Hussam Khattab

MBA, CISA, CGEIT, PMP, COBIT2019

President, ISACA Amman Chapter

Internal Audit

"Internal Auditing is an independent, objective assurance and consulting activity designed to **add value and improve an organization's operations**. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes"

Internal Audit

- Promotes organizational improvement
- Provides risk-based assurance
- Aligns with the strategies, objectives and risks of the organization
- Proactive and future-focused
- Communicates effectively

In middle of cybersecurity incidents and risks,

Where Should Internal Audit Stand?

Starts from the Top:

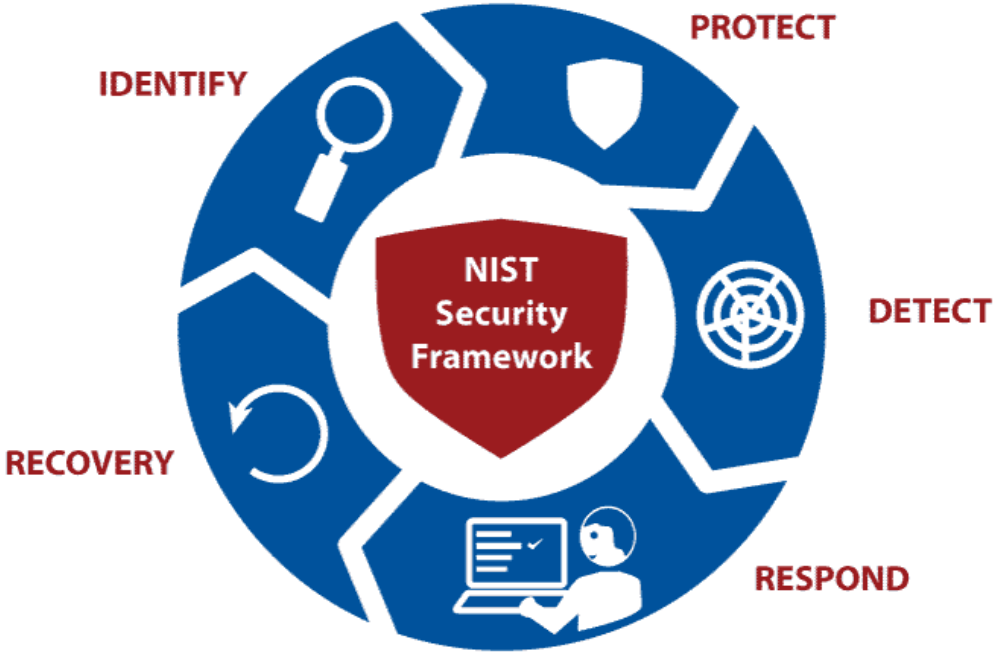
- Have a cybersecurity expertise on the Board
- Make cybersecurity a constant Board agenda item
- Define & establish a cybersecurity roadmap
- Regularly review cybersecurity strategies for effectiveness
- Monitor & evaluate

Internal Audit

- Understand the business crown jewels – Key processes and products.
- Understand the underlying IT environment.
- Assess the current risks.
- Identify threats and vulnerabilities

Key Questions:

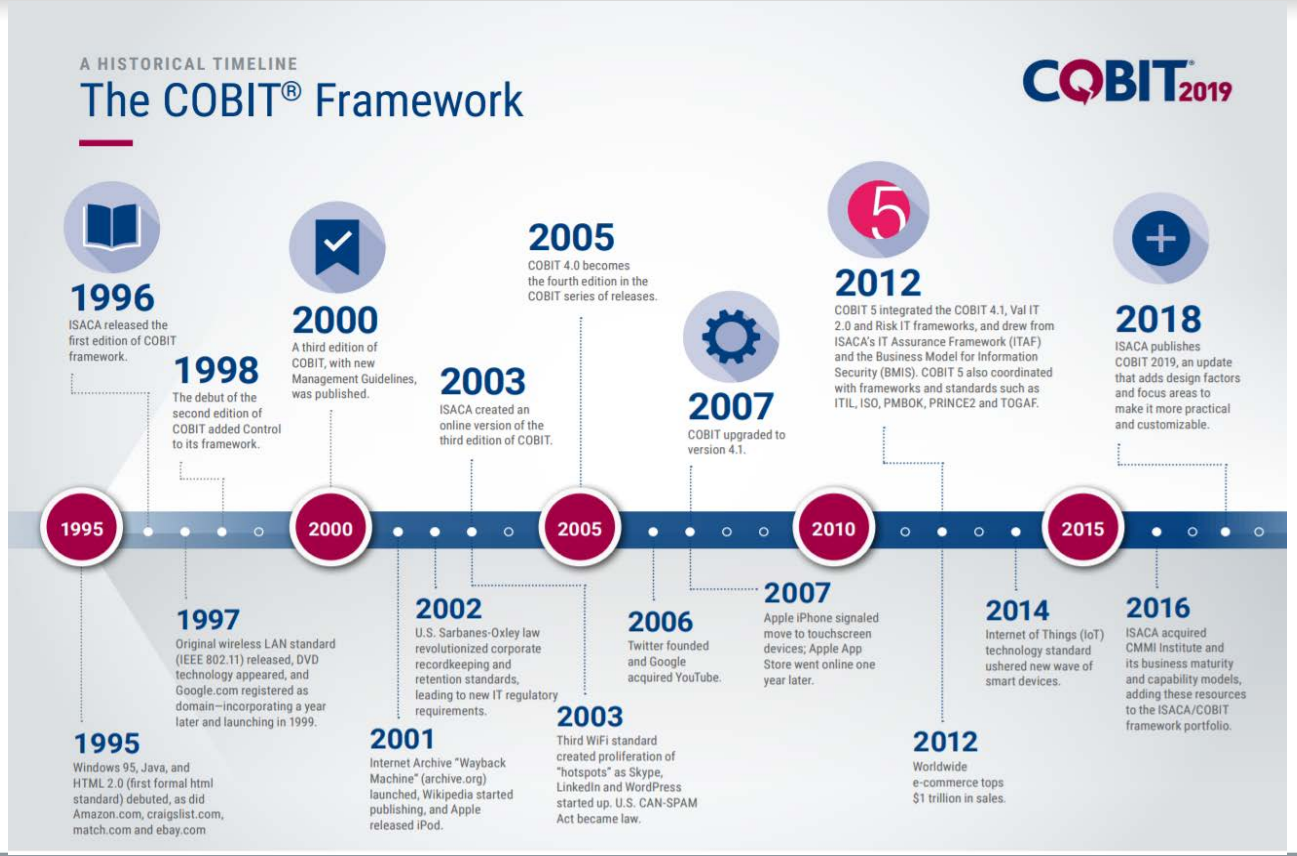
- Is cybersecurity on the current, previous and future audit plans?
- How frequently do we audit cybersecurity?
- Does Internal Audit have cybersecurity audit skills?
- Are cybersecurity issues communicated in business language?


