جامعة الحسين التقنية
Al Hussein Technical University

Information Security Management

J/618/7447
10203300

جامعة الحسين التقنية
Al Hussein Technical University

Topic 3: INFORMATION SECURITY FRAMWORKS

Eman Alzyoud
School of Computing and Informatics
Eman.Alzyoud@HTU.EDU.JO

جامعة الحسين التقنية
Al Hussein Technical University

Learning Objectives:

- Information security policy, standards and procedures
- including privacy policy, acceptable use , separation of duties , least privilege and the role of a company’s internal policies, including service level agreements (SLAs) with providers.
- Organisations and responsibilities
- Managing compliance and stakeholders.
- Information security frameworks
- IT governance
- Information assurance programme implementation

جامعة الحسين التقنية
Al Hussein Technical University

Introduction

- Information security program begins with policies, standards, and practices, which are the foundation for information security architecture and blueprint.
- Coordinated planning is required to create and maintain these elements.
- Strategic planning for the management of allocation of resources.
- Contingency planning for the preparation of uncertain business environment

جامعة الحسين التقنية
Al Hussein Technical University

Security Management Plan

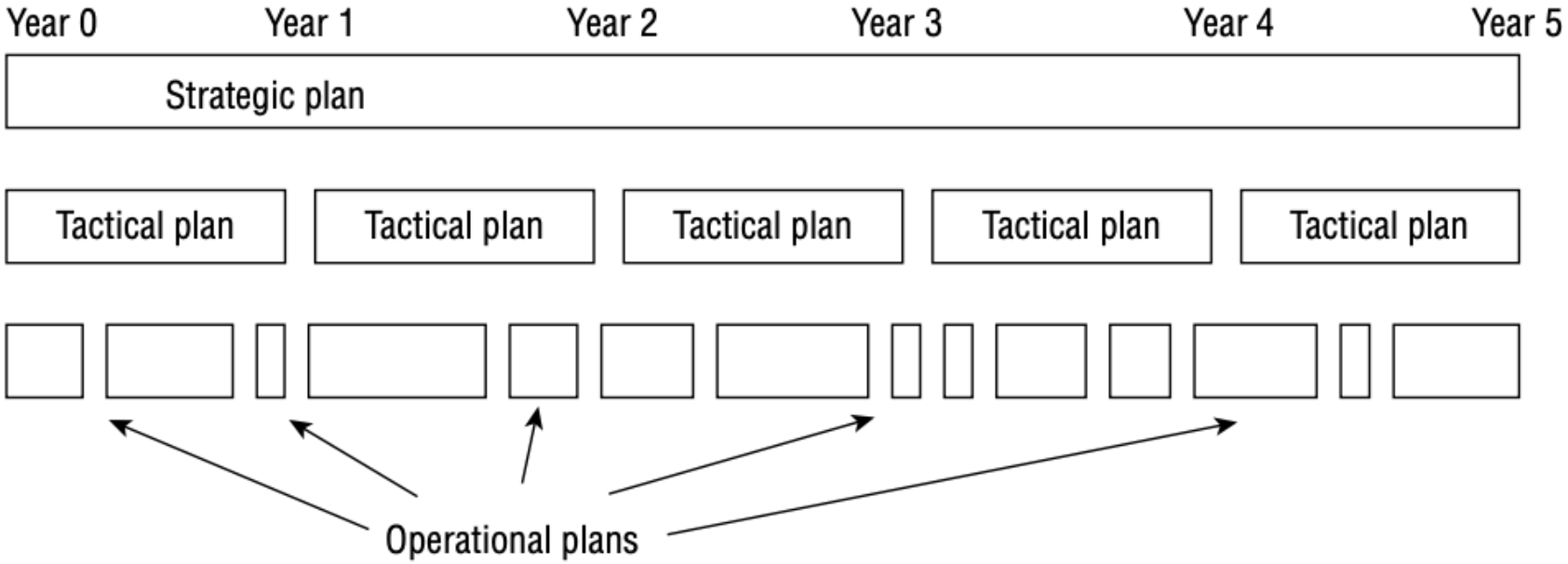
- SMP should use a top-down approach
  - Senior management is responsible for initiating and defining policies;
  - Middle management is responsible for releasing standards, baselines, guidelines in relation to the policy
  - Operations management/IT teams implement the controls defined above
  - End-users must comply with all the functions of the organization

