastructure by:

- Developing a long term vision and establishing priorities;
- Developing a coordinated work plan;
- Leading the development of strategies and designs to secure the enterprise IT infrastructure and establish enterprise IT security services;
- Coordinating and aligning enterprise IT security architecture activities with other initiatives to avoid duplication of effort and to ensure all needs are requirements are addressed;
- Harnessing industry expertise and experience as required;
- Ensuring that shared IT services achieve an appropriate level of security before they enter production/operation; and
- Developing or updating supporting GC-wide directive and policies to facilitate the implementation and oversight of standard IT security measures across the GC.

CSEC will support TBS in the establishment of the security architecture for the GC IT infrastructure by:

- Providing support for system security concepts and risk management activities;
- Supporting and reviewing high-level architectures for security-critical components;
- Providing cyber threat assessments to support enterprise architecture designs;
- Providing specialized technical expertise to identify solution concepts that protect GC assets, including the data and IT infrastructure, from sophisticated threats; and
- Providing security advice for emerging new technologies before they are introduced in the security architecture.

SSC will collaborate with TBS and CSEC on the design of the enterprise security architecture to ensure that controls are feasible, implemented in a timely manner, and do not unduly inhibit operations. It will achieve this by:

- Develop Cyber and IT security strategies, policies and assessments for IT services within SSC mandate in accordance with GC standards and policies;
- Developing and implementing designs based on approved architecture artifacts for consolidated IT infrastructure services;
- Implement architectures via a standardized service delivery approach based on GC IT Architecture Review Board (GC ITARB) approved architectures;
- Deploy approved solution architectures following an approved SDLC risk managed gating approach;
- Develop acquisition documents (e.g. RFPs) based on approved business-driven architectures and ConOps recommended by the ESA subject matter experts; and
- Report on implemented security controls and various KPIs.

Departments and Agencies

- Participating in the development of designs and identifying security requirements that satisfy departmental program needs; and
- Developing designs for departmental security services that are aligned with the enterprise IT security architecture.

3.2 Program Governance

Strengthening the IT infrastructure requires cross-departmental interaction, cooperation, and execution. To that end, a governance structure will be established to ensure the ESA activities are coordinated and limited resources are utilized efficiently. TBS-CIOB will lead the coordination of the program and has established a governance structure to facilitate the efficient implementation of the GC ESA program objectives, avoid duplication of effort and ensure all interests and requirements are addressed from a GC enterprise wide perspective.

To provide focused IT Security governance for addressing the horizontal initiatives for CCSS Pillar 1 activities, three standing executive committees comprised of executives from TBS-CIOB, CSEC and SSC have been established as outlined below:

- Deputy Minister (DM) Committee will focus on establishing DM-level strategic direction;

- Assistant DM (ADM) IT Security Tripartite will focus on setting priorities, aligning resources and monitoring results for the evolution of enterprise technology; and

