PMICS, July 2025

CSE 807

Information Security Management

Instructor:
Md. Faisal Hossain

faisal.csedu@gmail.com
faisal.pmics@cse.du.ac.bd

Information & Cyber Security Management & Governance Frameworks

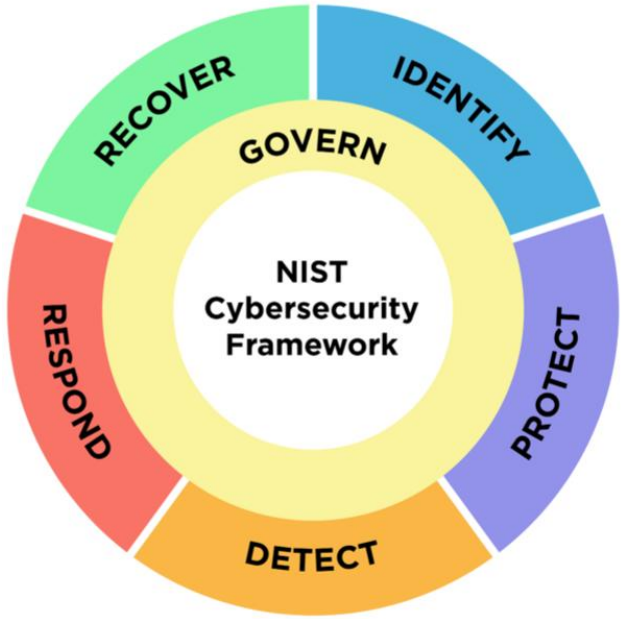
Disclaimer:

This material is designed & owned by the course instructor for the PMICS program of University of Dhaka. Use, copying, distributing, sharing, displaying, or reproducing the entire or any part of this material for any commercial purpose is strictly prohibited and illegal.

Discussed

- ✓ NIST Cyber Security Framework (CSF) 2.0
- ✓ NIST SP 800-37 (Rev 2) – Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- ✓ NIST SP 800-39 – Managing Information Security Risk: Organization, Mission, and Information System View
- ✓ NIST SP 800-53 (Rev 5) – Security and Privacy Controls for Information Systems and Organizations
- ✓ ISO/IEC 27001 – Information Security Management System
- ✓ ISO/IEC 31000
- ✓ COBIT 5

NIST Cyber Security Framework (CSF) 2.0



NIST CSF 2.0 – Overview

NIST CSF 2.0 – Overview (cont.)

1. **CSF Core**, the nucleus of the CSF, which is a taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks. The CSF Core components are a hierarchy of **Functions**, **Categories**, and **Subcategories** that detail each outcome. These outcomes can be understood by a broad audience, including executives, managers, and practitioners, regardless of their cybersecurity expertise. Because the outcomes are sector-, country-, and technology-neutral, they provide an organization with the flexibility needed to address its unique risks, technologies, and mission considerations.

2. **CSF Organizational Profiles**, which are a mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes.

3. **CSF Tiers**, which can be applied to CSF Organizational Profiles to characterize the rigor of an organization's cybersecurity risk governance and management practices. Tiers can also provide context for how an organization views cybersecurity risks and the processes in place to manage those risks.

NIST CSF 2.0 – Core

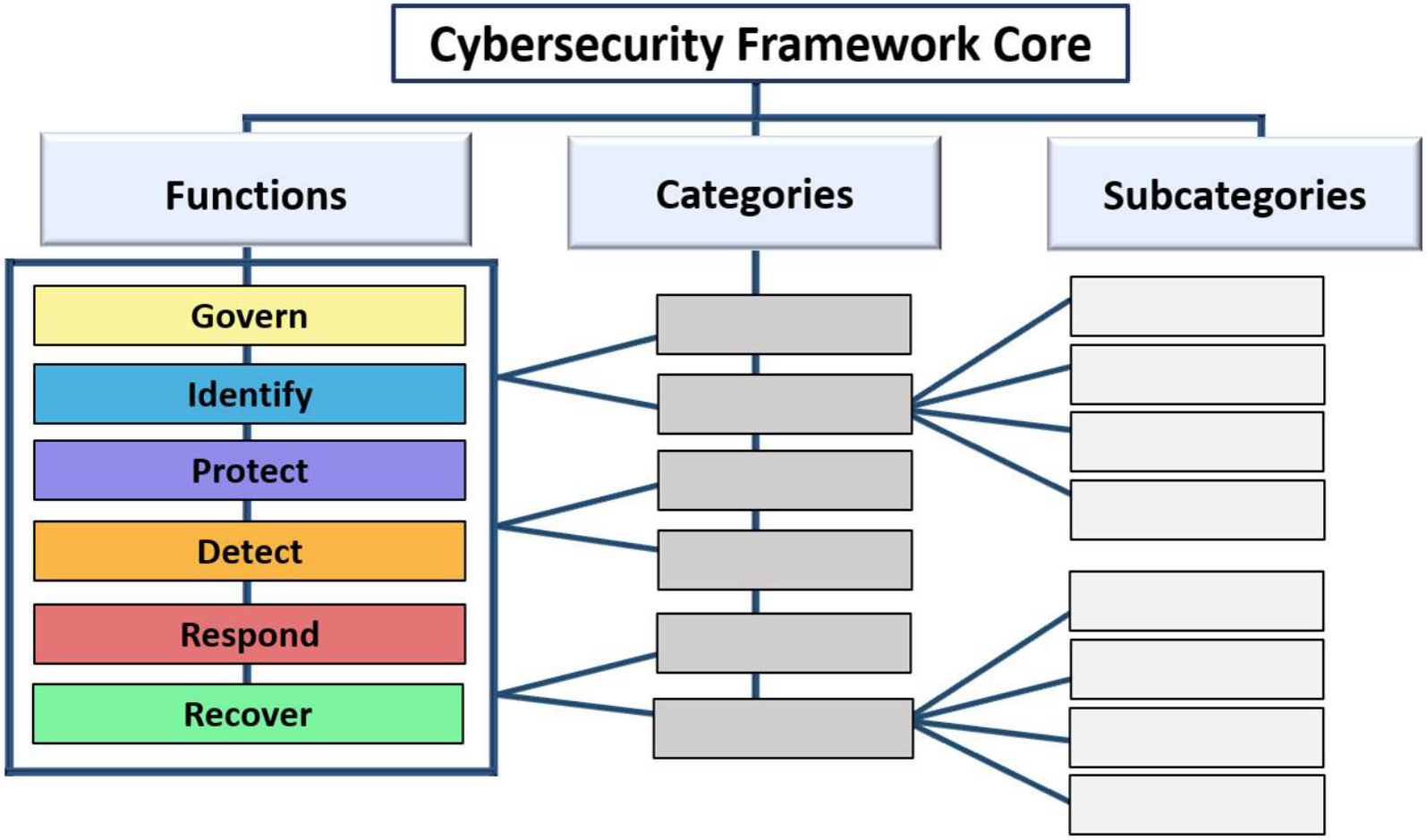


Fig: CSF Core Structure

NIST CSF 2.0 – Core (cont.)

Functions

The **Functions** should be addressed concurrently. Actions that support GOVERN, IDENTIFY, PROTECT, and DETECT should all happen continuously, and actions that support RESPOND and RECOVER should be ready at all times and happen when cybersecurity incidents occur. All Functions have vital roles related to cybersecurity incidents. GOVERN, IDENTIFY, and PROTECT outcomes help prevent and prepare for incidents, while GOVERN, DETECT, RESPOND, and RECOVER outcomes help discover and manage incidents. Each Function is named after a verb that summarizes its contents.

Categories

Each Function is divided into **Categories**, which are related cybersecurity outcomes that collectively comprise the Function.

NIST CSF 2.0 – Core (cont.)

Subcategories

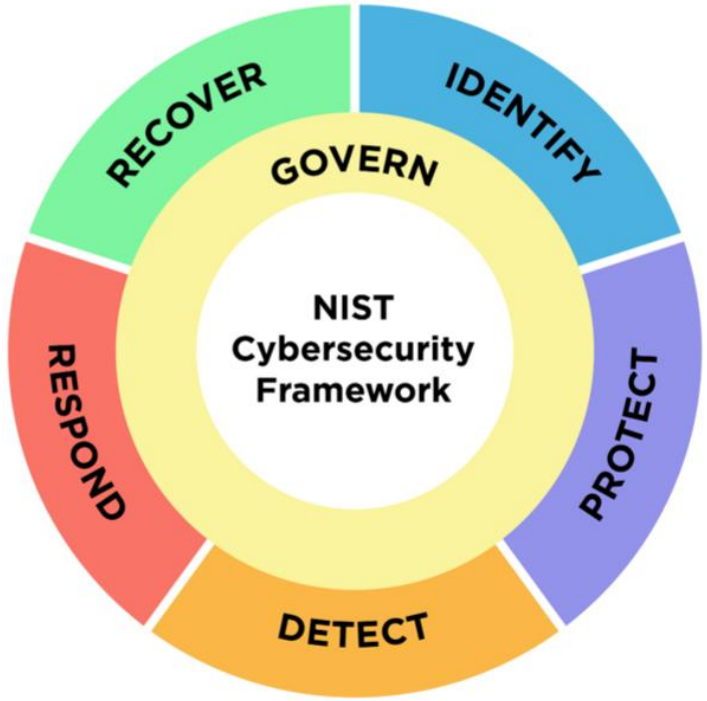
Subcategories further divide each Category into more specific outcomes of technical and management activities. The Subcategories are not exhaustive, but they describe detailed outcomes that support each Category.

Informative References

Informative References are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory. The Informative References presented in the Framework Core are illustrative and not exhaustive. They are based upon cross-sector guidance most frequently referenced during the Framework development process.

NIST CSF 2.0 – Core:: Functions

- **Govern** —Risk management strategy, expectations, and policy are established, communicated, and monitored.
- **Identify**—Use organizational understanding to minimize risk to systems, assets, data and capabilities.
- **Protect**—Design safeguards to limit the impact of potential events on critical services and infrastructure.
- **Detect**—Implement activities to identify the occurrence of a cybersecurity event.
- **Respond**—Take appropriate action after learning of a security event.
- **Recover**—Plan for resilience and the timely repair of compromised capabilities and services.