جامعة الحسين التقنية
Al Hussein Technical University

Security Management Plan Types

SMP Type	Description
Strategic Plan	Long term plan Defines the organization's security posture Useful for at least 5 years. Reviewed annually Helps understand security function and align it with business Should include Risk Assessment
Tactical Plan	Mid-term plan developed to provide more detailed goal Usually for an year or two More technology oriented Eg: Project plans, acquisition plan, budget plan, hiring plan
Operational Plan	Short-term plan Highly-detailed plan Must be updated often (monthly, quarterly) Spell-out how to accomplish various goals Eg: resource allotment, budgetary allocation, training plans

Strategic, tactical, and operational plan timeline comparison



جامعة الحسين التقنية
Al Hussein Technical University

Security Roles and Responsibility

Senior Management	• Ultimately responsible for security • Must signoff all policy issues • All activities must be approved • Will be held responsible for overall security success/failure • Responsible for due care and due diligence
Security Professional	• Responsible for following the directives mandated by SM • Has the functional responsibility for security • They are not decision makers
Data Owner	• Responsible for classifying information • Ultimately responsible for the data they own • Typically high level management representative
Data Custodian	• Responsible for tasks of implementing the prescribed protection defined by Data owner • Responsibilities include, preforming/testing backups, validating data integrity, deploying security solutions and managing data storage based on classification
User	• Has access to the secure system • Responsible for understanding and upholding the security policy
Auditor	• Responsible for reviewing and verifying the security policy implementation • Produces compliance and effectiveness reports

جامعة الحسين التقنية
Al Hussein Technical University

Due Care and Due Diligence

Showing due diligence and due care is the only way to disprove negligence in an occurrence of loss. Senior management must show due care and due diligence to reduce their culpability and liability when a loss occurs.

Due Care

- Is practicing the individual activities that maintain the due diligence effort
- Is doing the right action at the right time.
- Taking reasonable care in protecting the organization

Due Diligence

- Is establishing a plan, policy, and process to protect the interests of an organization
- Is knowing what should be done and planning for it .

For example, due diligence is developing a formalized security structure containing a security policy, standards, baselines, guidelines, and procedures. Due care is the continued application of this security structure onto the IT infrastructure of an organization.

جامعة الحسين التقنية
Al Hussein Technical University

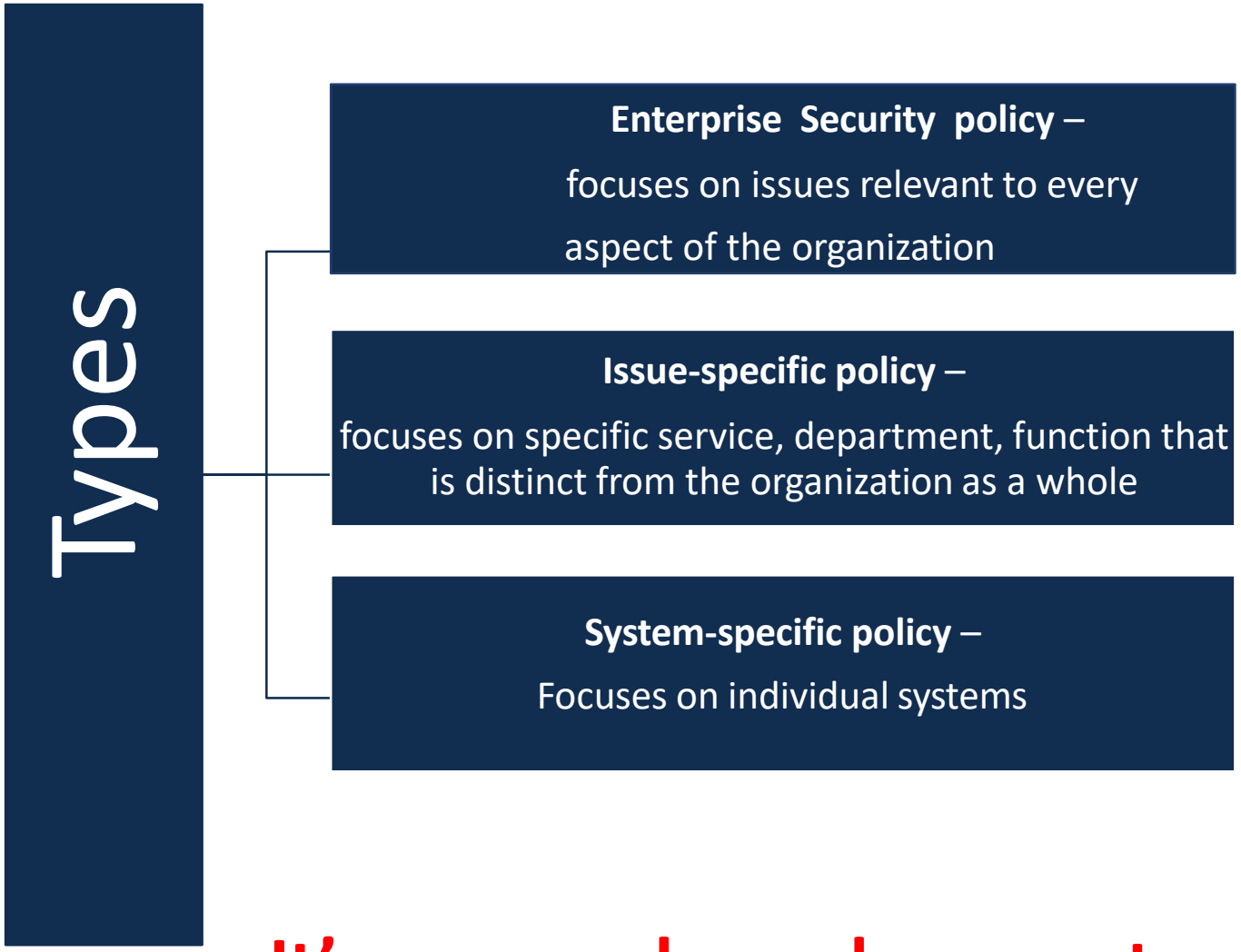
Information Security Policy, Standards, and Practices