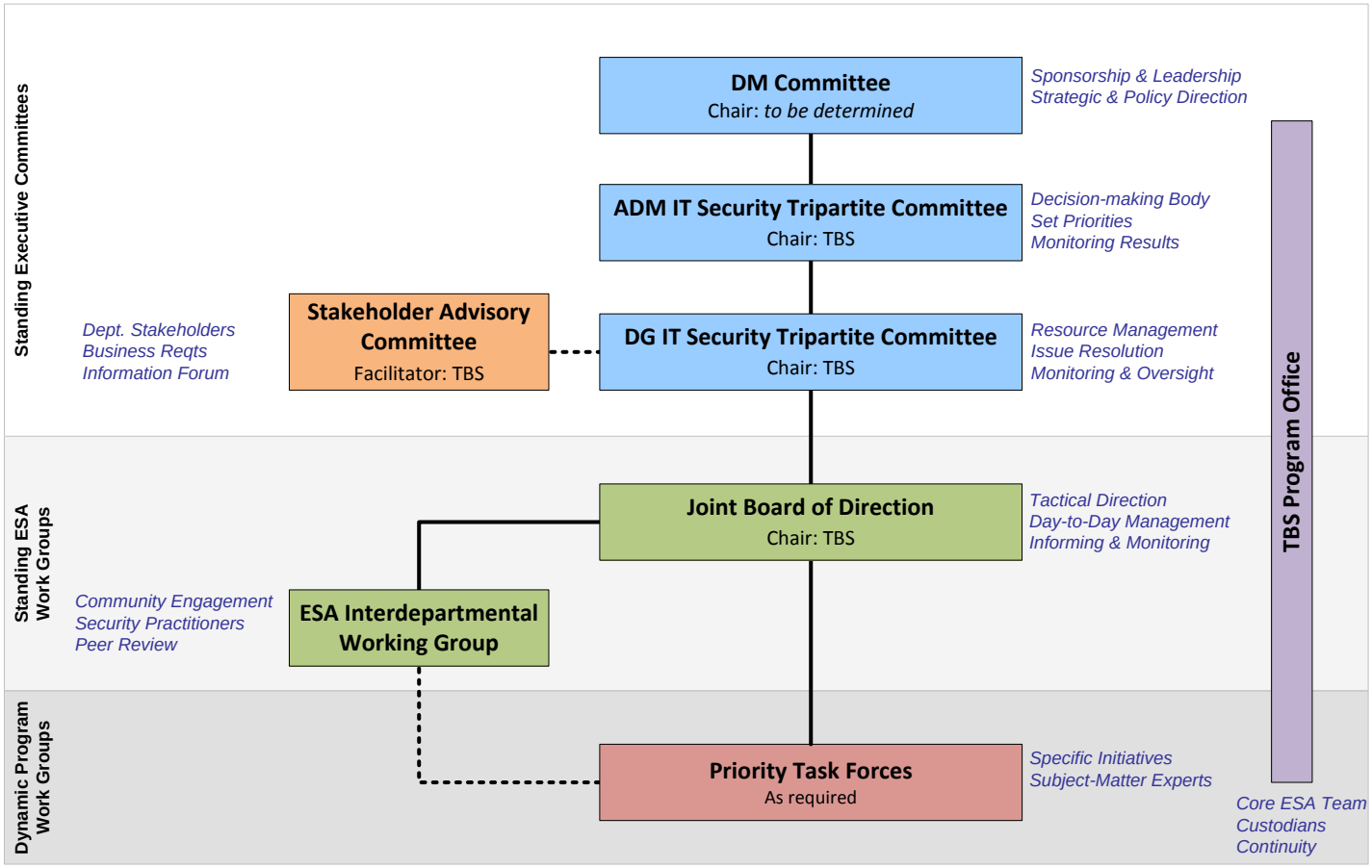
- Director General (DG) IT Security Tripartite will support the ADM Tripartite and will engage with business leads from various departments as part of the Stakeholder Advisory Committee.

In addition, the Director-level Joint Board of Direction has been stood up to provide day-to-day program management and tactical direction, and will establish dynamic work groups of subject-matter experts (SMEs) as required to develop specific initiatives. These SMEs are members of the ESA Interdepartmental Working Group which will provide a forum for security practitioners to review and provide inputs into the development of the GC Enterprise Security Architecture. Further details on these committees and working groups are included in the Roles and Responsibilities described in Section 4 of this document.

Support and direction from key stakeholders are critical so that improvements are adopted and sustained. Stakeholder Advisory Committee has been established as an information forum in the governance structure and to represent departmental business, IT and IT security requirements and concerns. All

stakeholders should be considered when making benefit, risk and resource assessment decisions. Stakeholder advisory committee can provide inputs to identify important initiatives that require access to experts who understand threats, IT risks, compliance requirements, and how to mitigate risks through technical and nontechnical controls.

The following figure depicts the program governance structure.