NIST CSF 2.0 – Core:: Functions (cont.)

1. GOVERN (GV) — The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored. The GOVERN Function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management (ERM) strategy. GOVERN addresses an understanding of **organizational context**; the establishment of **cybersecurity strategy** and **cybersecurity supply chain risk management**; **roles**, **responsibilities**, and **authorities**; **policy**; and the **oversight of cybersecurity strategy**.

2. IDENTIFY (ID) — The organization's current cybersecurity risks are understood. Understanding the organization's assets (e.g., data, hardware, software, systems, facilities, services, people), suppliers, and related cybersecurity risks enables an organization to prioritize its efforts consistent with its risk management strategy and the mission needs identified under GOVERN. This Function also includes the identification of improvement opportunities for the organization's **policies**, **plans**, **processes**, **procedures**, and **practices** that support **cybersecurity risk management** to inform efforts under all six Functions.

NIST CSF 2.0 – Core:: Functions (cont.)

3. PROTECT (PR) — Safeguards to manage the organization's cybersecurity risks are used. Once assets and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events, as well as to increase the likelihood and impact of taking advantage of opportunities. Outcomes covered by this Function include **identity management**, **authentication**, and **access control**; **awareness and training**; **data security; platform security** (i.e., securing the hardware, software, and services of physical and virtual platforms); and the **resilience of technology infrastructure**.

4. DETECT (DE) — Possible cybersecurity attacks and compromises are found and analyzed. DETECT enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring. This Function supports successful **incident response and recovery activities**.

NIST CSF 2.0 – Core:: Functions (cont.)

5. RESPOND (RS) — Actions regarding a detected cybersecurity incident are taken. RESPOND supports the ability to contain the effects of cybersecurity incidents. Outcomes within this Function cover **incident management**, **analysis**, **mitigation**, **reporting**, and **communication**.

6. RECOVER (RC) — Assets and operations affected by a cybersecurity incident are restored. RECOVER supports the **timely restoration of normal operations** to reduce the effects of cybersecurity incidents and **enable appropriate communication during recovery** efforts.

NIST CSF 2.0 – Core (cont.)

Function	Category	Subcategory
GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored	**Organizational Context (GV.OC):** The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood	**GV.OC-01:** The organizational mission is understood and informs cybersecurity risk management
		GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered

6 Functions **22 Categories** **106 Subcategories**

NIST CSF 2.0 – Core (cont.)

Function	Category	Subcategory	Informative References
GOVERN (GV) 6/31	Organizational Context (GV.OC)	GV.OC 1 - GV.OC 5 [5]	• CRI Profile v2.0 • CSF v1.1 • NICE Framework Components • SP-800-37 Rev 2 • SP 800-53 Rev 5.1.1 • SP 800-218 • SP 800-221A • CIS Controls v8.0 • CCMv4.0
	Risk Management Strategy (GV.RM)	GV.RM 1 - GV.RM 7 [7]	
	Roles, Responsibilities, and Authorities (GV.RR)	GV.RR 1 - GV.RR 4 [4]	
	Policy (GV.PO)	GV.PO 1 - GV.PO 2 [2]	
	Oversight (GV.OV)	GV.OV 1 - GV.OV 3 [3]	
	Cybersecurity Supply Chain Risk Management (GV.SC)	GV.SC 1 - GV.SC 10 [10]	
Identify (ID) 3/21	Asset Management (ID.AM)	ID.AM 1 - ID.AM 8 [7]	
	Risk Assessment (ID.RA)	ID.RA 1 - ID.RA 10 [10]	
	Improvement (ID.IM)	ID.IM 1 - ID.IM 4 [4]	
PROTECT (PR) 5/22	Identity Management, Authentication, and Access Control (PR.AA)	PR.AA 1 - PR.AA 6 [6]	
	Awareness and Training (PR.AT)	PR.AT 1 - PR.AT 2 [2]	
	Data Security (PR.DS)	PR.DS 1 - PR.DS 11 [4]	
	Platform Security (PR.PS)	PR.PS 1 PR.PS 6 [6]	
	Technology Infrastructure Resilience (PR.IR)	PR.IR 1 - PR.IR 4 [4]	
DETECT (DE) 2/11	Continuous Monitoring (DE.CM)	DE.CM 1 - DE.CM 9 [5]	
	Adverse Event Analysis (DE.AE)	DE.AE 2 - DE.AE 8 [6]	
RESPOND (RS) 4/13	Incident Management (RS.MA)	RS.MA 1 - RS.MA 5 [5]	
	Incident Analysis (RS.AN)	RS.AN 3 - RS.AN 8 [4]	
	Incident Response Reporting and Communication (RS.CO)	RS.CO 2 - RS.CO 3 [2]	
	Incident Mitigation (RS.MI)	RS.MI 1 - RS.MI 2 [2]	
RECOVER (RC) 2/8	Incident Recovery Plan Execution (RC.RP)	RC.RP 1 - RC.RP 6 [6]	
	Incident Recovery Communication (RC.CO)	RC.CO 3 - RC.CO 4 [2]	

NIST CSF 2.0 – Profiles

A CSF Organizational Profile describes an organization's current and/or target cybersecurity posture in terms of the Core's outcomes. Organizational Profiles are used to understand, tailor, assess, prioritize, and communicate the Core's outcomes by considering an organization's mission objectives, stakeholder expectations, threat landscape, and requirements. An organization can then prioritize its actions to achieve specific outcomes and communicate that information to stakeholders.

Every Organizational Profile includes one or both of the following:

1. A **Current Profile** specifies the Core outcomes that an organization is currently achieving (or attempting to achieve) and characterizes how or to what extent each outcome is being achieved.
2. A **Target Profile** specifies the desired outcomes that an organization has selected and prioritized for achieving its cybersecurity risk management objectives. A Target Profile considers anticipated changes to the organization's cybersecurity posture, such as new requirements, new technology adoption, and threat intelligence trends.

NIST CSF 2.0 – Profiles (cont.)

Fig: Steps for creating and using a CSF Organizational Profile

NIST CSF 2.0 – Profiles (cont.)

1. Scope the Organizational Profile. Document the high-level facts and assumptions on which the Profile will be based to define its scope. An organization can have as many Organizational Profiles as desired, each with a different scope. For example, a Profile could address an entire organization or be scoped to an organization's financial systems or to countering ransomware threats and handling ransomware incidents involving those financial systems.

2. Gather the information needed to prepare the Organizational Profile. Examples of information may include organizational policies, risk management priorities and resources, enterprise risk profiles, business impact analysis (BIA) registers, cybersecurity requirements and standards followed by the organization, practices and tools (e.g., procedures and safeguards), and work roles.

3. Create the Organizational Profile. Determine what types of information the Profile should include for the selected CSF outcomes, and document the needed information. Consider the risk implications of the Current Profile to inform Target Profile planning and prioritization. Also, consider using a Community Profile as the basis for the Target Profile.

NIST CSF 2.0 – Profiles (cont.)

4. Analyze the gaps between the Current and Target Profiles, and create an action plan. Conduct a gap analysis to identify and analyze the differences between the Current and Target Profiles, and develop a prioritized action plan (e.g., risk register, risk detail report, Plan of Action and Milestones [POA&M]) to address those gaps.

5. Implement the action plan, and update the Organizational Profile. Follow the action plan to address the gaps and move the organization toward the Target Profile. An action plan may have an overall deadline or be ongoing.

NIST CSF 2.0 – Tiers

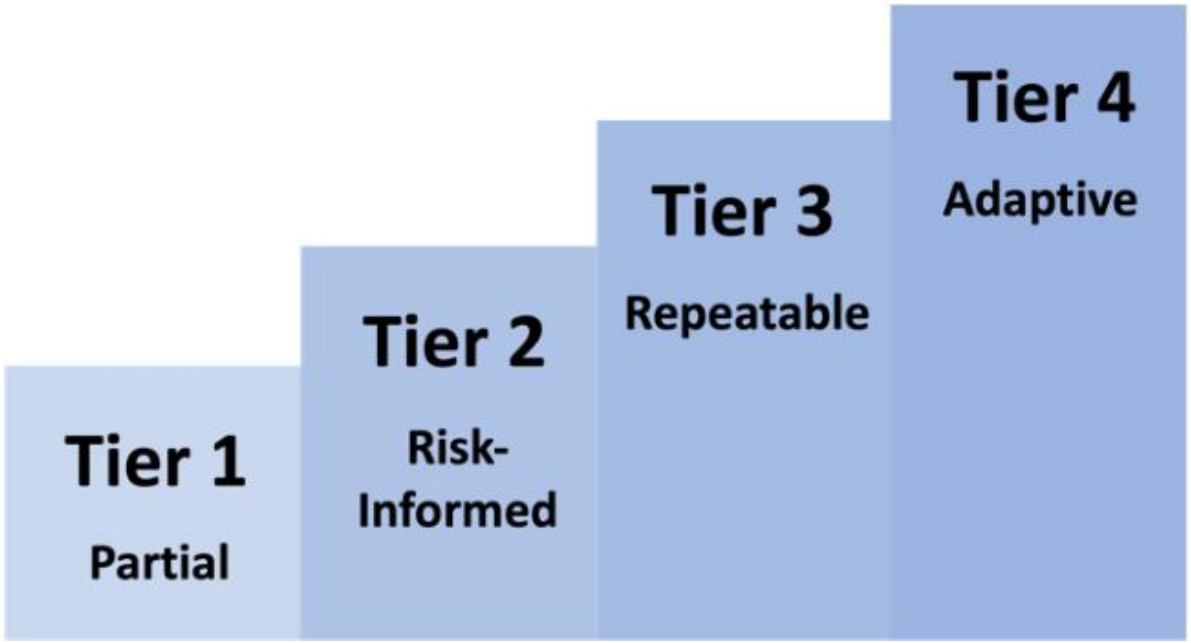


Fig: CSF Tiers for cybersecurity risk governance and management

NIST CSF 2.0 – Tiers

Tier 1: Partial

Tier 2: Risk Informed

Tier 3: Repeatable

Tier 4: Adaptive

	1	2	3	4
	Partial	**Risk Informed**	**Repeatable**	**Adaptive**
Risk Management Process	The functionality and repeatability of cybersecurity risk management			
Integrated Risk Management Program	The extent to which cybersecurity is considered in broader risk management decisions			
External Participation	The degree to which the organization: • **monitors and manages supply chain risk** • benefits my sharing or receiving information from outside parties			

NIST CSF 2.0 – Tiers (cont.)