- Management from communities of interest must make policies the basis for all information security planning, design, and deployment.
- Policies direct how issues should be addressed and technologies used.
- Policies should never contradict law, must be able to stand up in court, and must be properly administered.
- Security policies are the least expensive controls to execute but most difficult to implement properly.

جامعة الحسين التقنية
Al Hussein Technical University

Security Policy

- Strategic plan for implementing security
- Defines the scope of security needed for the organization
- Defines the main security objectives and outlines the security framework
- Identifies major functional areas of data processing
- Broadly outlines the security goals and practices that should be employed
- Its is used to assign responsibilities, define roles, specify audit requirements, outline enforcement process, indicate compliance requirements, and define acceptable risk levels



It’s a compulsory document

جامعة الحسين التقنية
Al Hussein Technical University

Security Categories

Regulatory	Advisory	Informative
• Required whenever industry or legal standards are applicable to your organization	• Discusses behaviors and activities are acceptable and defines consequences of violation	• Designed to provide information or knowledge about a specific subject • Not enforceable

جامعة الحسين التقنية
Al Hussein Technical University

Standard/Baseline/Guideline/Procedure

Standard

- Define compulsory requirements
- Provides a course of action for uniform deployment of technology
- Tactical documents

Baseline

- Defines minimum level of security that every system must meet
- System-specific
- Establishes common secure state

Guideline

- Offers recommendations on implementation
- Servers as an operating guide
- Flexible – can be customized for each unique system

Procedure

- Final element of the formalized security policy structure
- Detailed step-by-step document describes actions necessary to implement security mandates
- System and software specific
- Purpose is to ensure integrity of business process

جامعة الحسين التقنية
Al Hussein Technical University

Acceptable Use Policy

An acceptable use policy (AUP) is a commonly produced document that exists as part of the overall security documentation infrastructure . This policy defines a level of acceptable performance and expectation of behavior and activity. Failure to comply with the policy may result in job action warnings, penalties, or termination.

جامعة الحسين التقنية
Al Hussein Technical University

The Information Security Framework

- Basis for design, selection, and implementation of all security policies, education and training programs, and technological controls.
- Detailed version of security framework (outline of overall information security strategy for organization).
- Specifies tasks and order in which they are to be accomplished.
- Should also serve as a scalable, upgradeable, and comprehensive plan for the current and future information security needs

جامعة الحسين التقنية
Al Hussein Technical University

Definitions

Framework

Provide guidance on how to build Individual architectures that will be useful to a diverse set of individuals

Architecture

- Tool to help individuals understand complex items
- Conceptual Construct
- It expresses enterprise structure (form) and behaviour (function)

Security Program

- It is a framework made of many entities working together to provide a protection level for an environment
- A security program should work in layers
- Security via obscurity is not a healthy protective mechanism