Tripartite membership includes TBS, CSEC & SSC

Figure 6 – ESA Program Governance

3.3 Relationship to GC Security Governance

The following figure depicts the relationship of the IT Security Tripartite with the current GC Security Governance Structure. The scope of the GC Security Governance is broader than IT. The IT Security Tripartite consists of members from the ADM Security and Identity Committee, the Lead Security Agency Steering Committee (LSA SC). The IT Security Tripartite will align through the LSA SC and ADM SIDC. Communications will be required to both the DSO and ITSC community as well as to the Chief Information Officer Council (CIOC), which it the GC CIO's advisory body.

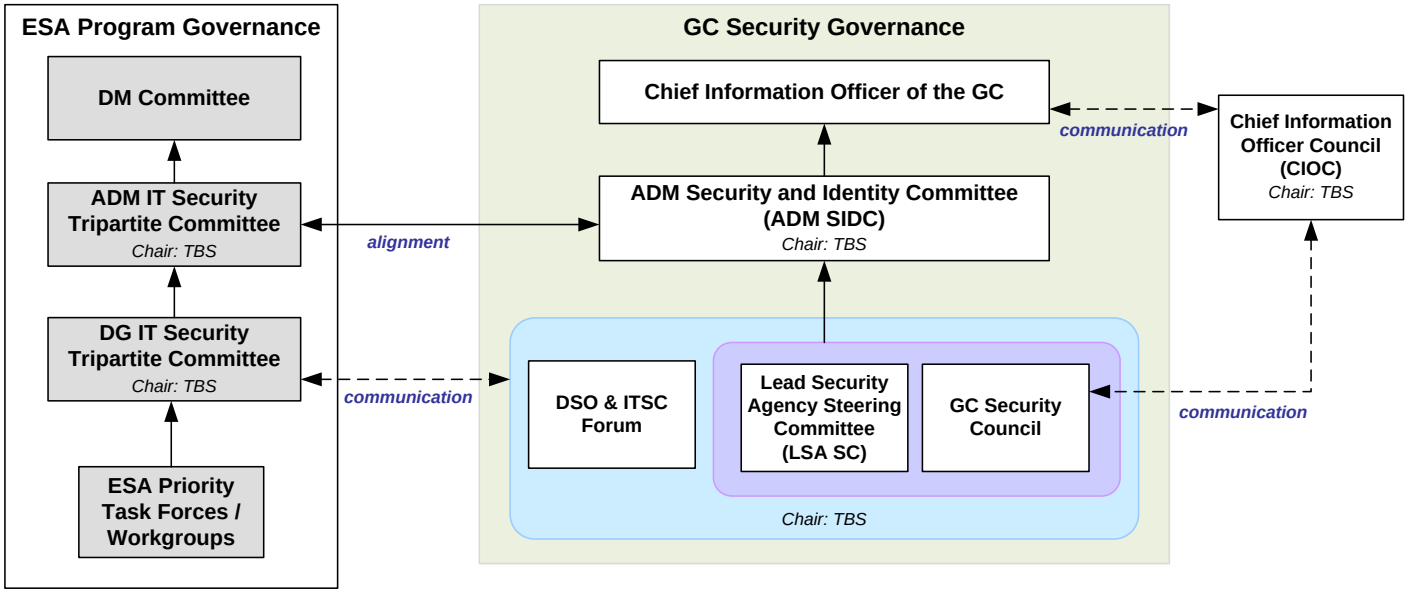


Figure 7 – Relationship Between ESA Program Governance and GC Security Governance

3.4 Relationship to Project Governance

There is a strong relationship between the ESA program governance as it relates to project governance. ESA program management involves coordination of the projects related to the ESA initiatives that in aggregate achieve an overarching set of objectives and focuses on integration, communications and control over program resources and priorities. Projects have more specific and more singular objectives. Thus, program management addresses the management of project management, setting up processes, monitoring and measuring project results, and coordinating related projects. The following figure is a notional representation of the relationship between the ESA program governance and a project governance structure. Within the project governance, there may be internal governance structures that impact and influence the projects. Alignment between ESA program governance, project governance and internal governance structures are required to ensure efficient and secure delivery of the system or solution.

