The Institute of Cost Accountants of India

INFORMATION SYSTEM SECURITY AUDIT

BATCH: 5

DISSA
INFORMATION SYSTEM SECURITY AUDIT

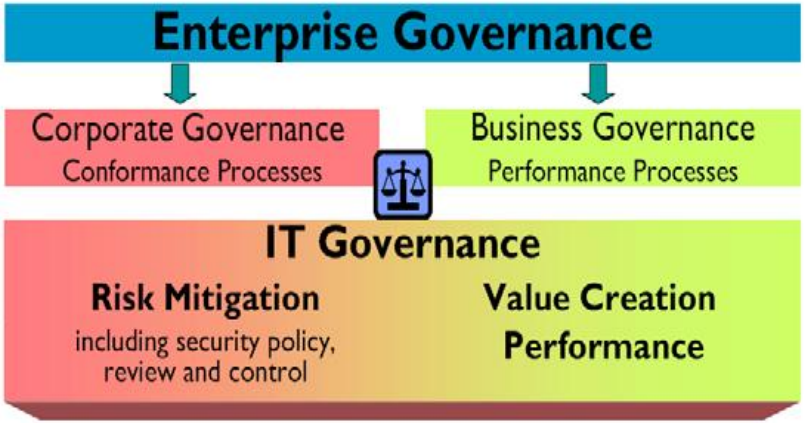
Elocutionist: Dr. Saurabh Maheshwari

Chapter - 2

COMPLIANCE AND SECURITY FRAMEWORK

GOVERNANCE

- ‘Corporate Governance’ differs from ’Business Governance’ in that CG is primarily about protecting a business, while BG is more about growing it. Corporate Governance refers to the policies and procedures set in place to ensure a business operates effectively within the law and for the optimal benefit of all stakeholders, while Business Governance is related to the operations of a business in an efficient manner.
- IT Governance (ITG) [COBIT 4.1] or Governance of enterprise IT (GEIT) [COBIT 5] or Enterprise Governance of IT (EGIT) [COBIT 2019], is the alignment of leadership, organizational structures, and processes to actualize and sustain the organizational objectives through the use of IT. Further, this also refers to IT governance in a manner that would be directed and controlled and consists of evaluating and monitoring the plans for the IT systems so that they are in alignment with the objectives of the organization.
  ITG / GEIT / EGIT is based on three pillars: (a) Ensure Benefits Realization (b) Optimize Resources and (c) Optimize Risks
- Enterprise governance is the structure and relationships that control, direct, and regulate an enterprise and its - projects, portfolios, infrastructure, and processes.



SYSTEMATIC APPROACH OF IMPLEMENTING ITG / GEIT / EGIT

1. Aligning IT Goals with Business Goals or [Establish the Desire to Change]
2. Formalize and implement the right IT Governance Processes [Choose a Governance Framework]
3. Establish the required IT Organization structure and Involve the Board of Directors/Executive Management in IT-related matters [Form an Effective Implementation Team]
4. Communicate Desired Vision to all Stakeholders and Finalize New Roles and Responsibilities
5. Plan, Align and Manage IT-Enabled Investment as a Portfolio
6. Enable Operations and Implement a Performance Measurement System Integrated with Regular Processes
7. Embed New Approaches
8. Establish Sustainability through Support, Monitoring, and Regular Communication

REGULATORY FRAMEWORKS

- Why a regulatory framework?
- Regulatory framework organizations / some common regulatory framework →
  - Sarbanes-Oxley (SOX)
  - PCI DSS
  - CMMI Model
  - ISACA's COBIT 2019
  - ISACA's ITAF
  - ISACA's COSO
  - NIST
  - HIPAA / HITECH
  - SSAE-16
  - AT-101
  - FedRAMP
  - ISO (International Organization for Standardization) [27000, 31000, 38500, 22301, etc.]
  - Privacy Shield (Replaced US-EU Safe Harbor)
  - Information Technology (Amendment) Act 2008
  - DPDPA 2023

