IT Governance Framework & Information Security Governance

VCPL-SEC-22-V1.0

DOCUMENT AND RECORD CONTROL

Version Control

Document Control ID	VCPL-SEC-22_IT Governance Framework & Information Security Governance-V1.0
Issued Date	16-September-2022
Effective Date:	16-September-2022
Owner:	IT

Revision Table

Date	Version	Affected Sections	Author
16-September-2022	Draft		Mr Ramesh T.P

Release Authorization

Task	Author	Title
Prepared by	Mr Ramesh T.P	Deputy Vice President

Reviewer Authorization

Name	Title	Signature	Date
Mr. Prasenjit Datta	Head of Technology	Prasenjit Datta	16-September-2022

Approval Authorization

Name	Signature	Date
Board of Directors		

TABLE OF CONTENTS

1. IT Governance Framework

1.1 What is IT Governance?

IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives.

The purpose of IT governance is to direct IT endeavours, to ensure that IT's performance meets the following objectives:

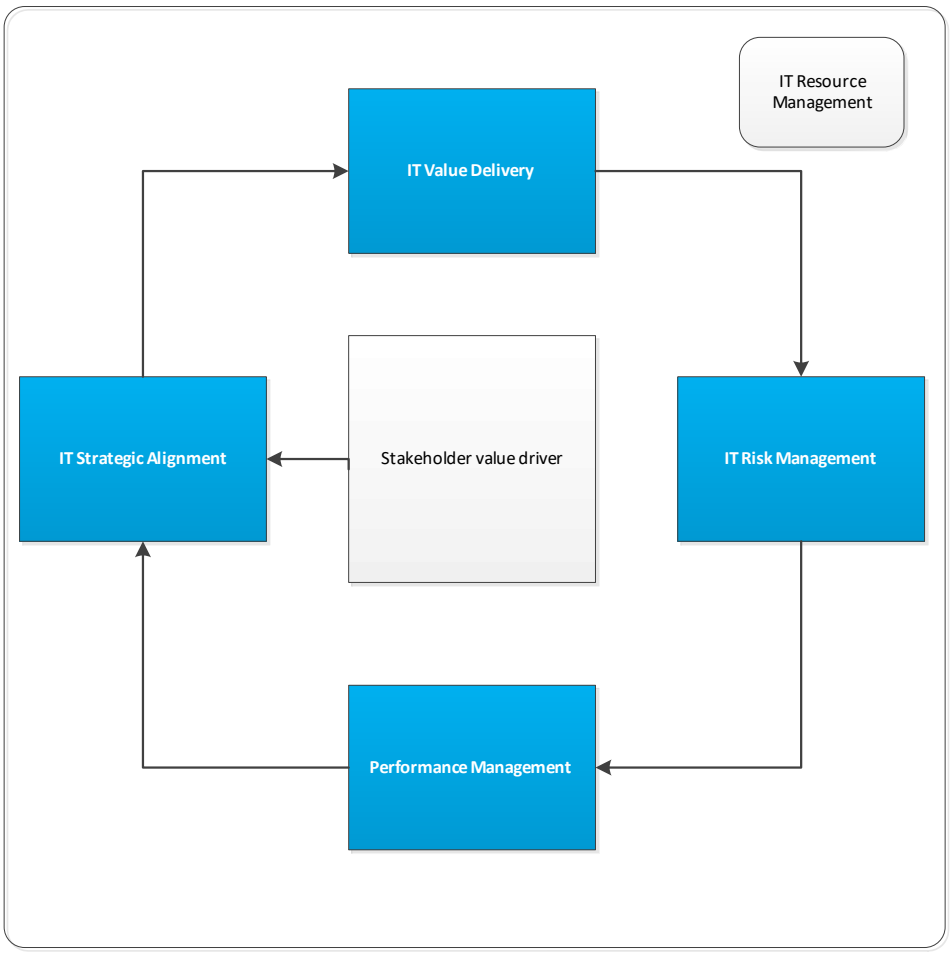
- Alignment of IT with the enterprise and realisation of the promised benefits
- Use of IT to enable the enterprise by exploiting opportunities and maximising benefits
- Responsible use of IT resources
- Appropriate management of IT-related risks

1.2 What Does IT Governance Cover?

Fundamentally, IT governance is concerned about two things: IT's delivery of value to the business and mitigation of IT risks. The first is driven by strategic alignment of IT with the business. The second is driven by embedding accountability into the enterprise. Both need to be supported by adequate resources and measured to ensure that the results are obtained.