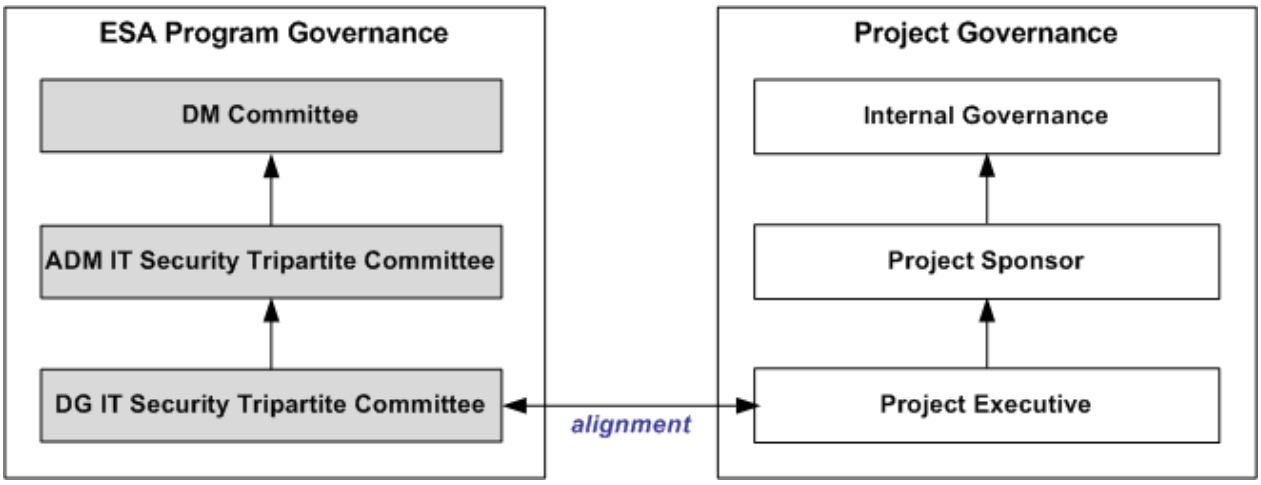


Figure 8 – Relationship Between ESA Program Governance and Project Governance

4. Roles and Responsibilities

This section describes the detailed roles and responsibilities (R&R) of the program stakeholders and supporting committees that have a significant influence on the program delivery.

4.1 Summary of Roles and Responsibilities – Governance Level

Role	Assigned	Duties and Responsibilities
Executive Sponsors	DM Committee	• Deputy Minister (DM) Level Committee • Provide strategic direction and guidance toward the prioritization of enterprise-wide IT security initiatives (focus of the 2012 GC cyber security initiative) • Establish over-arching enterprise IT security priorities for the Government of Canada • Set strategic and policy direction in the area of IT security for the Government of Canada • Address issues or resolve problems relating to specific IT security priority initiatives
Executive Oversight Committee	ADM IT Security Tripartite (ADM ITST) Committee *Consists of Deputy CIO, TBS; Senior ADM, SSC; Deputy Chief, IT Security, CSEC*	• Assistant Deputy Minister (ADM) Level Committee • Provides DM-level committee with guidance toward setting strategic and policy direction in the area of IT security for the Government of Canada • Serves as a decision-making body supporting the effective design, delivery and management of enterprise IT security related initiatives • Establish priorities for horizontal IT security initiatives that align with enterprise strategic objectives • Provides direction and oversight to DG ITST to resolve issues that are impeding the progress of horizontal IT security initiatives • Monitors the results of the horizontal IT security initiatives
Steering Committee	DG IT Security Tripartite (DG ITST) Committee *Consisting of Executives from TBS-CIOB, SSC-PCRB/Business Solutions, SSC-TSSD/EAS, SSC-Operations/National Security Portfolio, CSEC*	• Director General (DG) Level Committee • Align IT security strategic priorities with the enterprise direction established by ADM and DM-level tripartite committees • Provide advice, guidance, oversight, and direction to address significant issues of coordination, implementation, timelines and other obstacles that may impact progress of enterprise IT security initiatives • Monitors the progress and health of horizontal projects and initiatives related to enterprise IT security on an ongoing basis • Provides ADM and DM-level tripartite committees with guidance toward setting strategic and policy direction in the area of IT security for the Government of Canada • Reports on a regular basis to the ADM ITST on the status and health, as well as risks and issues along with mitigation strategies, in relation to enterprise IT Security initiatives • Reviews documentation intended for ADM ITST Steering Committee • Provides direction and oversight to individual working groups