An organization can choose to use the Tiers to inform its Current and Target Profiles. Tiers characterize the rigor of an organization's cybersecurity risk governance and management practices, and they provide context for how an organization views cybersecurity risks and the processes in place to manage those risks. The Tiers, reflect an organization's practices for managing cybersecurity risk as **Partial (Tier 1)**, **Risk Informed (Tier 2)**, **Repeatable (Tier 3)**, and **Adaptive (Tier 4)**. The Tiers describe a progression from informal, ad hoc responses to approaches that are agile, risk-informed, and continuously improving. Selecting Tiers helps set the overall tone for how an organization will manage its cybersecurity risks.

Tiers should complement an organization's cybersecurity risk management methodology rather than replace it. For example, an organization can use the Tiers to communicate internally as a benchmark for an organization-wide approach to managing cybersecurity risks. Progression to higher Tiers is encouraged when risks or mandates are greater or when a cost-benefit analysis indicates a feasible and cost-effective reduction of negative cybersecurity risks.

NIST CSF 2.0 – Tiers (cont.)

Tier 1: Partial

• **Risk Management Process** – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.

• **Integrated Risk Management Program** – There is limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.

• **External Participation** – The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. The organization does not collaborate with or receive information (e.g., threat intelligence, best practices, technologies) from other entities (e.g., buyers, suppliers, dependencies, dependents, ISAOs, researchers, governments), nor does it share information. The organization is generally unaware of the cyber supply chain risks of the products and services it provides and that it uses.

NIST CSF 2.0 – Tiers (cont.)

Tier 2: Risk Informed

• **Risk Management Process** – Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.

• **Integrated Risk Management Program** – There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established. Cybersecurity information is shared within the organization on an informal basis. Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs, but is not typically repeatable or reoccurring.

• **External Participation** – Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both. The organization collaborates with and receives some information from other entities and generates some of its own information, but may not share information with others. Additionally, the organization is aware of the cyber supply chain risks associated with the products and services it provides and uses, but does not act consistently or formally upon those risks.

NIST CSF 2.0 – Tiers (cont.)

Tier 3: Repeatable

• **Risk Management Process** – The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.

• **Integrated Risk Management Program** – There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. The organization consistently and accurately monitors the cybersecurity risk of organizational assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risk. Senior executives ensure consideration of cybersecurity through all lines of operation in the organization.

• **External Participation** - The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks. It collaborates with and receives information from other entities regularly that complements internally generated information, and shares information with other entities. The organization is aware of the cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it usually acts formally upon those risks, including mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring.

NIST CSF 2.0 – Tiers (cont.)

Tier 4: Adaptive

• **Risk Management Process** – The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing threat and technology landscape and responds in a timely and effective manner to evolving sophisticated threats.

• **Integrated Risk Management Program** – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risk and organizational objectives is clearly understood and considered when making decisions. Senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement an executive vision and analyze system-level risks in the context of organizational risk tolerances. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities and continuous awareness of activities on their systems and networks. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated.

• **External Participation** - The organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks. It receives, generates, and reviews prioritized information that informs the continuous analysis of its risks as the threat and technology landscapes evolve. The organization shares that information internally and externally with other collaborators. The organization uses real-time or near real-time information to understand and consistently act upon cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it communicates proactively, using formal (e.g. agreements) and informal mechanisms to develop and maintain strong supply chain relationships.

Improving Cybersecurity Risk Communication and Integration

- Improving Risk Management Communication
- Improving Integration with Other Risk Management Programs

Improving Risk Management Communication

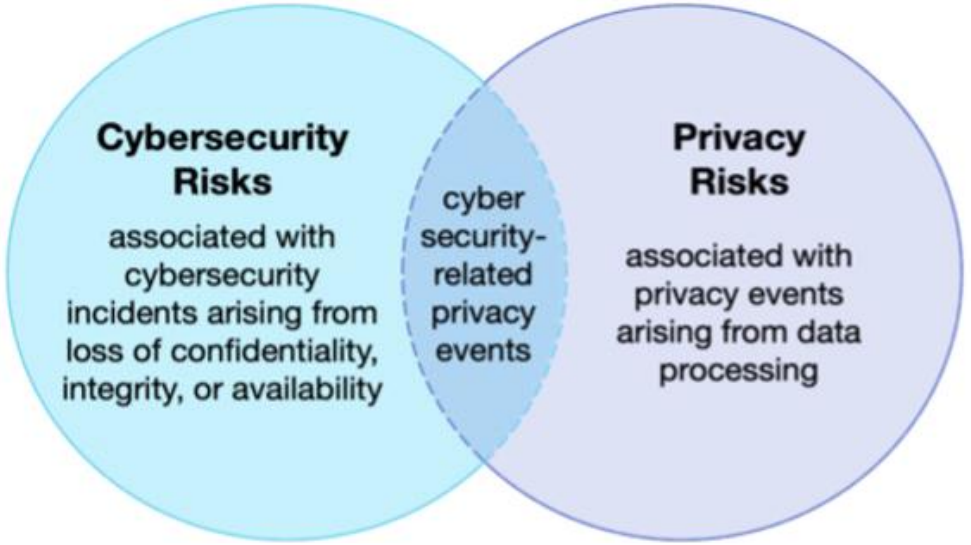
Fig: Using the CSF to improve risk management communication

Improving Integration with Other Risk Management Programs

Every organization faces numerous types of ICT risk (e.g., privacy, supply chain, artificial intelligence) and may use frameworks and management tools that are specific to each risk. Some organizations integrate ICT and all other risk management efforts at a high level by using ERM, while others keep the efforts separate to ensure adequate attention on each small organizations by their nature may monitor risk at the enterprise level, while larger companies may maintain separate risk management efforts integrated into the ERM.

Organizations can employ an ERM approach to balance a portfolio of risk considerations, including cybersecurity, and make informed decisions. Executives receive significant input about current and planned risk activities as they integrate governance and risk strategies with results from previous uses of the CSF. The CSF helps organizations to translate their terminology for cybersecurity and cybersecurity risk management into general risk management language that executives will understand.

Cybersecurity Risk & Privacy Risk



While cybersecurity and privacy are independent disciplines, their objectives overlap in certain circumstances.

Cybersecurity risk management is essential for addressing privacy risks related to the loss of the confidentiality, integrity, and availability of individuals' data. For example, data breaches could lead to identity theft. However, privacy risks can also arise by means that are unrelated to cybersecurity incidents.

An organization processes data to achieve mission or business purposes, which can sometimes give rise to *privacy events* whereby individuals may experience problems as a result of the data processing. These problems can be expressed in various ways, but NIST describes them as ranging from dignity-type effects (e.g., embarrassment or stigma) to more tangible harms (e.g., discrimination, economic loss, or physical harm).

Cybersecurity Risk Governance vs Management Practices

Tier	Cybersecurity Risk Governance Practices (GV)	Cybersecurity Risk Management Practices (ID, PR, DE, RS, and RC)
Tier 1: Partial	Application of the organizational cybersecurity risk strategy is managed in an ad hoc manner. Prioritization is ad hoc and not formally based on objectives or threat environment.	There is limited awareness of cybersecurity risks at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis. The organization may not have processes that enable cybersecurity information to be shared within the organization. The organization is generally unaware of the cybersecurity risks associated with its suppliers and the products and services it acquires and uses.
Tier 2: Risk Informed	Risk management practices are approved by management but may not be established as organization-wide policy. The prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/ mission requirements.	There is an awareness of cybersecurity risks at the organizational level, but an organization-wide approach to managing cybersecurity risks has not been established. Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs but is not typically repeatable or reoccurring. Cybersecurity information is shared within the organization on an informal basis. The organization is aware of the cybersecurity risks associated with its suppliers and the products and services it acquires and uses, but it does not act consistently or formally in response to those risks.

Cybersecurity Risk Governance vs Management Practices

Tier	Cybersecurity Risk Governance Practices (GV)	Cybersecurity Risk Management Practices (ID, PR, DE, RS, and RC)
Tier 3: Repeatable	The organization's risk management practices are formally approved and expressed as policy. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/ mission requirements, threats, and technological landscape.	There is an organization-wide approach to managing cybersecurity risks. Cybersecurity information is routinely shared throughout the organization. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. The organization consistently and accurately monitors the cybersecurity risks of assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risks. Executives ensure that cybersecurity is considered through all lines of operation in the organization. The organization risk strategy is informed by the cybersecurity risks associated with its suppliers and the products and services it acquires and uses. Personnel formally act upon those risks through mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring. These actions are implemented consistently and as intended and are continuously monitored and reviewed.

Cybersecurity Risk Governance vs Management Practices

Tier	Cybersecurity Risk Governance Practices (GV)	Cybersecurity Risk Management Practices (ID, PR, DE, RS, and RC)
Tier 4: Adaptive	There is an organization-wide approach to managing cybersecurity risks that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risks and organizational objectives is clearly understood and considered when making decisions. Executives monitor cybersecurity risks in the same context as financial and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances. Cybersecurity risk management is part of the organizational culture. It evolves from an awareness of previous activities and continuous awareness of activities on organizational systems and networks. The organization can quickly and efficiently account for changes to business/ mission objectives in how risk is approached and communicated.	The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement that incorporates advanced cybersecurity technologies and practices, the organization actively adapts to a changing technological landscape and responds in a timely and effective manner to evolving, sophisticated threats. The organization uses real-time or near real-time information to understand and consistently act upon the cybersecurity risks associated with its suppliers and the products and services it acquires and uses. Cybersecurity information is constantly shared throughout the organization and with authorized third parties.