جامعة الحسين التقنية
Al Hussein Technical University

Enterprise Architecture

- Two important key aspects of an Enterprise Architecture

➢ **Identifying the stakeholders**

- people who will be looking at it and using it

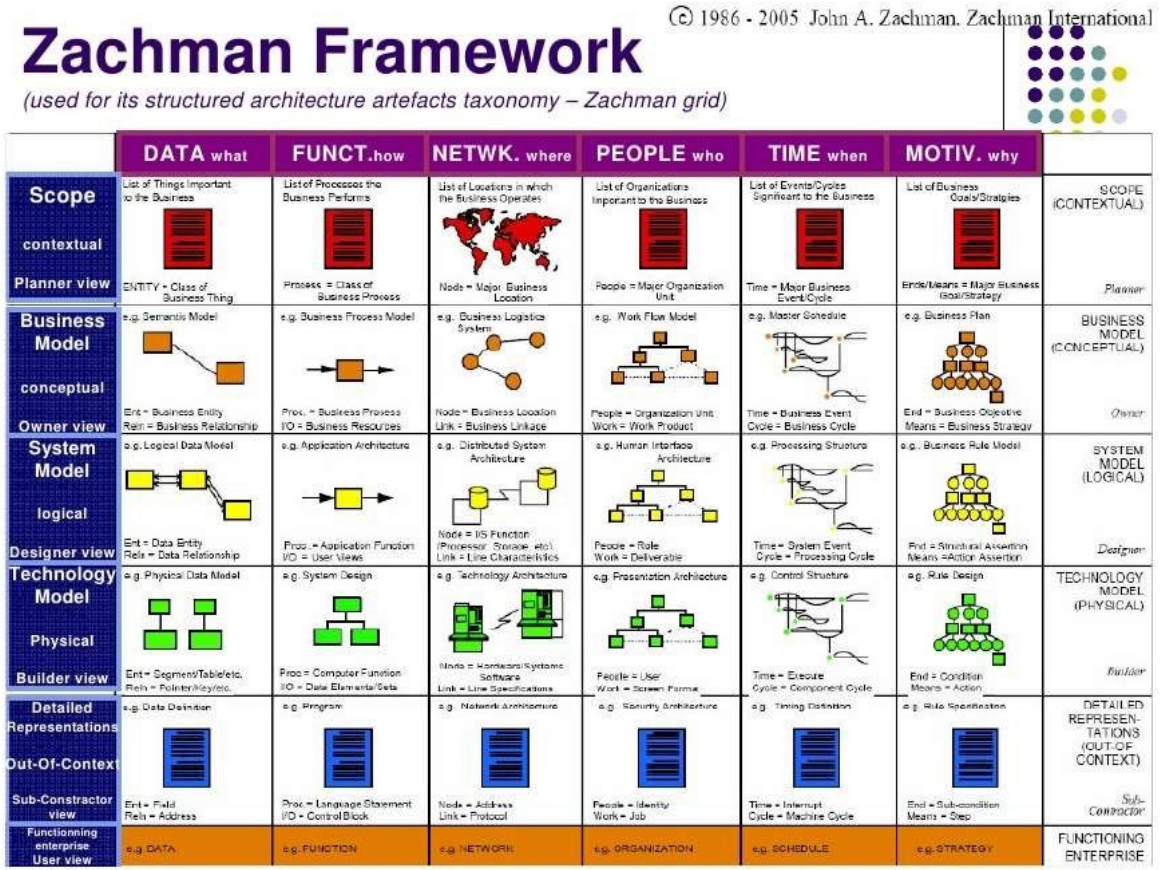
➢ **Developing Views**

- How the information that is most important to different stakeholders will be illustrated in the most useful manner
- Architecture allows not only to understand the business from different views, but also understand how a change takes place at one level will affect items at all other levels