Role	Assigned	Duties and Responsibilities
Advisory Committee	Stakeholder Advisory Committee *Consisting of Executives from TBS, SSC, CSEC, DFAIT, DND, PS, etc.*	• Provides an interdepartmental senior management forum to guide the ESA program, facilitate agreements between departments and resolve interdepartmental issues • Represent and communicate client department's priorities and business requirements • Assist with prioritizing security initiatives in support of the ESA strategic plan • Provide departmental input and guidance to the scope, planning and implementation of the ESA initiatives
Management Committee	Joint Board of Direction *Consisting of Directors from TBS, SSC, and CSEC*	• Director Level Committee • Responsible for providing direction and guidance to day-to-day program-level delivery including resource management • Coordination of interrelated activities to ensure delivery on commitments and objectives are achieved including establishment of dynamic program work groups as appropriate • Ensure overall alignment with long term strategy, broader ESA program direction, architecture and policies and ensure that gaps and overlaps are identified and addressed • Resolving ambiguities, issues, or conflicts that have been escalated and identify emerging risks and compliance issues • Recommend higher level approval of deliverables to DG ITST • Monitor progress of implementation activities on a regular basis
Architecture Review Board *(Under development)*	GC ITARB Dept. ITARB	• Provide leadership for the IT architecture process across the GC and provides strategic counsel to Chief Information Officers (CIOs) • Reviewing architectures of departmental IT-enabled projects that have satisfied the entry criteria for escalation to the GC ITARB • Assessing review requests from departments for prioritization and inclusion in the GC ITARB work-plan as departmental entry criteria dictate • Reviewing the architectures of IT-enabled projects should they span more than one department or is a shared or common government asset • Performing an architectural review of any IT-enabled project at the behest of the GC CIO

4.2 Summary of Roles and Responsibilities – Program Management Level

Role	Assigned	Duties and Responsibilities
Program Owner	Federal CIO	• Overall responsibility of the Enterprise Security Architecture Program • Provide leadership to the program • Promote collaboration and cooperation among organizational entities
Program Office	TBS-CIOB/ Security Division	• Responsible for overall program delivery and management • Develop, implement and manage program wide processes to account for program level risk, program change and issues management • Developing an integrated work plan to address work activities, priorities, timelines and milestones • Oversee and advise ESA workgroups and sub-working groups • Custodians of architecture tools and repository • Manage the meeting minutes, agendas, terms of references for the committees and work groups including promulgation of meeting outputs to ensure that escalations and reviews happen at the right levels on time. • Harmonize the reporting to TBS on the GC cyber security initiative positions and outcomes as part of the Public Safety Canada (PSC) Horizontal Performance Management Strategy • Effect regular and accurate communications with senior management, governance committees and departments on progress