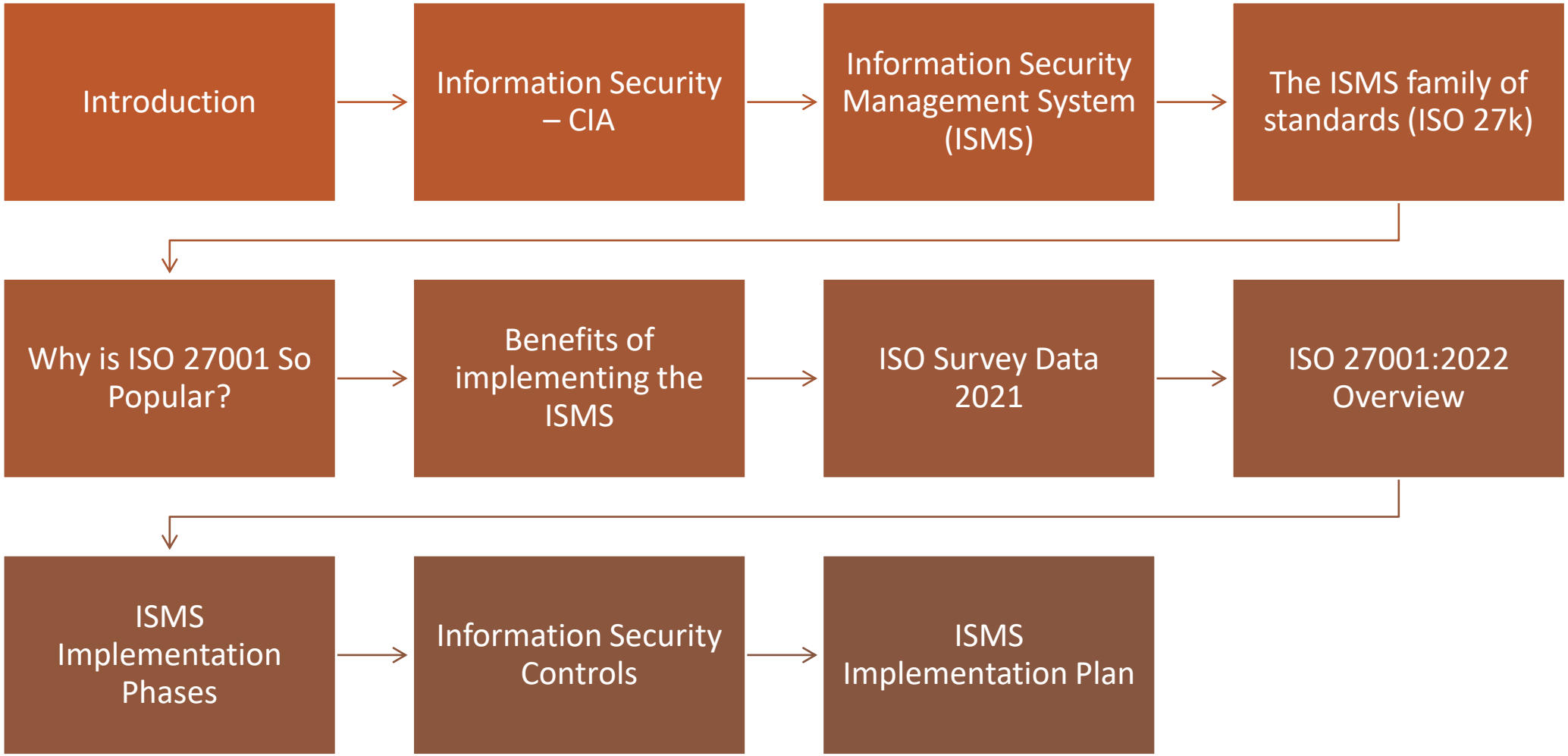
NIST CSF 2.0 – Core - Informative References:
CIS CSC [Center for Internet Security – Critical Security Controls]

SL	Controls
1	Inventory and Control of Hardware Assets
2	Inventory and Control of Software Assets
3	Continuous Vulnerability Management
4	Controlled Use of Administrative Privileges
5	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6	Maintenance, Monitoring, and Analysis of Audit Logs
7	Email and Web Browser Protections
8	Malware Defenses
9	Limitation and Control of Network Ports, Protocols, and Services
10	Data Recovery Capability
11	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on the Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Security Skills Assessment
18	Application Software Security
19	Incident Response and Management
20	Penetration Tests and Red Team Exercises

THIS PAGE INTENTIONALLY LEFT BLANK

ISO 27001
Information Security Management System (ISMS)

ISO 27000 Series – Outline



Introduction

What is ISO 27001?

- This International Standard has been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS).
- Published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
- The latest version is ISO 27001:2022.

Introduction (cont.)

Purpose of ISO 27001:

- ❑ Helps organizations identify, assess, and manage information security risks.
- ❑ Ensures compliance with regulatory and legal requirements.
- ❑ Builds trust with customers and stakeholders by demonstrating commitment to security.

Who Needs ISO 27001?

- ❑ Any organization that handles sensitive information, including:
  - Financial institutions
  - Healthcare providers
  - IT service companies
  - Government agencies
- ❑ Any business concerned with data protection

Information Security - CIA

Information Security:

- Confidentiality
- Integrity
- Availability

In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

Information Security Management System (ISMS)

An Information Security Management System (ISMS) is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives.

Information Security Management System (ISMS) (cont.)

Components of an ISMS:

- ❑ Policy
- ❑ Persons with defined responsibilities
- ❑ Documented information
- ❑ Information security risk assessment
- ❑ Information security risk treatment, including determination and implementation of controls

- ❑ **Management processes related to:**
  - Policy establishment
  - Awareness and competence provision
  - Planning
  - Implementation
  - Operation
  - Performance assessment
  - Management review
  - Improvement

Information Security Management System (ISMS) (cont.)

Risk:

- Risk is often expressed in terms of a combination of the consequences of an event and the associated "likelihood" of occurrence.
- Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.

Information Security Management System (ISMS) (cont.)

- An **ISMS** is based on a **risk assessment** and the organization's risk acceptance levels designed to effectively treat and manage risks.
- Analyzing **requirements** for the protection of information assets and applying appropriate **controls** to ensure the protection of these information assets, as required, contributes to the successful implementation of an **ISMS.**

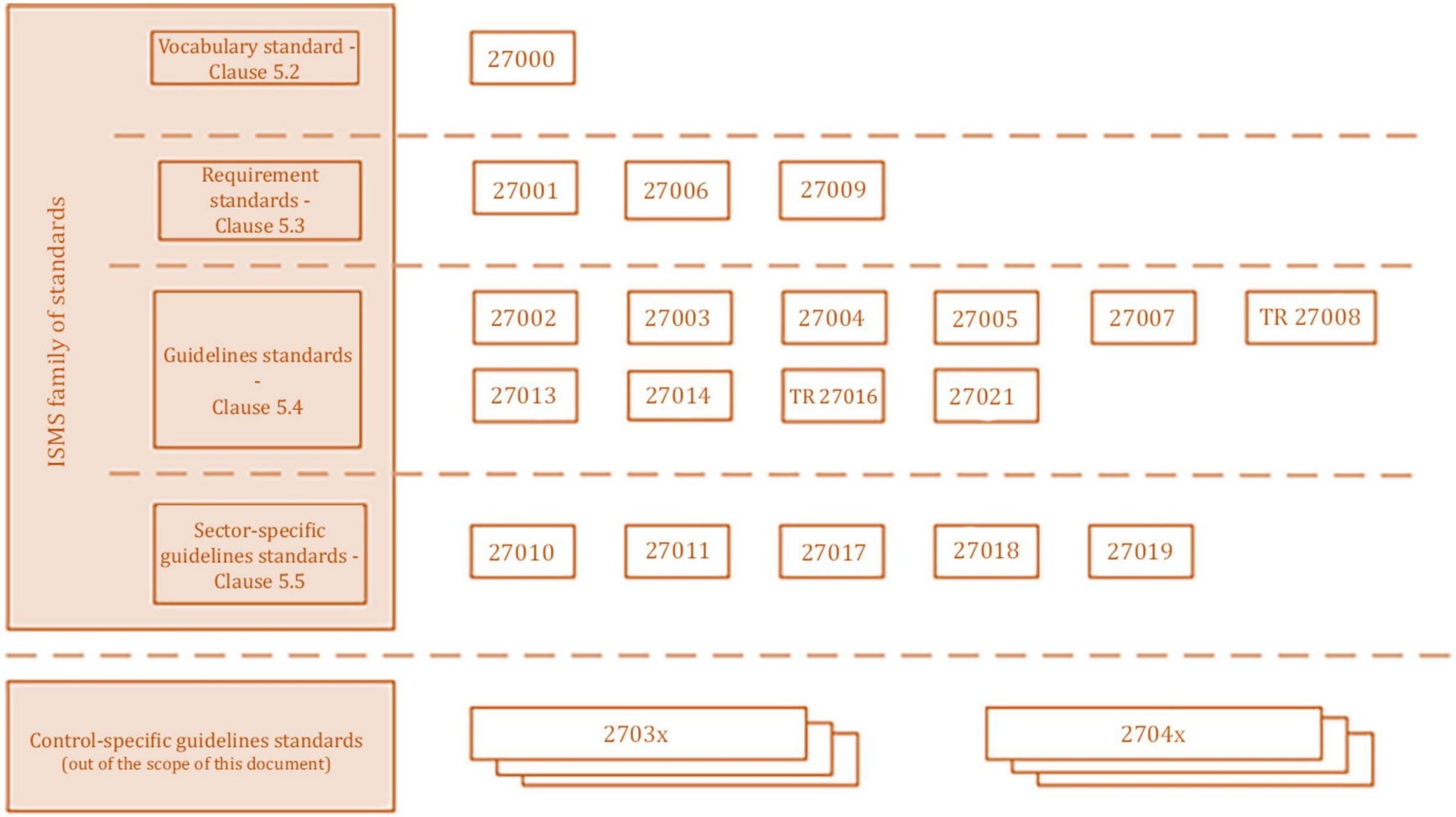
ISO 27001 is the commonly used standard for ISMS implementation and certification

Information Security Management System (ISMS) (cont.)