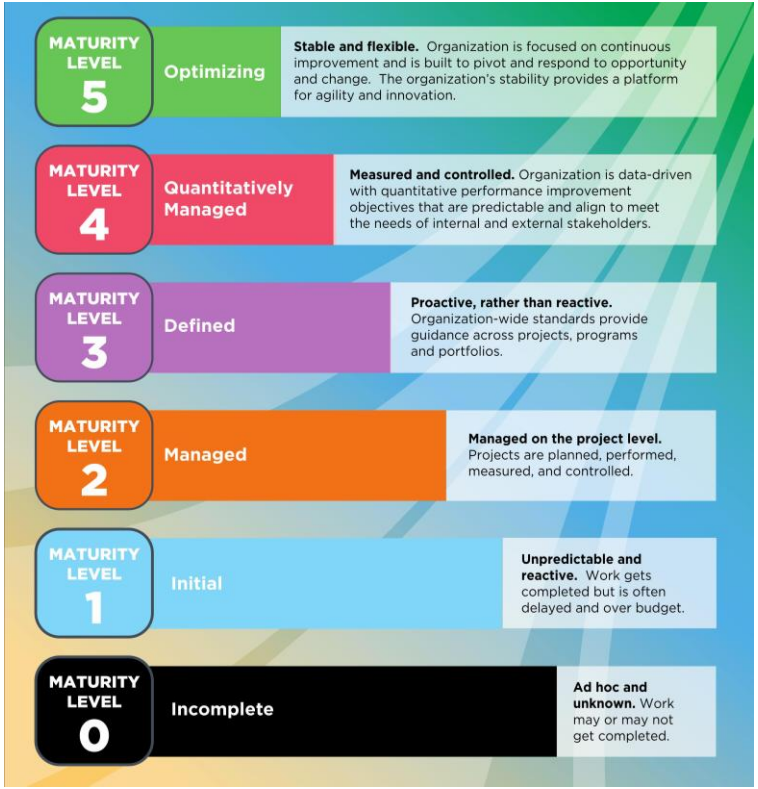
SOX

- The Sarbanes–Oxley Act of 2002 is a United States federal law that mandates certain practices in financial record keeping and reporting for corporations.
- The act is also known as the "Public Company Accounting Reform and Investor Protection Act" and "Corporate and Auditing Accountability, Responsibility, and Transparency Act“, contains eleven sections that place requirements on all U.S. public company boards of directors and management and public accounting firms.
- The law was enacted as a reaction to a number of major corporate and accounting scandals, including Enron and WorldCom. The sections of the bill cover responsibilities of a public corporation's board of directors, add criminal penalties for certain misconduct and require the Securities and Exchange Commission to create regulations to define how public corporations are to comply with the law.
- All provisions of SOX are directly or indirectly applicable in India through SEBI & MCA.

PCI DSS

- The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle cards related data and payment options from the major card schemes.
- The PCI Standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce card fraud.
- Compliances of PCI Data Security Standard is organized into six logically related groups called "control objectives".
  - Build and Maintain a Secure Network and Systems
  - Protect Cardholder Data
  - Maintain a Vulnerability Management Program
  - Implement Strong Access Control Measures
  - Regularly Monitor and Test Networks
  - Maintain an Information Security Policy