4.3 Summary of Roles and Responsibilities – Architecture Development

Role	Assigned	Duties and Responsibilities
Subject Matter Experts	Priority Task Forces *TBS-CIOB* *CSEC* *SSC*	• Provide subject matter expertise and contribute to key decisions and issues relating to the ESA work priorities • Participate in defining ESA requirements, architectures, and roadmaps for ESA work priorities • Identify emerging risks and compliance issues to JBD as appropriate • Provide regular updates and recommendations to Joint Board of Direction on resolution of issues that are impeding implementation and change requests that have a major impact on program scope or schedule • Ensure regular representation at the working group meetings
Security Practitioners	ESA Interdepartmental Working Group	• Members of the ESA Interdepartmental Working Group lead by TBS-CIOB • Acts as a “clearing house” and peer review for major initiatives/common services • Review and recommend proposed changes to architecture designs • Identify emerging risks and compliance issues • Ensure regular representation at the working group meetings

5. Key Terms and Definitions

Term	Definition
Architecture Definition	The deliverable container for the core architectural artifacts created for a given IT security architecture view. An ADD examines all relevant states of the architecture (a baseline, one or more transition, and a target architecture).
Architecture Description	A document that provides a detailed description of the architectural approach that will realize a particular solution in support of the Business (IT) Services. It is the architecture blueprint of the solution and will include descriptions of various views of the solution such as systems engineering, enterprise security, communications, data flow, enterprise manageability. It enables further gap analysis to be performed with the identification of the detailed Baseline (or Current) Architecture and detailed Target Architecture. It also includes high-level implementation recommendations to transition from current state to target state.
Architecture Roadmap	An Architecture Roadmap lists individual work packages that will realize the Target Architecture and lays them out on a timeline to show progression from the Baseline Architecture to the Target Architecture.
Architecture View	A perspective from which an architecture may be viewed in order to ensure that a specific topic is considered in a coherent manner.
Baseline Architecture	Describes the current state for an enterprise architecture.
Control Objectives	A statements of desired results or purposes to be achieved by implementing security controls (adapted from COBIT)
Enterprise Security Architecture Definition Document (EADD)	Provides sufficient high-level and context-specific information that it can be used by managers and technical staff to rapidly develop and deploy solutions that satisfactorily address the identified security concerns and requirements, and to do so without the need to reference other sources. The document includes an executive summary, a problem statement, a list of high-level business and technical requirements, business and design constraints, a *Target Architecture*, a *Transition Strategy and Roadmap* and *Intermediate Architecture(s)* for one or more steps along the transition strategy.
Enterprise IT Security Architecture	The translation of government-wide IT security vision and strategy into effective enterprise change by creating, communicating and improving the key requirements, principles and models that describe the enterprise's future IT security state and enable its evolution.
Enterprise IT Security Architecture Framework	A collection of tools, techniques, artefact descriptions, process models, reference models and guidance used by architects in the production of enterprise-level IT security architectural artifacts.
Intermediate Architecture	Provides detailed and context-specific information required to implement one of the transition states described in a transition strategy and roadmap.
Reference Architecture	A predefined architectural pattern, or set of patterns, possibly partially or completely instantiated, designed, and proven for use in particular business and technical contexts, together with supporting artifacts to enable their use. *(From Rational Unified Process)*
Residual Risk	Level of risk remaining after security measures (controls) have been applied
Risk	The uncertainty that can create exposure to undesired future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to impede the achievement of an organization's objectives
Risk management	A systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk issues *(From IRMF)*

Term	Definition
Security Control	An administrative, operational, technical, physical or legal measure for managing security risk. This term is synonymous with safeguard. *(From Guideline on Developing a Departmental Security Plan)* Safeguard or countermeasure to avoid, counteract or minimize security risks. *(From ITSG-33)*
Security Design Pattern	A general reusable solution to a commonly occurring problem in creating and maintaining secure information systems.
Security Requirements Traceability Matrix	A tool used to trace the correspondence between high-level business and security requirements through successively more detailed designs.
Security risk	An expression of the likelihood and impact of events with the potential to cause injury to information, assets, individuals or services
Solution Architecture	Adds an implementation layer to the intermediate architecture. Describes “how” specific security controls will be implemented (e.g., the security control will be implemented using the following mechanism …). A solution architecture is immediately “implementable”; it includes sufficient detail that no additional architectural decisions are required to implement a solution.
Target Architecture	Defines a future state for an enterprise architecture that the GC will strive to achieve.
Transition Architecture	Shows the enterprise at an architecturally significant state between the Baseline and Target Architectures.
Transition Strategy and Roadmap	Outlines an incremental approach to evolve from current state to the target architecture. Each transition state described in a roadmap provides a clear milestone with measurable business value.
Threat	An event or act, deliberate or accidental, that could cause injury to information, assets or individuals.
Vulnerability	An inadequacy related to security that could increase susceptibility to compromise or injury.