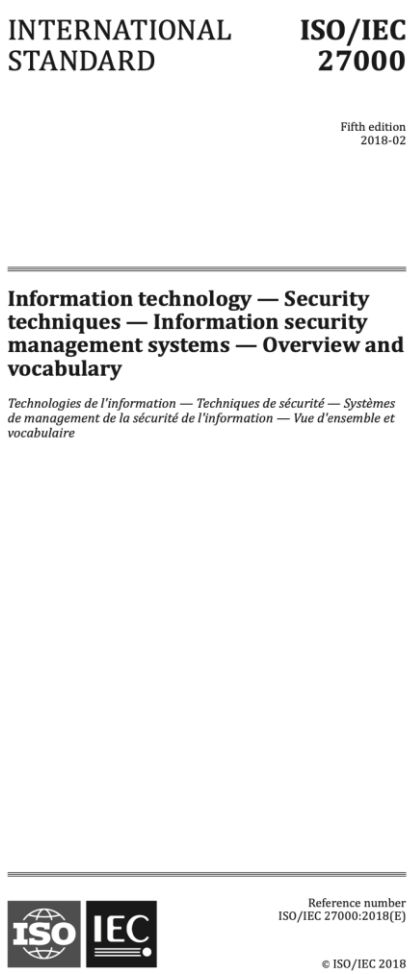
What You Need to know about the ISMS:

- The requirements set in ISO 27001 are generic, flexible and useful to all types of organizations.
- The ISMS focuses on interested parties, their needs and expectations.
- The ISMS uses a risk-based approach.
- The ISMS is about processes and continual improvement.
- Processes are more important than policies and other documents! Start collecting records (evidence) right now!
- Don't focus on certification in the beginning, implement the processes first. It usually takes 1-2 years.
- Implementing an ISMS is a long and complicated project.

The ISMS Family of Standards (ISO 27k)



The ISMS Family of Standards (ISO 27k) (cont.)


INTERNATIONAL STANDARD

ISO/IEC 27000

Fifth edition
2018-02

Information technology — Security techniques — Information security management systems — Overview and vocabulary

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire

ISO IEC

Reference number
ISO/IEC 27000:2018(E)

© ISO/IEC 2018

ISO 27000 Overview and Vocabulary:

ISO/IEC 27000:2018 provides the overview of information security management systems (ISMS).

It also provides terms and definitions commonly used in the ISMS family of standards. This document is applicable to all types and sizes of organization.

The terms and definitions provided in this document

- ❑ cover commonly used terms and definitions in the ISMS family of standards;
- ❑ do not cover all terms and definitions applied within the ISMS family of standards; and
- ❑ do not limit the ISMS family of standards in defining new terms for use.

The ISMS Family of Standards (ISO 27k) (cont.)


INTERNATIONAL STANDARD

ISO/IEC 27001

Third edition
2022-10

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences

ISO IEC

Reference number
ISO/IEC 27001:2022(E)

© ISO/IEC 2022

ISO 27001 ISMS Requirements:

- This standard specifies the requirements for establishing, implementing, maintaining and continually improving an
- information security management system (ISMS) within the context of the organization.
- This document also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.
- The requirements set out in this document are generic and are intended to be applicable to all organizations, regardless of type, size or nature.
- Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this document.

The ISMS Family of Standards (ISO 27k) (cont.)


INTERNATIONAL STANDARD

ISO/IEC 27002

Third edition
2022-02

Information security, cybersecurity and privacy protection — Information security controls

Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information

Reference number
ISO/IEC 27002:2022(E)

© ISO/IEC 2022

ISO 27002 Information Security controls:

This document provides a reference set of generic information security controls including implementation guidance. This document is designed to be used by organizations:

- ❑ within the context of an information security management system (ISMS) based on ISO/IEC 27001;
- ❑ for implementing information security controls based on internationally recognized best practices;
- ❑ for developing organization-specific information security management guidelines.

The ISMS Family of Standards (ISO 27k) (cont.)


INTERNATIONAL STANDARD

ISO/IEC 27003

Second edition
2017-03

Information technology — Security techniques — Information security management systems — Guidance

Technologies de l'information — Techniques de sécurité --Systèmes de management de la sécurité de l'information — Lignes directrices

Reference number
ISO/IEC 27003:2017(E)

© ISO/IEC 2017

ISO 27003 ISMS Guidance:

- This document provides guidance on the requirements for an information security management system (ISMS) as specified in ISO/IEC 27001 and provides recommendations ('should'), possibilities ('can') and permissions ('may') in relation to them.
- It is not the intention of this document to provide general guidance on all aspects of information security.

The ISMS Family of Standards (ISO 27k) (cont.)


INTERNATIONAL STANDARD

ISO/IEC 27005

Fourth edition
2022-10

Information security, cybersecurity and privacy protection — Guidance on managing information security risks

Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information

Reference number
ISO/IEC 27005:2022(E)

© ISO/IEC 2022

ISO 27005 Guidance on Managing IS Risks:

This document provides guidance to assist organizations to:

- ❑ fulfil the requirements of ISO/IEC 27001 concerning actions to address information security risks;
- ❑ perform information security risk management activities, specifically information security risk assessment and treatment.

This document is applicable to all organizations, regardless of type, size or sector.

The ISMS Family of Standards (ISO 27k) (cont.)


INTERNATIONAL STANDARD

ISO/IEC 27701

First edition
2019-08

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

Techniques de sécurité — Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée — Exigences et lignes directrices

Reference number
ISO/IEC 27701:2019(E)

© ISO/IEC 2019

ISO 27701 Extension for Privacy:

- This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization.
- This document specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing.
- This document is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which are PII controllers and/or PII processors processing PII within an ISMS.

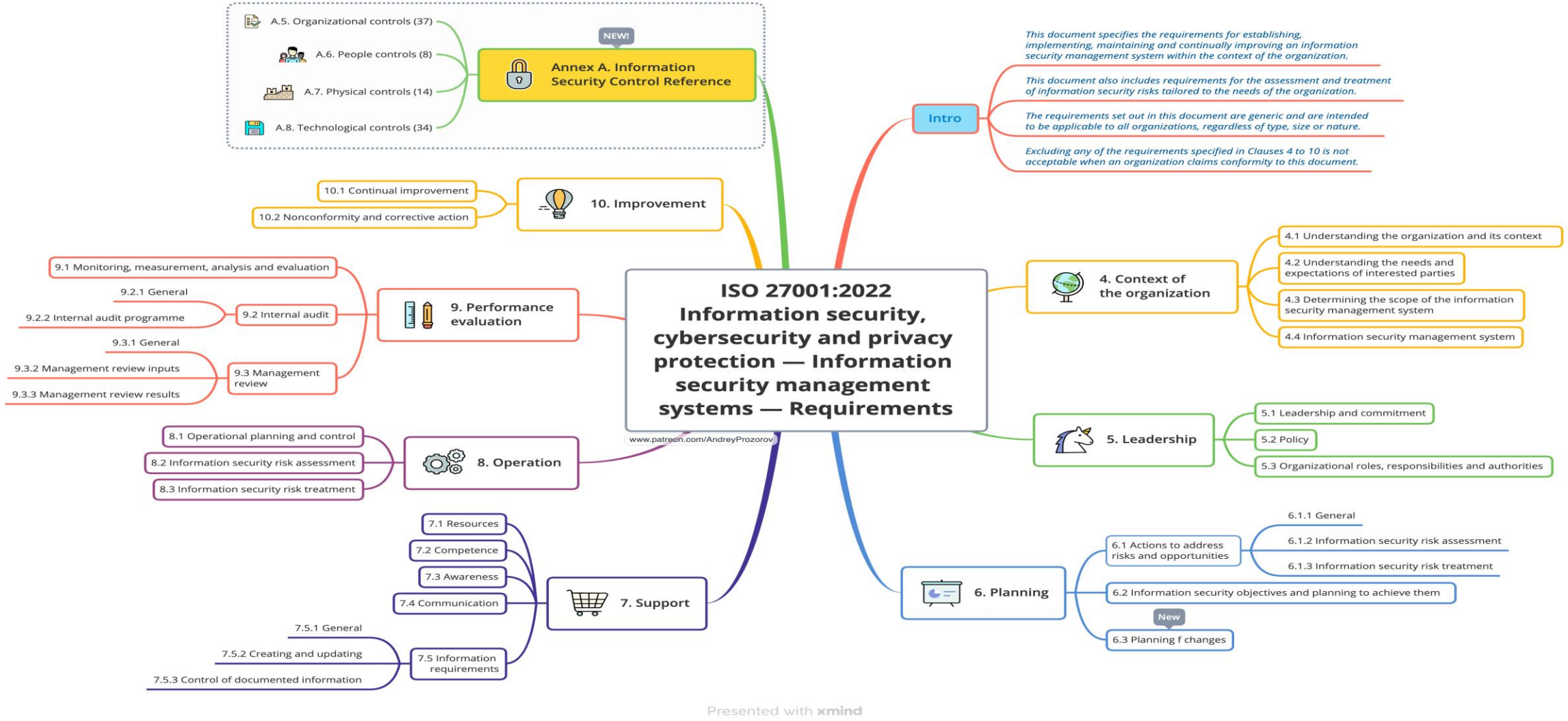
Why is ISO 27001 So Popular?

