Compliance & Security Framework

(Chapter -2 : DISSA Course)

Arijit Chakraborty

Jan 22, 2022

IS & CSF - Focus Areas

- Application Reviews
- Security Reviews
- IS department Operations review
- Technology Reviews (firewall audit, email audit)
- Corporate and Department Training
- Operational Support through Audit Software
- Transaction Trails in digital form
- Guarding against Newest Malware Threats - Example. Spyware

IT Control Frameworks

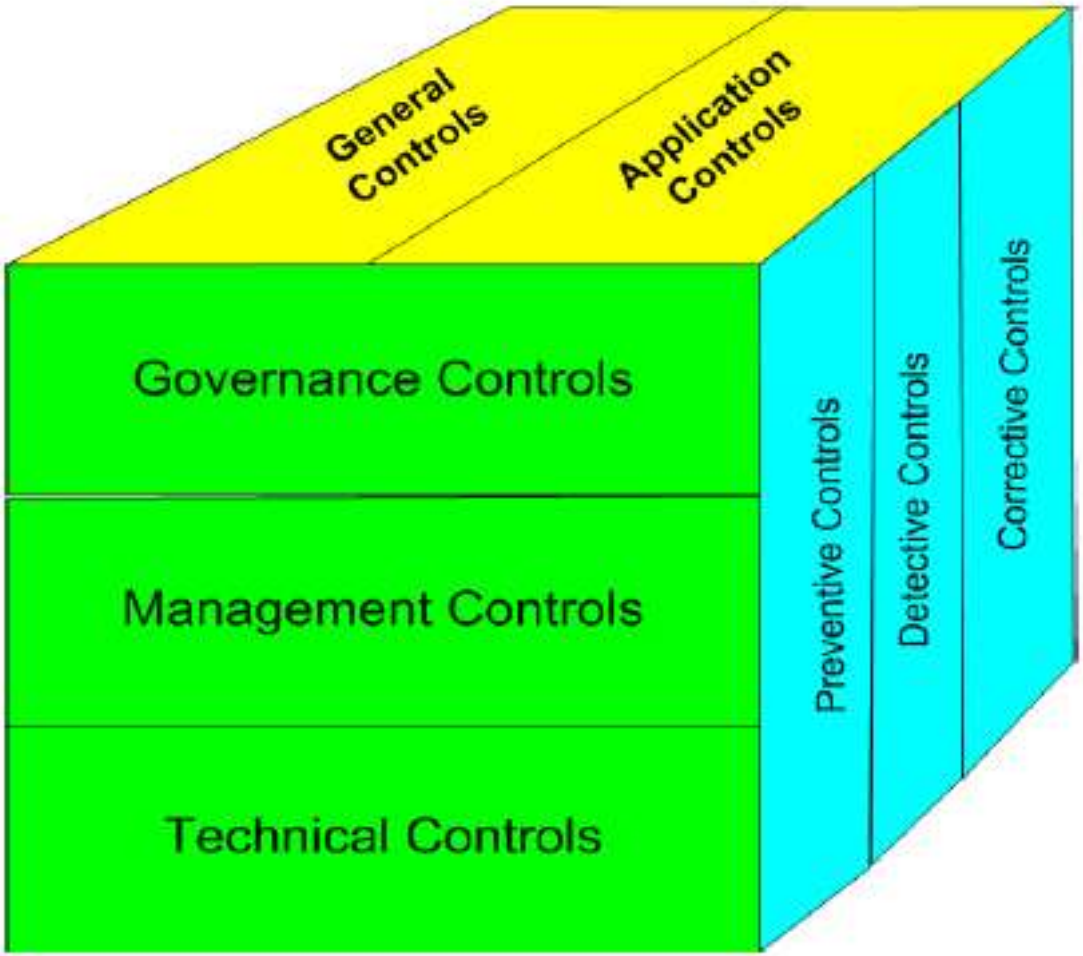
COSO

– Consists of 5 interrelated components =derived from the way management runs business:

1. **Control Environment** - Tone from the top, policies, governance committees, IT architecture
2. **Risk Assessment** - Incorporate IT into risk assessment, identify IT controls
3. **Control Activities** - Review board for change management, approval of IT plans, technology standards compliance enforcement
4. **Information and Communication** - Communication of best practices, IT performance surveys, training, IT help desk
5. **Monitoring**- Review of IT performance metrics, periodic management assessments, internal audit reviews

IT Controls Review

- Classification
  - General Controls
  - Application Controls
- Classification
  - Preventative
  - Detective
  - Corrective
- Classification
  - Governance controls
  - Management controls
  - Technical controls



Source: IIA GTAG-1

COBIT- Introduction

- COBIT (Control Objectives for Information and Related Technology) = globally accepted = most comprehensive work for IT governance, organization, & IT process and risk management

- COBIT = good practices for management of IT processes in a manageable and logical structure, meeting multiple needs of enterprise management by **bridging gaps between business risks, technical issues, control needs and performance measurement requirements.**

- The COBIT mission = research, develop, publicize and promote an authoritative, up-to-date, international set of generally accepted IT control objectives for day-to-day use by business managers and auditors.

- COBIT 2019 Framework

CobiT

- Designed to be used by auditors , business process owners
- Uses a set of 34 high-level control objectives grouped into 4 domains:
  - Plan and Organize
  - Acquire and Implement
  - Deliver and Support
  - Monitor and Evaluate

COBIT History

- Technical Standards
  - ISO
- Codes of Conduct
  - Council of Europe, ISACA, OECD
- Qualification Criteria for IT Systems and Processes
  - ITSEC, ISO 9000, Common Criteria
- Professional Standards
  - COSO, IFAC, AICPA, CICA, ISACA, IIA, GAO
- Industry Practices and Requirements
  - Industry forums, Government-sponsored platforms (NIST, BS7799)

COBIT’s core components

- ✓ Control objectives
- ✓ Frameworks
- ✓ Management guidelines
- ✓ Maturity models
- ✓ Process descriptions
- **COBIT’s framework embraces these principles:**