6. Acronyms and Abbreviations

Term or Acronym	Definition
ADM	Associate/Assistant Deputy Minister
BCP	Business Continuity Plan (aka Continuity of Operations Plan)
C&A	Certification and Accreditation
CIO	Chief Information Officer
CIOB	Chief Information Officer Branch
CSEC	Communication Security Establishment Canada
CSIS	Canadian Security Intelligence Service
DFAIT	Department of Foreign Affairs and International Trade
DG	Director General
DM	Deputy Minister
DND	Department of National Defence
EA	Enterprise Architecture
EADD	Enterprise Security Architecture Description Document
ESA	Enterprise Security Architecture
GC	Government of Canada
ISSIP	Information System Security Implementation Process
IT	Information Technology
ITSG	IT Security Guidance
ITST	IT Security Tripartite
OPI	Office of Primary Interest
PIA	Privacy Impact Assessment
PSC	Public Safety Canada
R&R	Roles and Responsibilities
RACI	Responsible, Accountable, Consulted, Informed
RDIMS	Records and Document Information Management System
SRTM	Security Requirements Traceability Matrix
SOW	Statement of Work
SPC	Services partagés Canada
SSC	Shared Services Canada
TA	Threat Assessment
TBD	To be determined
TBS	Treasury Board Secretariat
TRA	Threat and Risk Assessment

7. References

More information concerning this program and the various projects can be found in the following documents:

Document Title	Version No.	Date	Author and Organization	Location (link or path)
Canada Cyber Security Strategy		2010	Public Safety	http://www.publicsafety.gc.ca/prg/ns/cbr/ccss-scc-eng.aspx
IT Modernization Strategy	V0.9	25 July 2012	TBS-CIOB	
Strengthening the Security of Federal Cyber Systems: A Backgrounder	V1.1	March 2013	TBS-CIOB	
Framework for the Management of Risk		27 Aug 2010	TBS	http://publiservice.tbs-sct.gc.ca/pol/doc-eng.aspx?id=19422&section=text
Policy on Government Security		1 April 2012	TBS	http://publiservice.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578&section=text
Directive on Departmental Security Management		1 July 2009	TBS	http://publiservice.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16579&section=text
Operational Security Standard: Management of IT Security			TBS	http://publiservice.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12328&section=text
Open Security Architecture			OSA	http://www.opensecurityarchitecture.org/cms/
The Open Group Architecture Framework (TOGAF)	V9.1		The Open Group	http://pubs.opengroup.org/architecture/togaf9-doc/arch/index.html
Enterprise Security Architecture: A Business-Driven Approach (SABSA)		2005	SABSA	http://www.sabsa-institute.org/publications.aspx
IT Security Risk Management: A Lifecycle Approach (ITSG-33)		March 2012	CSEC	
ESA Framework	V0.3	June 2013	TBS-CIOB	GCDOCS# 1128800
COBIT 5 for Information Security	V5	2012	ISACA	https://www.isaca.org/COBIT/Pages/info-sec.aspx
A Systematic, Comprehensive Approach to Information Security	G00204023	24 June 2010	Gartner	
Information Technology Architecture Review Board Concept of Operations Guideline	V0.06		TBS-CIOB	
A Guide to Project Gating for IT-Enabled Projects			TBS-CIOB	http://publiservice.tbs-sct.gc.ca/itp-pti/pog-spg/irp-gpgitep/irp-gpgitep00-eng.asp