- Applicable to all organizations, regardless of type, size or nature
- It is short (21 pages) and simple (ISMS + IS controls)
- It is aligned with other management systems (e.g., QMS, PIMS, SMS, BCMS)
- It is time-tested (BS 7799-1 was published in 1995)
- It contains simple but valuable principles (e.g., understanding the needs and expectations of interested parties, leadership and commitment, continual improvement, process approach, risk-based approach)
- You can find many additional recommendations, guidelines and courses
- You can certify your ISMS (for some countries / industries this is a mandatory requirement)
- Many other IS standards and frameworks are inspired by ISO 27001
- Many IS professionals use this standard, so they speak the same language

Benefits of Implementing the ISMS

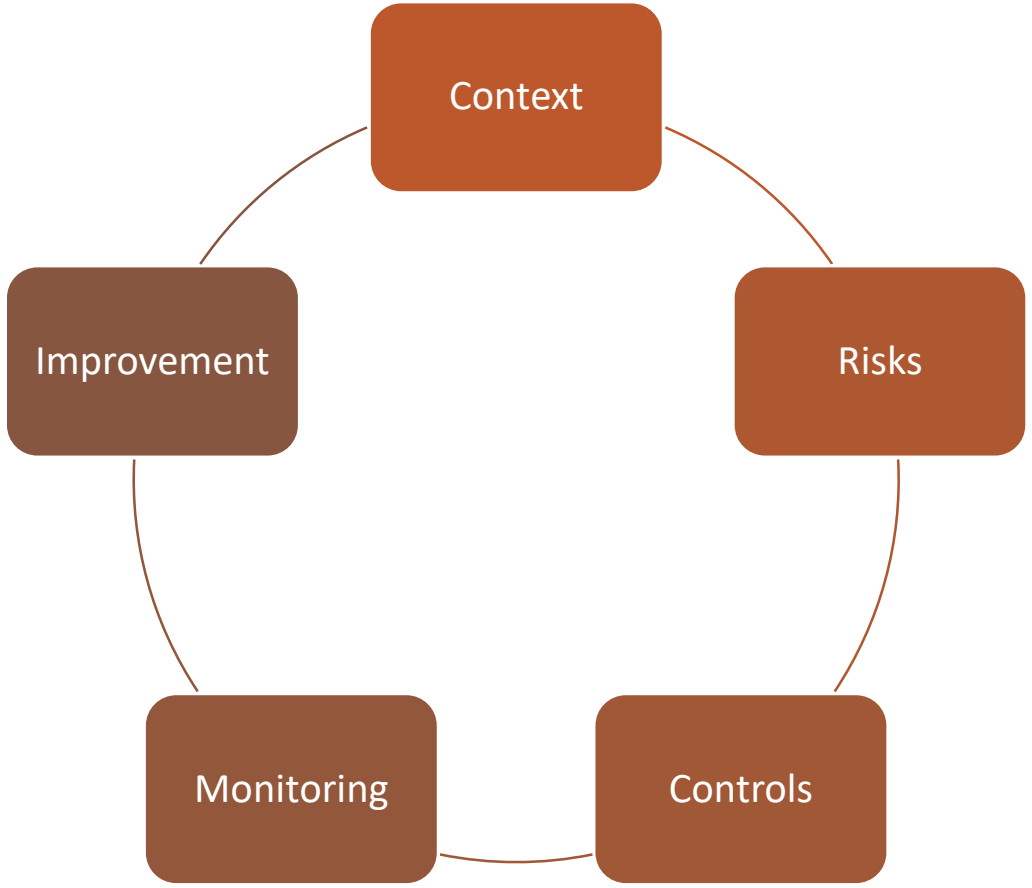
- Improved overall security (including incident response and cyber resilience)
- Raising awareness and information security culture
- Reducing business risks
- Building stakeholder trust (external and internal)
- Legal, regulatory and contractual compliance (information security and data protection)
- A common approach to compliance with different information security requirements
- Increasing the maturity of related processes (e.g., IT, HR, Governance)
- Increasing the transparency and justification of information security budgets
- Marketing opportunities

ISO 27001:2022 Overview



ISMS Implementation Phases

1. Understanding the organization's needs and the necessity for establishing information security policy and information security objectives.
2. Assessing the organization's risks related to information security.
3. Implementing and operating information security processes, controls and other measures to treat risks.
4. Monitoring and reviewing the performance and effectiveness of the ISMS.
5. Practicing continual improvement.



Information Security Controls

Control: measure that maintains and/or modifies risk.

Total number of controls – 93, 11 new (2022)

Controls are categorized as:

- **People**, if they concern individual people
- **Physical**, if they concern physical objects
- **Technological**, if they concern technology
- otherwise, they are categorized as **Organizational**

Five attributes only in ISO 27002:2022:

1. Control type (Preventive, Detective, Corrective)
2. Information security properties (CIA)
3. Cybersecurity concepts (Identify, Protect, Detect, Respond and Recover)
4. Operational capabilities
5. Security domains

Information Security Controls (cont.)

5. Organizational controls	6. People controls	8. Technological controls
5.1. Policies for information security	6.1. Screening	8.1. User endpoint devices
5.2. Information security roles and responsibilities	6.2. Terms and conditions of employment	8.2. Privileged access rights
5.3. Segregation of duties	6.3. Information security awareness, education and training	8.3. Information access restriction
5.4. Management responsibilities	6.4. Disciplinary process	8.4. Access to source code
5.5. Contact with authorities	6.5. Responsibilities after termination or change of employment	8.5. Secure authentication
5.6. Contact with special interest groups	6.6. Confidentiality or non-disclosure agreements	8.6. Capacity management
5.7. Threat intelligence	6.7. Remote working	8.7. Protection against malware
5.8. Information security in project management	6.8. Information security event reporting	8.8. Management of technical vulnerabilities
5.9. Inventory of information and other associated assets	**7. Physical controls**	8.9. Configuration management
5.10. Acceptable use of information and other associated assets	7.1. Physical security perimeter	8.10. Information deletion
5.11. Return of assets	7.2. Physical entry	8.11. Data masking
5.12. Classification of information	7.3. Securing offices, rooms and facilities	8.12. Data leakage prevention
5.13. Labelling of information	7.4. Physical security monitoring	8.13. Information backup
5.14. Information transfer	7.5. Protecting against physical and environmental threats	8.14. Redundancy of information processing facilities
5.15. Access control	7.6. Working in secure areas	8.15. Logging
5.16. Identity management	7.7. Clear desk and clear screen	8.16. Monitoring activities
5.17. Authentication information	7.8. Equipment siting and protection	8.17. Clock synchronization
5.18. Access rights	7.9. Security of assets off-premises	8.18. Use of privileged utility programs
5.19. Information security in supplier relationships	7.10. Storage media	8.19. Installation of software on operational systems
5.20. Addressing information security within supplier agreements	7.11. Supporting utilities	8.20. Network security
5.21. Managing information security in the ICT supply chain	7.12. Cabling security	8.21. Security of network services
5.22. Monitoring, review and change management of supplier services	7.13. Equipment maintenance	8.22. Segregation of networks
5.23. Information security for use of cloud services	7.14. Secure disposal or re-use of equipment	8.23. Web filtering
5.24. Information security incident management planning and preparation		8.24. Use of cryptography
5.25. Assessment and decision on information security events		8.25. Secure development life cycle
5.26. Response to information security incidents		8.26. Application security requirements
5.27. Learning from information security incidents		8.27. Secure system architecture and engineering principles
5.28. Collection of evidence		8.28. Secure coding
5.29. Information security during disruption		8.29. Security testing in development and acceptance
5.30. ICT readiness for business continuity		8.30. Outsourced development
5.31. Legal, statutory, regulatory and contractual requirements		8.31. Separation of development, test and production environments
5.32. Intellectual property rights		8.32. Change management
5.33. Protection of records		8.33. Test information
5.34. Privacy and protection of PII		8.34. Protection of information systems during audit testing
5.35. Independent review of information security		
5.36. Compliance with policies, rules and standards for information security		
5.37. Documented operating procedures		

*New control, 2022

ISMS Implementation Plan

Stage	Duration (days)						
	Optimistic	Realistic	Pessimistic	PERT	ΔPERT	Min	Max
0. Read ISO 27001 and additional materials	0,0	1,0	5,0	1,5	0,8	0,7	2,3
1. Conduct awareness trainings for the top management	0,5	1,0	5,0	1,6	0,8	0,8	2,3
2. Conduct a GAP analysis	2,0	5,0	10,0	5,3	1,3	4,0	6,7
3. Understand the Context	2,0	5,0	10,0	5,3	1,3	4,0	6,7
4. Plan the Implementation	1,0	3,0	5,0	3,0	0,7	2,3	3,7
5. Conduct the first IS Committee meeting	0,5	1,0	5,0	1,6	0,8	0,8	2,3
6. Establish Information Security Policy and Information Security Objectives	1,0	3,0	10,0	3,8	1,5	2,3	5,3
7. Take an inventory of the assets	3,0	6,0	15,0	7,0	2,0	5,0	9,0
8. Define a Method of Risk Assessment, identify and assess information security risks	5,0	15,0	30,0	15,8	4,2	11,7	20,0
9. Prepare Statement of Applicability (SoA) and Risk Treatment Plan (RTP)	5,0	10,0	20,0	10,8	2,5	8,3	13,3
10. Define requirements for documentation management	3,0	5,0	30,0	8,8	4,5	4,3	13,3
11. Develop ISMS Framework and define roles and responsibilities	5,0	10,0	30,0	12,5	4,2	8,3	16,7
12. Develop and implement a set of ISMS policies and procedures	30,0	90,0	180,0	95,0	25,0	70,0	120,0
13. Plan and implement additional information security measures	0,0	40,0	180,0	56,7	30,0	26,7	86,7
14. Plan, prepare and conduct awareness trainings	10,0	20,0	40,0	21,7	5,0	16,7	26,7
15. Operate the ISMS	60,0	120,0	360,0	150,0	50,0	100,0	200,0
16. Monitor the ISMS	5,0	10,0	20,0	10,8	2,5	8,3	13,3
17. Audit the ISMS	3,0	10,0	20,0	10,5	2,8	7,7	13,3
18. Conduct the ISMS Management review	2,0	5,0	10,0	5,3	1,3	4,0	6,7
19. Practice continual improvement	30,0	60,0	180,0	75,0	25,0	50,0	100,0
20. Prepare for the certification audit	20,0	30,0	60,0	33,3	6,7	26,7	40,0
Total	188,0	450,0	1225,0	535,5	172,8	362,7	708,3