جامعة الحسين التقنية
Al Hussein Technical University

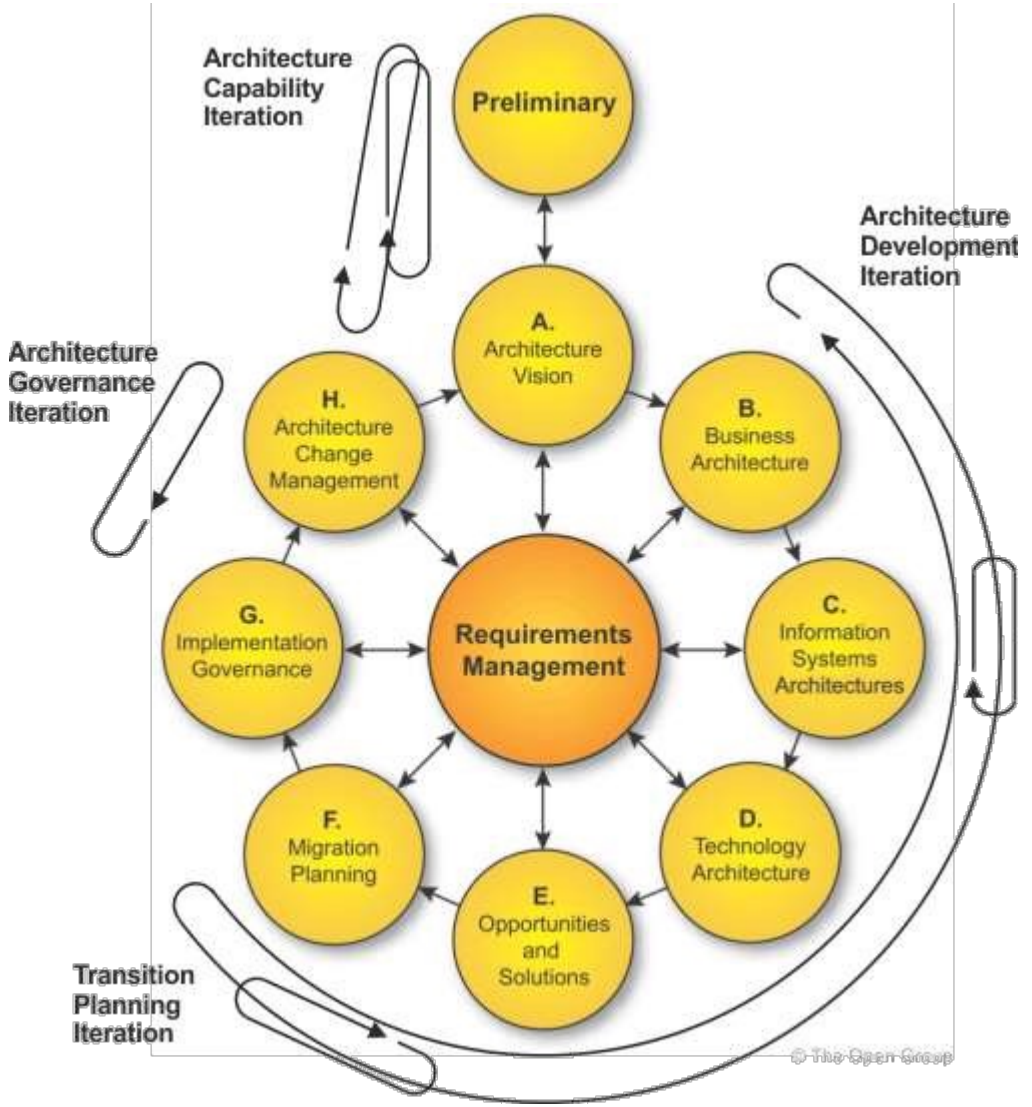
Zachman Architecture Framework

- First architecture Framework
- This is not a security oriented framework
- The Zachman framework is not a methodology, but it is a structure.
- It is a two-dimensional framework that combines six basic interrogatives (What, How, Where, Who, When, and Why).
- The framework intersects with different perspectives: Executives, Business Managers, System Architects, Engineers, and Technicians.
- It enables holistic understanding of the enterprise by looking at the organization from various viewpoints.



The Open Group Architecture (TOGAF)

- Has its origins from US DoD
- Provides an approach to design, implement, and govern an enterprise Information architecture
- Used to develop the following architecture types:
  - Business Architecture
  - Data Architecture
  - Applications Architecture
  - Technology Architecture
- Uses Architecture Development Method to create Individual architectures
- ADM is an iterative and cyclic process that allows requirements to be continuously reviewed and updated



جامعة الحسين التقنية
Al Hussein Technical University

Enterprise Security Architecture

- Subset of Enterprise Architecture
- Defines information security strategy that consists of layers of solutions, process, and procedures
- It ensures that security efforts align with business practices in a standardized and cost-effective manner
- For a successful ESA the following must be understood and followed
  - Strategic alignment
  - Business enablement
  - Process enhancement
  - Security effectiveness