CMMI MODEL



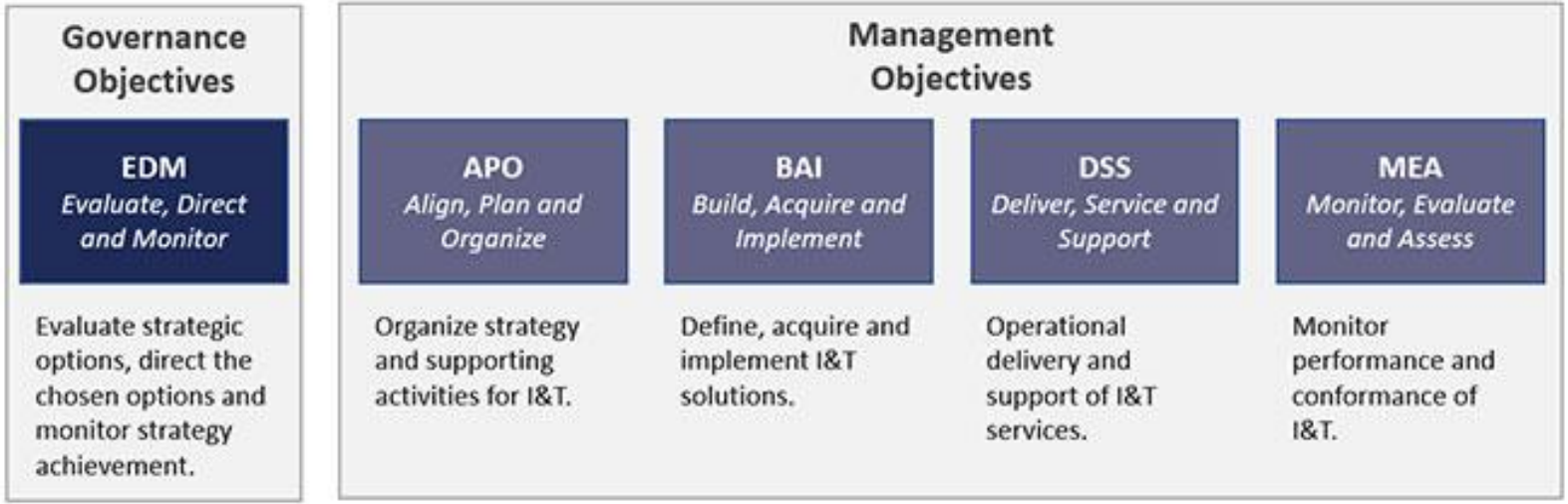
- The purpose of the Capability Maturity Model Integration (CMMI) model is to assess the maturity of an organization's processes and to provide guidance on improving processes, with the goal of improving products.
- CMMI is a successor of CMM and is a more evolved model that incorporates the best components of individual disciplines of CMM like Software CMM, Systems Engineering CMM, People CMM, etc. Since CMM is a reference model of matured practices in a specific discipline, so it becomes difficult to integrate these disciplines as per the requirements. This is why CMMI is used as it allows the integration of multiple disciplines as and when needed.
- Objectives of CMMI:
  - Fulfilling customer needs and expectations
  - Value creation for investors/stockholders
  - Market growth is increased
  - Improved quality of products & services
  - Enhanced reputation in Industry

COBIT 2019

- COBIT 2019 defines the components to build and sustain a governance system: policies and procedures, processes, organizational structures, culture and behaviors, infrastructure, information, and skills.
- COBIT 2019: The COBIT 2019 framework can help organizations of all types and sizes to improve and maintain high-quality information to support business decisions:
  - Use IT effectively to achieve business goals;
  - Use technology to promote operational excellence;
  - Ensure IT risk is managed effectively;
  - Ensure organizations realize the value of their investments in IT; and
  - Achieve compliance with laws, regulations, and contractual agreements.