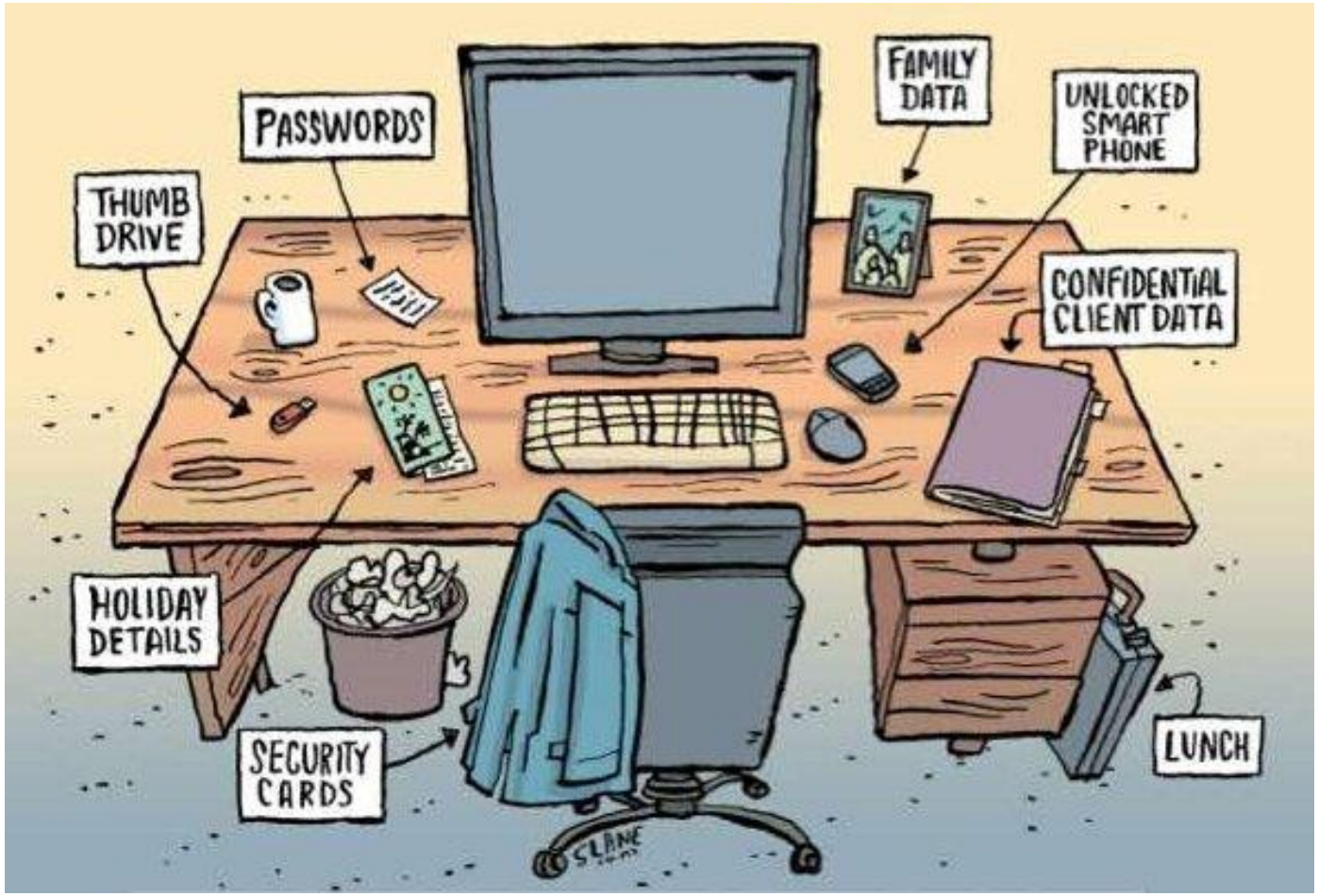
ISO 27001: 2022

Domain/Control Name	Number of Controls
Organizational controls	37
People controls	8
Physical controls	14
Technological controls	34
4	**93**

ISO 27001: 2013

Domain/Control Name	Number of Controls
Information security policies	2
Organization of information security	7
Human resource security	6
Asset management	10
Access control	14
Cryptography	2
Physical and environmental security	15
Operations security	14
Communications security	7
System acquisition, development and maintenance	13
Supplier relationships	5
Information security incident management	7
Information security aspects of business continuity management	4
Compliance	8
14	**114**

ISO 27001 (Glimpses)



Clean Desk Clear Screen

ISO 27001 (Glimpses)

Control of IT Asset

ISO 27001 (Glimpses)

Data Sharing Etiquettes

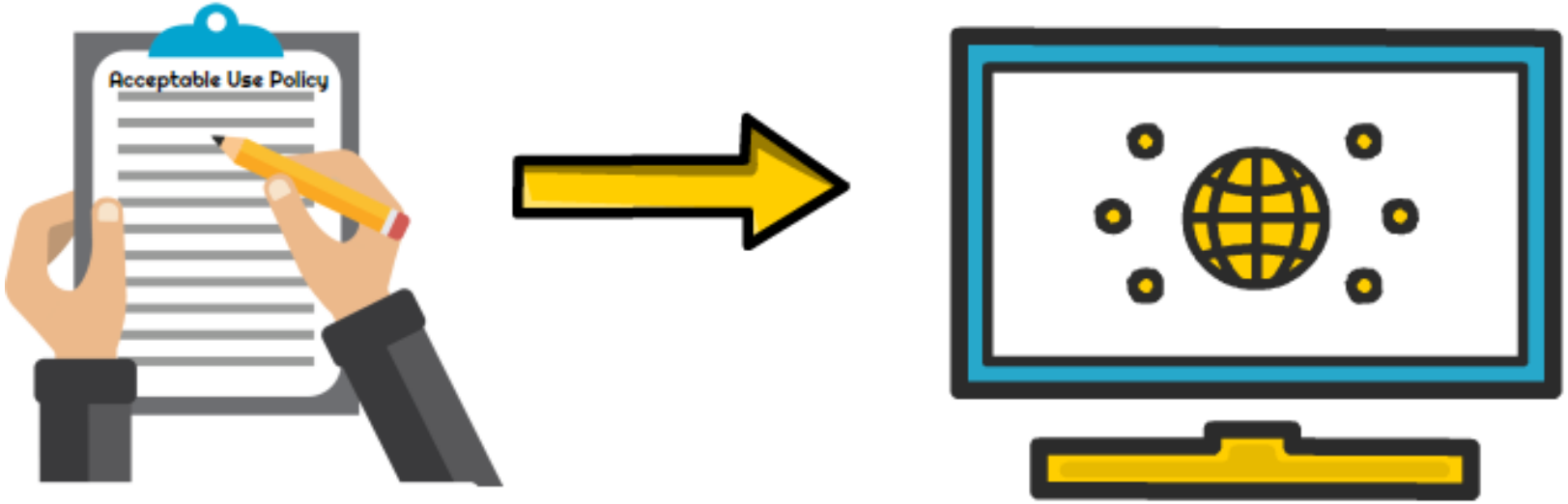
ISO 27001 (Glimpses)

CCTV Implementation

ISO 27001 (Glimpses)

Acceptable Use Policy (AUP)

Specific policy for a computer network
that employees must sign before receiving access.



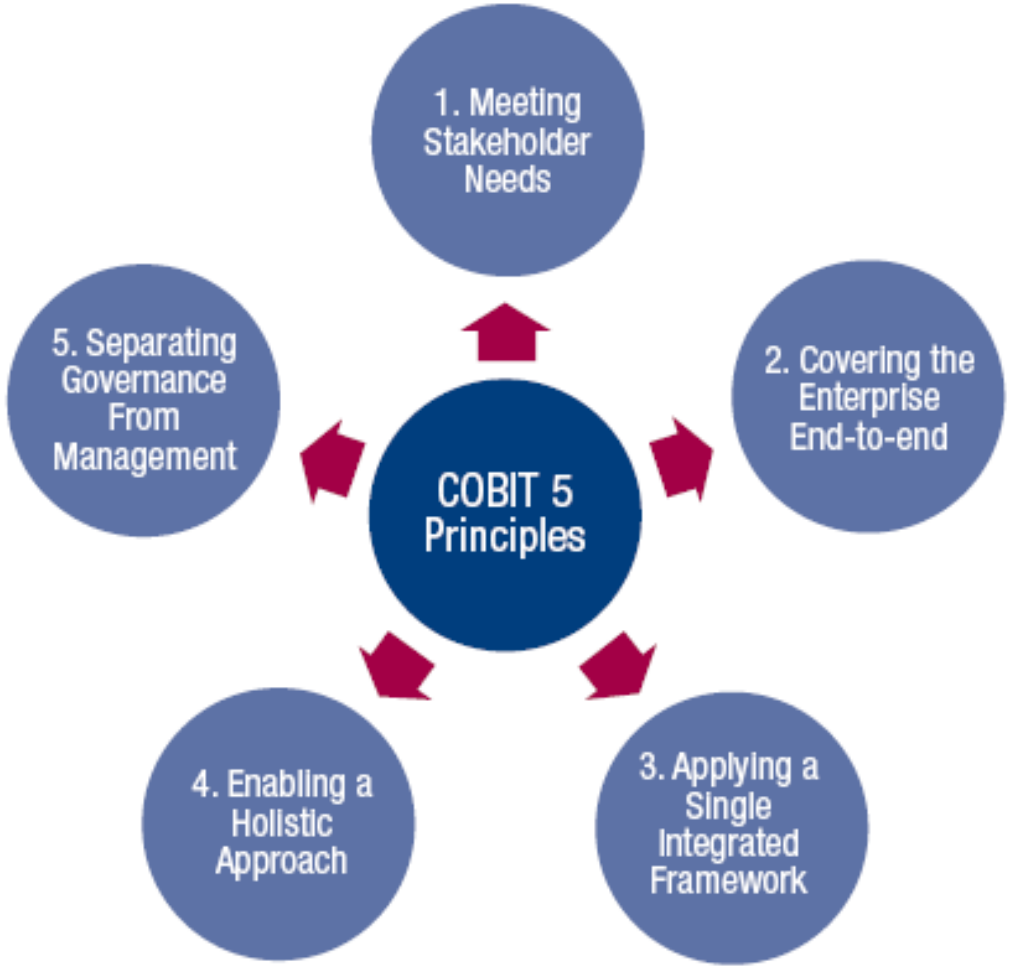
THIS PAGE INTENTIONALLY LEFT BLANK

COBIT 5

Control OBjectives for Information and related Technologies

COBIT 5 Overview

COBIT 5 provides a comprehensive framework for the governance and management of enterprise IT and extensively addresses IT security, governance, risk and information security in general. Because many aspects of information security involve IT and related activities, it can serve as a framework for determining the desired state for effective information security. COBIT 5 for Information Security builds on the COBIT 5 framework and focuses on information security, providing detailed and practical guidance for information security professionals and other stakeholders.