This leads to the five main focus areas for IT governance, all driven by stakeholder value. Two of them are outcomes: value delivery and risk management. Three of them are drivers: strategic alignment, resource management (which overlays them all) and performance measurement.

- **Strategic Alignment**, with focus on aligning with the business and collaborative solutions
- **Value Delivery**, concentrating on optimising expenses and proving the value of IT
- **Risk Management**, addressing the safeguarding of IT assets, disaster recovery and continuity of operations
- **Resource Management**, optimising knowledge and IT infrastructure
- **Performance Measurement**, tracking project delivery and monitoring IT services



Focus Area of IT Governance

IT governance is a continuous life cycle, which can be entered at any point. Usually, one starts with the strategy and its alignment throughout the enterprise. Then implementation occurs, delivering the value the strategy promised and addressing the risks that need mitigation. At regular intervals the strategy needs to be monitored and the results measured, reported and acted upon. Generally, on an annual basis, the strategy is re-evaluated and realigned, if needed.

This life cycle does not take place in a vacuum. Each enterprise operates in an environment that is influenced by:

- Stakeholder values
- The mission, vision and values of the enterprise
- The community and company ethics and culture
- Applicable laws, regulations and policies
- Industry practices

IT governance is also a process in which the IT strategy drives the IT processes, which obtain resources necessary to execute their responsibilities. The IT processes report against these responsibilities on process outcome, performance, risks mitigated and accepted, and resources consumed. These reports should either confirm that the strategy is properly executed or provide indications that strategic re-direction is required.

1.3 High Level IT Governance Implementation Plan

To get its IT governance initiatives headed in the right direction, the enterprise needs an effective action plan that suits its particular circumstances and needs. First, it is important for the board to take ownership of IT governance and set the direction management should follow. This is best done by making sure that the board operates with IT governance in mind:

- Making sure IT is on the board agenda
- Challenging management's activities with regard to IT, to make sure IT issues are uncovered
- Guiding management by helping it to align IT initiatives with real business needs, and ensuring that it appreciates the potential impact on the business of IT-related risks
- Insisting that IT performance be measured and reported to the board
- Establishing an IT strategy committee with responsibility for communicating IT issues between the board and management
- Insisting that there be a management framework for IT governance based on a common approach (e.g., COBIT)

With this mandate and direction in place, management then can initiate and put into action an IT governance approach. To help management decide where to begin and to ensure that the IT governance process delivers positive results where they are needed most, the following steps are suggested:

- **Set Up a Governance Organizational Framework** that will take IT governance forward and own it as an initiative, with clear responsibilities and objectives and participation from all interested parties.
- **Align IT Strategy with Business Goals.** What are the current business concerns and issues where IT has a significant influence, e.g., cost reduction, competitive advantage and/or merger/acquisition? Obtain a good understanding of the business environment, risk appetite and business strategy as they relate to IT. Identify the top IT issues on management's agenda.
- **Understand/Define the Risks.** Given top management's business concerns, what are the risk indicators relating to its ability to deliver against these concerns? Consider:
  - Previous history and patterns of performance
  - Current IT organizational factors
  - Complexity and size/scope of the existing or planned IT environment

- Inherent vulnerability of the current and planned IT environment
- Nature of the IT initiatives being considered, e.g., new systems projects, outsourcing considerations, architectural changes

- **Define Target Areas.** Identify the process areas in IT that are critical to managing these risk areas. Use the COBIT process framework as a guide.
- **Analyze Current Capability and Identify Gaps**. Perform a maturity capability assessment to find out where improvements are needed most. Use COBIT's management guidelines as a guide.
- **Develop Improvement Strategies.** Decide the highest priority projects that will help improve the management and governance of these significant areas. This decision should be based on most potential benefit and ease of implementation, and a focus on important IT processes and core competencies. Define specific IT governance projects as the first step in the IT governance continuous improvement initiative.
- **Measure Results.** Establish a balanced scorecard mechanism for measuring current performance. Monitor the results of new improvements considering, as a minimum, the following key considerations:
  - Will the organizational structures support strategy implementation?
  - Are responsibilities for risk management embedded in the organization?
  - Do infrastructures exist that will facilitate and support the creation and sharing of vital business information?
  - Have strategies and goals been communicated effectively to everyone who needs to know within the organization?
- **Repeat steps 2-7 on a regular basis.**

  There are also some obvious but pragmatic rules that management ought to follow:

  - Treat the IT governance initiative as a project activity with a series of phases rather than a "one-off" step.
  - Remember that IT governance involves cultural change as well as new processes, and therefore a key success factor is the enablement and motivation of these changes.
  - Make sure there is a clear understanding of the objectives.
  - Manage expectations. In most enterprises, achieving successful oversight of IT will take some time and is a continuous improvement process.
  - Focus first on where it is easiest to make changes and deliver improvements. Build from there one step at a time.