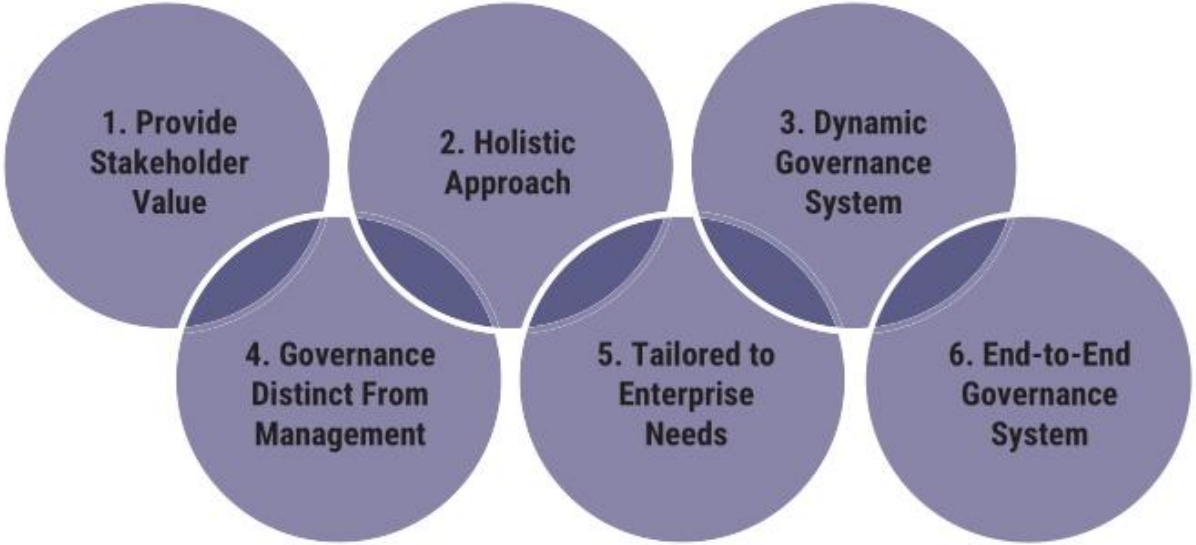
--

COBIT 2019 - DOMAINS

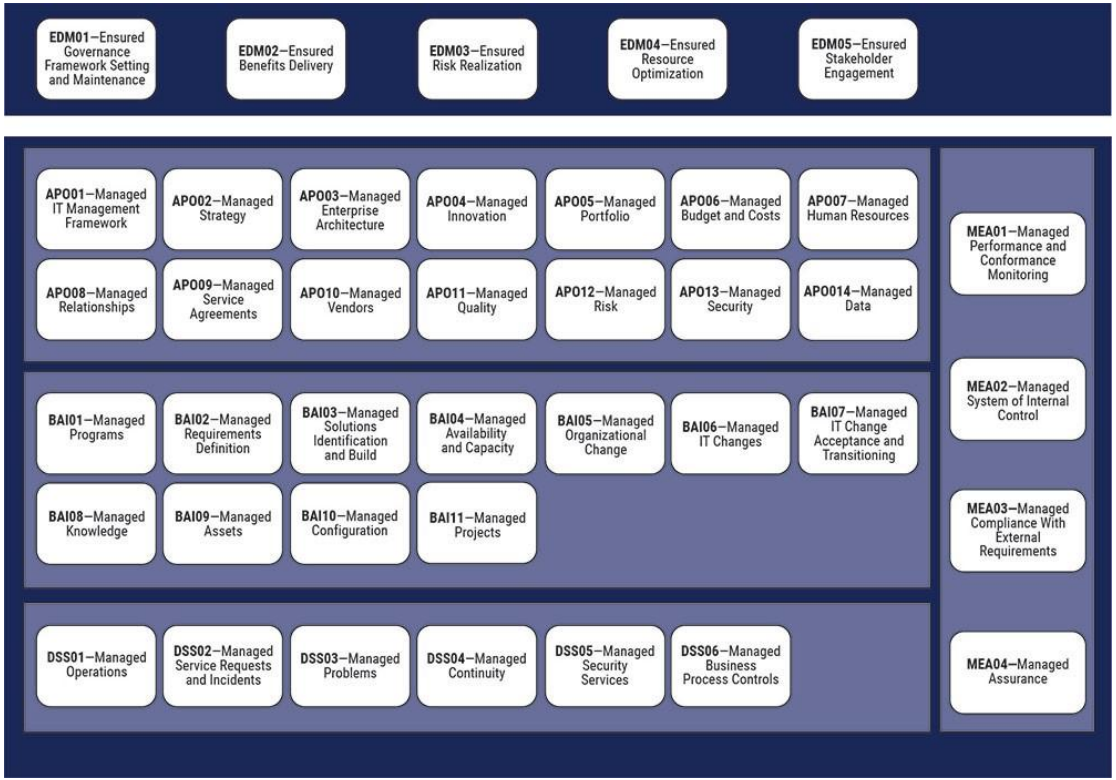


--

COBIT 2019 - PRINCIPLES



--



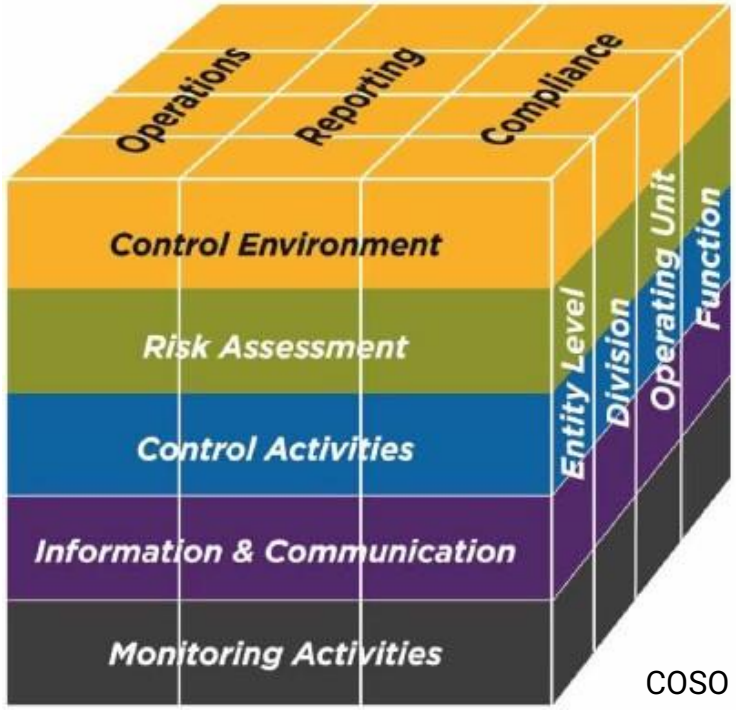
COBIT 2019 – DETAILED MODEL

ITAF

- The ITAF is a model that
  - defines terms and concepts relating to IT assurance
  - gives guidance on the design, process, and communication of IT audit and assurance assignments
  - creates standards to address requirements such as Audit roles and responsibilities, knowledge and skills identification, and
  - Provides guidance for audit conduct, diligence, and reporting

- Additionally, this framework includes a set of standards that relate to the auditor's professional characteristics. As an auditor, you are provided with a clear definition of your roles and responsibilities in auditing and assurance tasks, as well as the knowledge and skills required to carry out the tasks.
  - ITAF 1000 Series – General Standards
  - ITAF 1200 Series – Performance Standards
  - ITAF 1400 Series – Reporting Standards

COSO



COSO Cube

The COSO cube has 3 dimensions. The first dimension depicts internal controls and the 5 interrelated components. The second dimension depicts control objectives and the third dimension provides controls at different levels of the enterprise. The titles of the 17 internal control principles organized by the five internal control component

HIPAA / DISHA "Digital Information Security in Healthcare Act 2018”

- It modernized the flow of healthcare information, stipulates how personally identifiable information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and addressed some limitations on healthcare insurance coverage. It generally prohibits healthcare providers and healthcare businesses, called covered entities, from disclosing protected information to anyone other than a patient and the patient's authorized representatives without their consent. With limited exceptions, it does not restrict patients from receiving information about themselves. It does not prohibit patients from voluntarily sharing their health information however they choose, nor does it require confidentiality where a patient discloses medical information to family members, friends, or other individuals not a part of a covered entity. While HIPAA primarily applies to healthcare providers and health plans in the US, DISHA could potentially encompass a wider range of entities handling digital health data.