❖ Applying a single integrated framework to the organization

❖ Enabling a holistic approach

❖ End-to-end coverage of the enterprise

❖ Meeting stakeholder needs

❖ Separating governance from management

Intro to ISO 27001

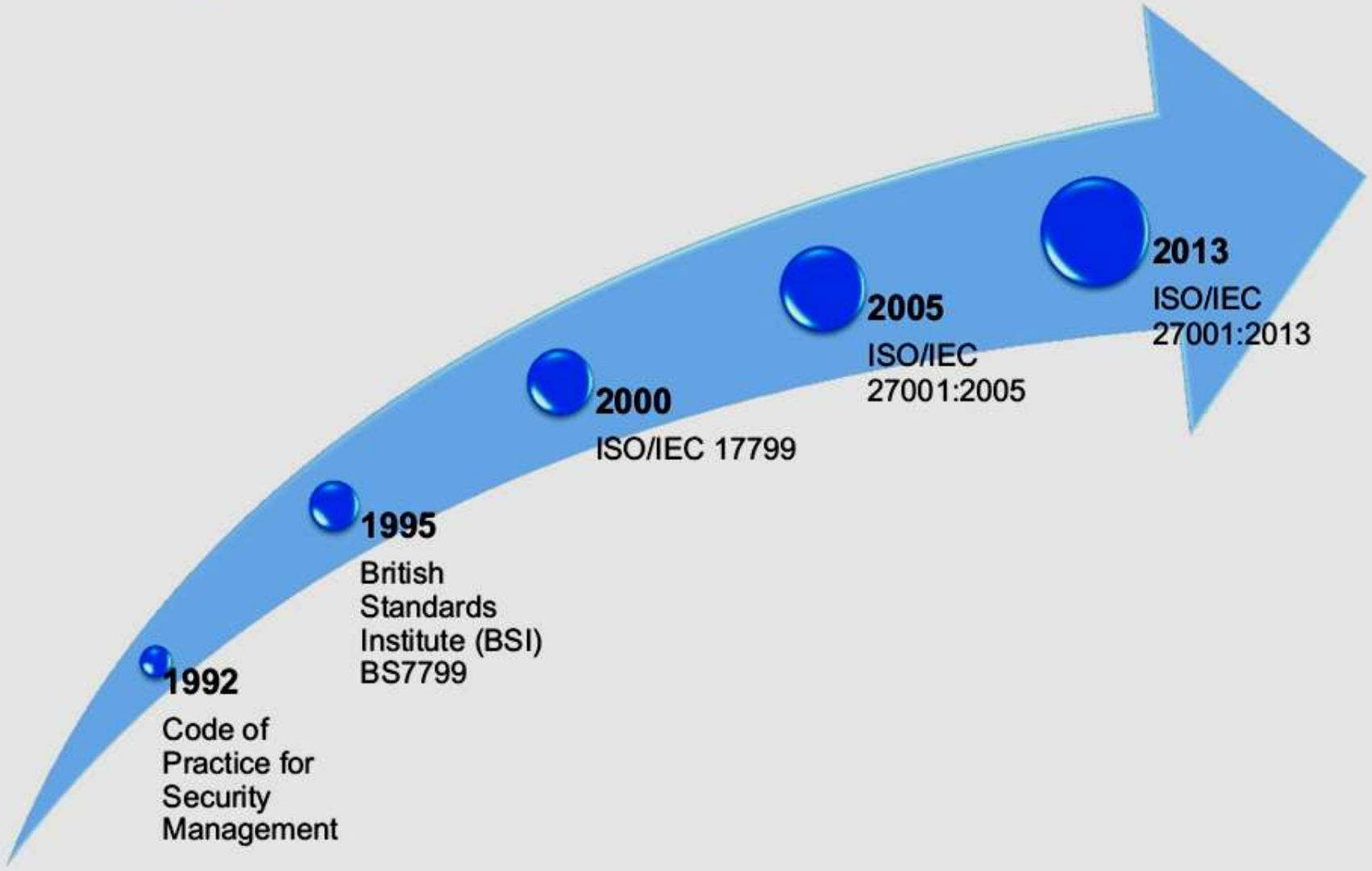
- **ISO 27001 = international standard = describes best practice for an ISMS (information security management system).**
- ISMS = **framework of policies & procedures** that includes all **legal, physical & technical controls** involved in an organization's **IS risk management processes.**
- Being ISO 270001 approved is a certification which shows that business **has defined and implemented effective IS** processes.
- ISO 27001 (formally known as ISO/IEC 27001:2005)

Purpose & importance

The goal of ISO 27001

- to provide a **framework of standards for how a modern organization should manage their information and data.**
- Risk management is a key part of ISO 27001
- ***Benefits include:***
- Increased reliability and security of systems and information.
- Improved customer and business partner confidence.

History of ISO/IEC 27001



Needs of ISO 27001

- ***Comply with Legal Requirements***
- ***Achieve Competitive Edge***
- ***Lower Cost***
- ***Better Organization***

IMPLEMENTATION PROCESS

- Step 1: Assemble an implementation team
- Step2: Develop the implementation plan
- Step 3: Initiate the ISMS
- Step 4: Define the ISMS scope
- Step 5: Identify your security baseline
- Step 6: Establish a risk management process
- Step 7: Implement a risk treatment plan
- Step 8: Measure, monitor and review
- Step 9: Certify your ISMS

ISO27001 Internal Audit Process

- **A. Document review.** read all the documentation of ISMS/BCMS to audit in order to:
- (1) become acquainted with the processes in the ISMS, and
- (2) to find out if there are nonconformities in the documentation with regard to **ISO 27001** or **ISO 22301**.
- **B. Creating the checklist.**
- **C. Planning the main audit.** should plan which departments and/or locations to visit and when – checklist will give an idea on where to focus the most.
- **D. Performing the main audit.** -have to walk around the company and talk to employees, check computers and other equipment, observe physical security, etc.
- A checklist is crucial in this process.

- **E. Reporting.** After completion of main audit, have to summarize all nonconformities, draft Internal audit report with checklist & detailed notes to write a precise report.
- Based on this report, have to open corrective actions according to Corrective action procedure.
- **F. Follow-up.** Internal auditor to check whether all corrective actions raised during internal audit are closed