2. Information Security Governance

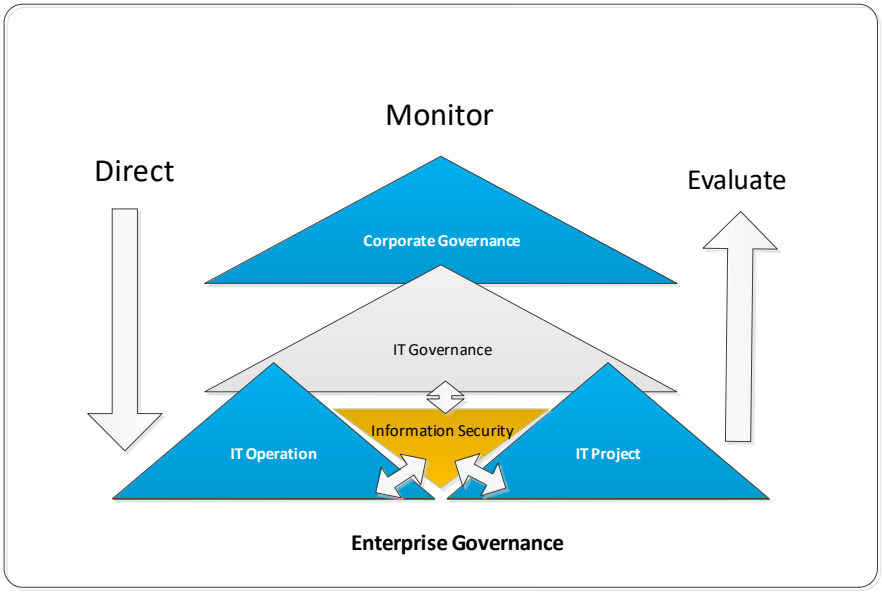
2.1 What is Information Security Governance?

IT governance is the responsibility of the board of directors and executive management. It must be an integral and transparent part of enterprise governance and be aligned with the IT governance framework. Whilst senior executive has the responsibility to consider and respond to the concerns and sensitivities raised by information security, board of directors will increasingly be expected to make information security an intrinsic part of governance, integrated with processes they already have in place to govern critical organisational resources.

To exercise effective enterprises and information security governance there are several matters that can be assist in focusing on the question, "what is information security governance?" These are

- Desired outcome of information security governance
- Knowledge and protection of information assets
- Benefits of information security governance
- Process integration

Information security is an important part of the enterprise's overall governance, IT operation and IT Projects (i.e., future state of IT). Information Security governance should not be practices only on IT, but it should one of the focus areas for any organization.



Information Security Governance Triangle

2.2 Benefit of Information Security Governance

Information security governance generates significant benefits, including:

- An increase in the share value for organizations that practice good governance.
- Increased predictability and reduce uncertainty of business operation by lowering information security – related risk to definable and acceptable level.
- Protection from the increasing potential for civil and legal liability as a result of information inaccuracy or the absence of due care.
- The structure and framework to optimize allocation of limited security resources.
- Assurance of effective information security policy and policy compliance.
- A level of assurance that critical decision is not based on faulty information.

2.3 How to Achieve Effective Information Security Governance

To achieve effective information security governance framework, management must establish and maintain a framework to guide the development and maintenance of comprehensive information security program.

The information security governance framework generally consists of:

- An information security risk management methodology.
- A comprehensive security strategy explicitly linked with business and IT objectives.
- An effective security organizational structure.
- A security strategy that talks about the value of information protected and delivered.
- Security policy that addresses each aspect of strategy, control and regulation.
- A complete set of security standards for each policy to ensure that procedures and guidelines comply with policy.
- Institutionalized monitoring process to ensure compliance and provide feedback on effectiveness and mitigation of risk.
- A process to ensure continued evaluation and update of security policies, standards, procedures and risks.

---End of Document---