- It consists of following key things:
  - Prohibition of Data Sharing Without Consent
  - Roles of the National and State Authorities [National Digital Health Authority (NDHA)]
  - Rights of Individuals
  - Data Protection and Privacy
  - Penalties for Non-Compliance

INFORMATION TECHNOLOGY ACT 2000

- Purpose
- Some important sections

ISO 27001

- ISO 27001 consists of 14 Domains [Controls] aligning IT Goals with Business Goals or [Establish the Desire to Change]
- By implementing this organizations will be able to secure information in all forms, increase resilience to cyber attacks, adapt to evolving security threats, and reduces the costs associated with information security.

SOME MORE ISO STANDARDS

- ISO 38500

ISO 38500 is the ISO standard for Corporate Governance of IT. The standard is focused at a high level and states that the board of directors should govern IT by:

  - **Evaluating** the current and future use of IT.
  - **Directing** preparation and implementation of plans and policies to ensure that the use of IT meets business objectives.
  - **Monitoring** conformance to policies and performance against the plans.

- ISO 31000

ISO has developed a new standard for IT Risk Management.

- ISO 22301

Specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.

- ISO 12207

SDLC Standard.

ITAF

- The ITAF is a model that
  - defines terms and concepts relating to IT assurance
  - gives guidance on the design, process, and communication of IT audit and assurance assignments
  - creates standards to address requirements such as Audit roles and responsibilities, knowledge and skills identification, and
  - Provides guidance for audit conduct, diligence, and reporting

- Additionally, this framework includes a set of standards that relate to the auditor's professional characteristics. As an auditor, you are provided with a clear definition of your roles and responsibilities in auditing and assurance tasks, as well as the knowledge and skills required to carry out the tasks.
  - ITAF 1000 Series – General Standards
  - ITAF 1200 Series – Performance Standards
  - ITAF 1400 Series – Reporting Standards

Two-thirds of the Earth is covered with Water and the rest one-third is covered with Auditors from different verticals evaluating the business operations from different angles.

- Dr. Saurabh Maheshwari

THANKS!

Any questions?