جامعة الحسين التقنية
Al Hussein Technical University

Strategic Alignment	Business Enablement	Process Enhancement	Security Effectiveness
• Business drivers and legal/regulatory requirements must be met by the Security architecture	• Core business processes are integrated into the security operating model	• Security enterprise components must be integrated into the business processes to be effective	• Metrics, meeting SLA, achieving ROI, meeting set baselines, providing management dashboards

We can do new stuff

We can do stuff better

جامعة الحسين التقنية
Al Hussein Technical University

ISO27000 Security Program

- Outlines how an information security management system should be built and maintained
- A lengthy list of standards for developing and maintaining an Information Security Management System (ISMS)

- Provides guidance to design, implement and maintain policies, procedures, and technologies to manage risks to the sensitive information assets of an organization

- International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) 27000 family group (www.itgovernanceusa.com/iso27000- family) is an international standard that can be the basis of implementing organizational security and related management practices.

- Some key ISO27000 standards
  - ISO27001 – ISMS requirements
  - ISO27002 – Code of practice for ISMS
  - ISO27005 – Risk Management
  - ISO27031 – Business continuity

جامعة الحسين التقنية
Al Hussein Technical University

- **ISO/IEC 27001:2022/Amd 1:2024 .Information security, cybersecurity and privacy protection ISMS**
  - **27000:2018—Published overview of ISMSs and vocabulary**
  - **27001:2013—Published ISMS requirements**
  - **27002:2013—Published code of practice for information security controls**
  - **27003:2017—Published guidance on the requirements for an ISMS**
  - **27004:2016—Published ISMS monitoring, measurement, analysis, and evaluation guidelines**
  - **27005:2011—Published information security risk management guidelines**
  - **27042:2015—Published digital evidence analysis and interpretation guidelines**
  - **27043:2015—Published incident investigation principles and processes**
  - **27050-1:2016—Published electronic discovery (eDiscovery) overview and concepts**
  - **27050-3:2017—Published code of practice for electronic discovery**
  - **27799:2016—Published information security in health organizations guidelines**

جامعة الحسين التقنية
Al Hussein Technical University

COBIT 2019

- Control Objectives for Information and Related Technology (COBIT).
- COBIT is a documented set of best IT security practices crafted by the Information Systems Audit and Control Association (ISACA).
- It prescribes goals and requirements for security controls and encourages the mapping of IT security ideals to business objectives.

- COBIT is based on six key principles for governance and management of enterprise IT:
  - Provide Stakeholder Value
  - Holistic Approach
  - Dynamic Governance System
  - Governance Distinct from Management
  - Tailored to Enterprise Needs
  - End-to-End Governance System

جامعة الحسين التقنية
Al Hussein Technical University

NIST

- **NIST 800-53 Rev. 5,** "Security and Privacy Controls for Information Systems and Organizations"

contains U.S. government–sourced general recommendations for organizational security.

- **NIST Risk Management Framework (RMF)**

establishes mandatory requirements for federal agencies. The RMF has six phases: Categorize, Select, Implement, Assess, Authorize, and Monitor.

- **NIST Cybersecurity Framework (CSF)** is designed for critical infrastructure and commercial organizations, and consists of five functions: Identify, Protect, Detect, Respond, and Recover. It is a prescription of operational activities that are to be performed on an ongoing basis for the support and improvement of security over time.

جامعة الحسين التقنية
Al Hussein Technical University

ITIL

- Information Technology Infrastructure Library (ITIL),initially crafted by the British government, is a set of recommended best practices for optimization of IT services to support business growth, transformation, and change.
- ITIL focuses on understanding how IT and security need to be integrated with and aligned to the objectives of an organization.
- Customizable framework.
- It provides the goals, the general activities necessary to achieve the goals, and the input/output values for each process required to meet the goals.
- It focuses more towards internal SLA between the IT department and the customer it serves (predominantly Internal functions)

جامعة الحسين التقنية
Al Hussein Technical University

Reference

- Alexander, D., Finch, A., Sutton, D. and Taylor, A. (2020) Information Security Management Principles BCS. 3rd edn. BCS The Chartered Institute for IT.

- Calder, A. and Watkins, S. (2019) IT Governance: An International Guide to Data Security and ISO27001/ISO27002. 7th edn. Kogan Page.

- Chapple, Mike - CISSP Official Study Guide (2021, Sybex). 9th edn.