PROTECT
IDENTIFY
NIST
Security
Framework
DETECT
RECOVERY
RESPOND

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

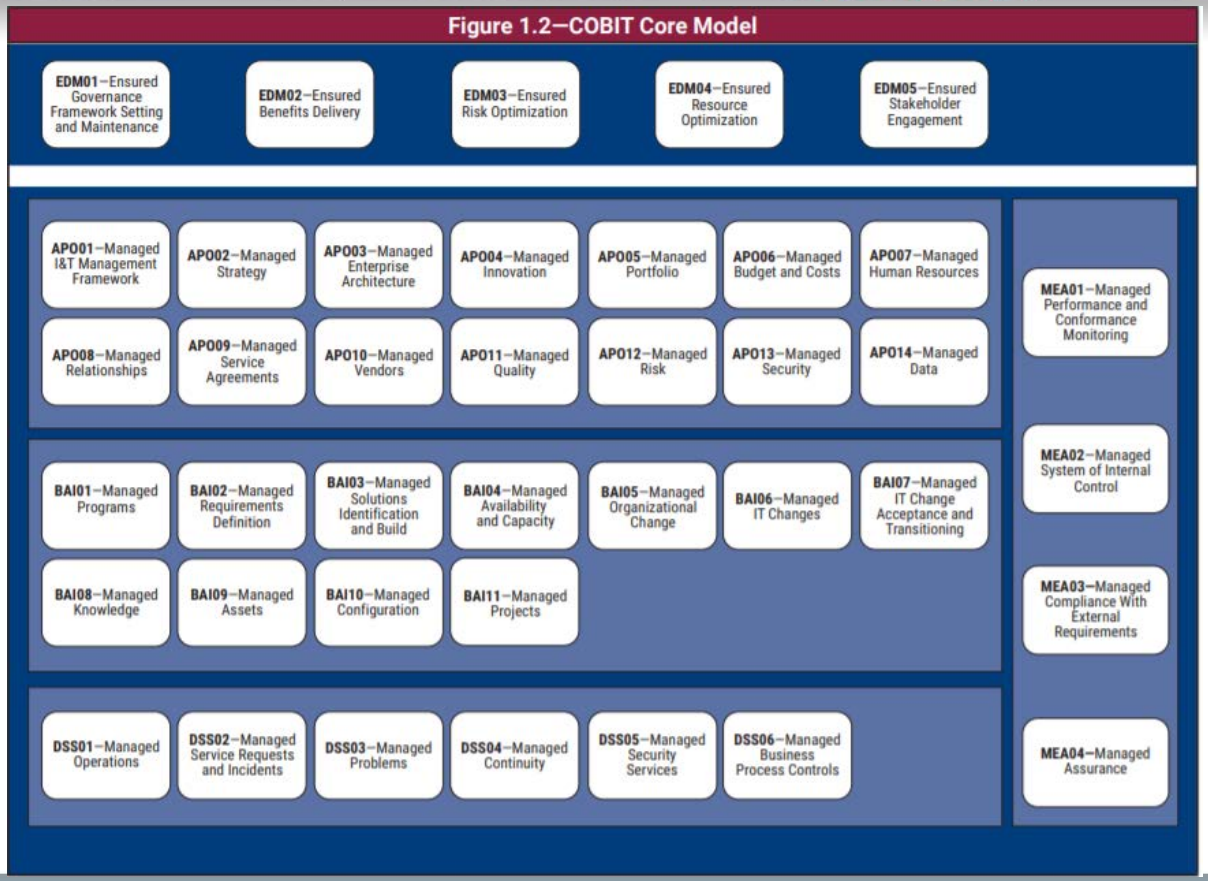
Reference:
NIST Cybersecurity V1.1

COBIT® 2019



Reference:
www.isaca.org

Figure 1.2—COBIT Core Model



Governance Objectives

Management Objectives

EVALUATE, DIRECT & MONITOR (EDM)

- **EDM01** Ensured Governance Framework Setting and Maintenance
- **EDM02** Ensured Benefits Delivery
- **EDM03** Ensured Risk Optimization
- **EDM04** Ensured Resource Optimization
- **EDM05** Ensure Stakeholder Engagement

ALIGN, PLAN & ORGANIZE (APO)

- **APO01** Managed I&T Framework
- **APO02** Managed Strategy
- **APO03** Managed Enterprise Architecture
- **APO04** Managed Innovation
- **APO05** Managed Portfolio
- **APO06** Managed Budget & Costs
- **APO07** Managed Human Resources
- **APO08** Managed Relationships
- **APO09** Managed Service Agreements
- **APO10** Managed Vendors
- **APO11** Managed Quality
- **APO12** Managed Risk
- **APO13** Managed Security
- **APO14** Managed Data

BUILD, ACQUIRE & IMPLEMENT (BAI)

- **BAI01** Managed Programs
- **BAI02** Managed Requirements Definition
- **BAI03** Managed Solutions Identification and Build
- **BAI04** Managed Availability and Capacity
- **BAI05** Managed Organizational Change
- **BAI06** Manage IT Changes
- **BAI07** Manage IT Change Acceptance and Transitioning
- **BAI08** Managed Knowledge
- **BAI09** Managed Assets
- **BAI10** Managed Configuration
- **BAI11** Managed Projects

DELIVER, SERVICE & SUPPORT (DSS)

- **DSS01** Managed Operations
- **DSS02** Managed Service Requests & Incidents
- **DSS03** Managed Problems
- **DSS04** Managed Continuity
- **DSS05** Managed Security Services
- **DSS06** Managed Business Process Controls

MONITOR, EVALUATE & ASSESS (MEA)

- **MEA01** Managed Performance and Conformance Monitoring
- **MEA02** Managed System of Internal Control
- **MEA03** Managed Compliance with External Requirements
- **MEA04** Managed Assurance

Reference: COBIT 2019 Framework: Governance and Management Objectives, Chapter 1 Introduction

Areas to Assess:

- Penetration testing & vulnerability assessment; frequency, remediation & reporting
- Effectiveness of patch management procedures
- Review for critical security systems configurations
- Review for end points controls
- Training & awareness program

Areas to Assess:

- Access controls; logical & physical
- Third party management
- Detection capabilities
- Business Continuity planning & disaster recovery
- Data backup arrangements
- Incident Response planning

"Internal Auditors are Partners of Management"


CYBER SECURITY AND RESILIENCE SYMPOSIUM
TOWARDS A RESILIENT AVIATION CYBERSPACE
AMMAN, JORDAN | 15-17 OCTOBER 2019
ICAO
Thank You