COBIT 5 Principles Cont.

Principle 1 – Meeting Stakeholder Needs:

Enterprises exist to create value for their stakeholders by maintaining a balance between the realization of benefits and the optimization of risk and use of resources.

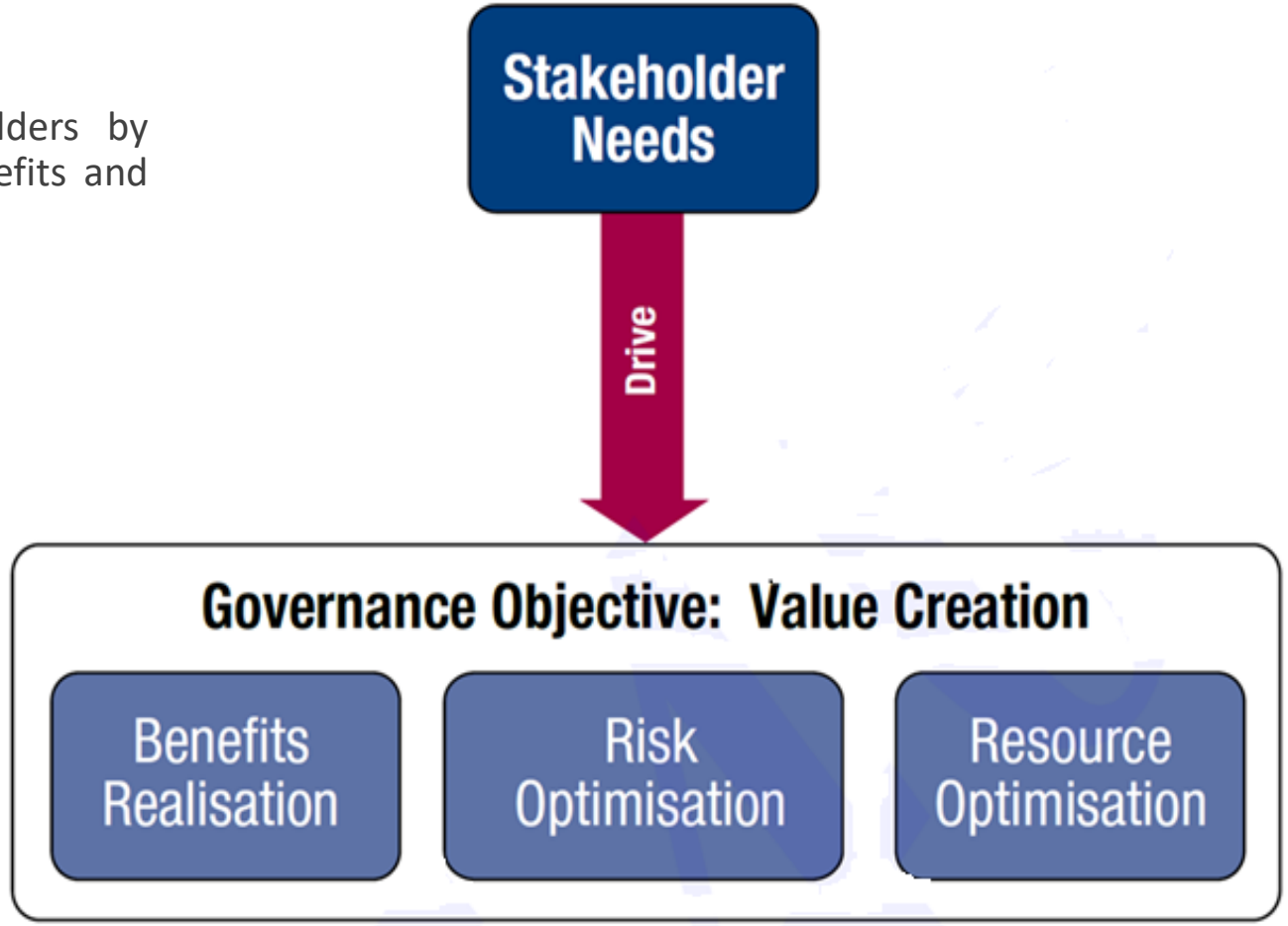


Fig: The Governance Objective: Value Creation

COBIT 5 Principles Cont.

Principle 2 – Covering the Enterprise End-to-end:

Covering the Enterprise End-to-end—COBIT 5 integrates governance of enterprise IT into enterprise governance:

- It covers all functions and processes within the enterprise; COBIT 5 does not focus on only the
- "IT function," but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise.
- It considers all IT-related governance and management enablers to be enterprise wide and end-to-end.

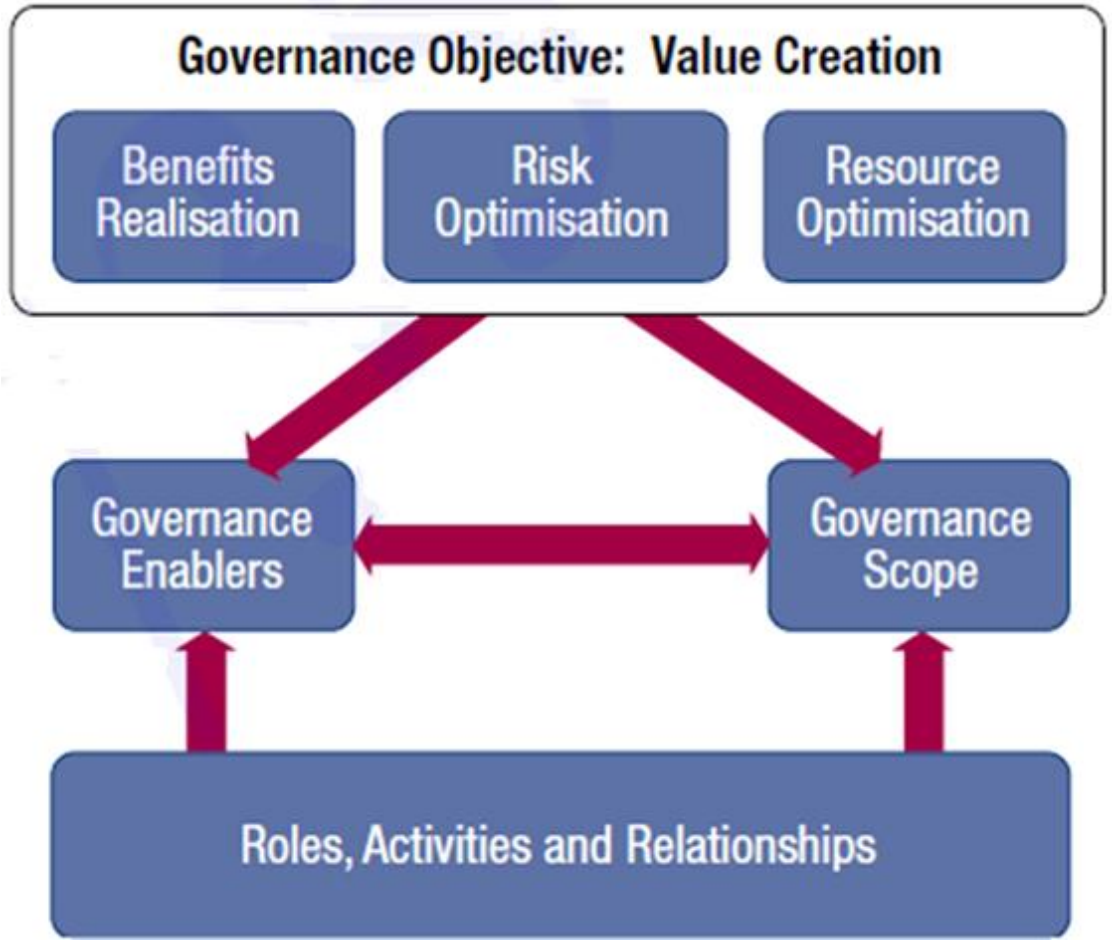


Fig: Governance and Management in COBIT 5

COBIT 5 Principles Cont.

Principle 2 – Covering the Enterprise End-to-end (Continued):

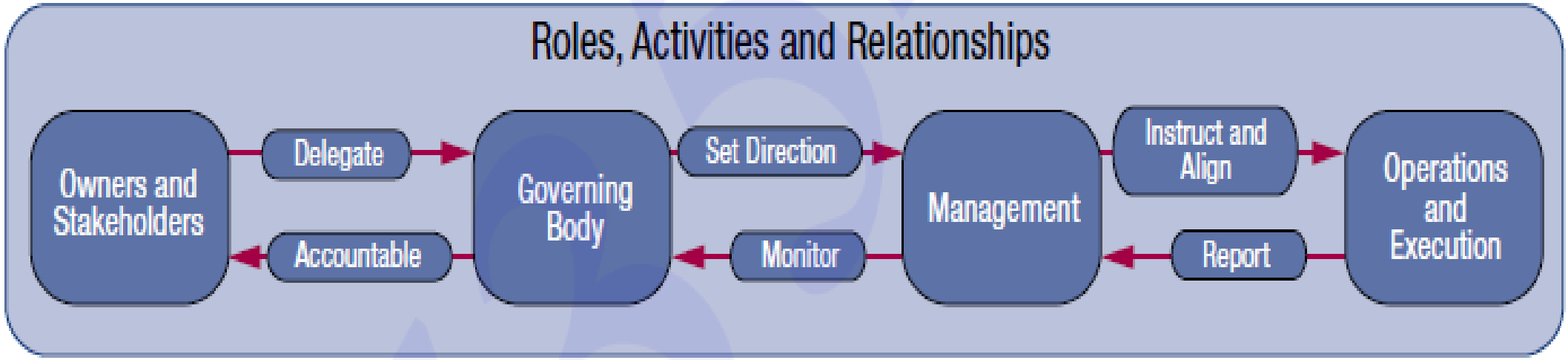


Fig: Key Roles, Activities and Relationships

COBIT 5 Principles Cont.

Principle 3 – Applying a Single, Integrated Framework:

There are many IT-related standards and good practices, each providing guidance on a subset of IT and information security activities. At a high level, COBIT 5 aligns with other relevant standards and frameworks such as the ISO 27000 series.

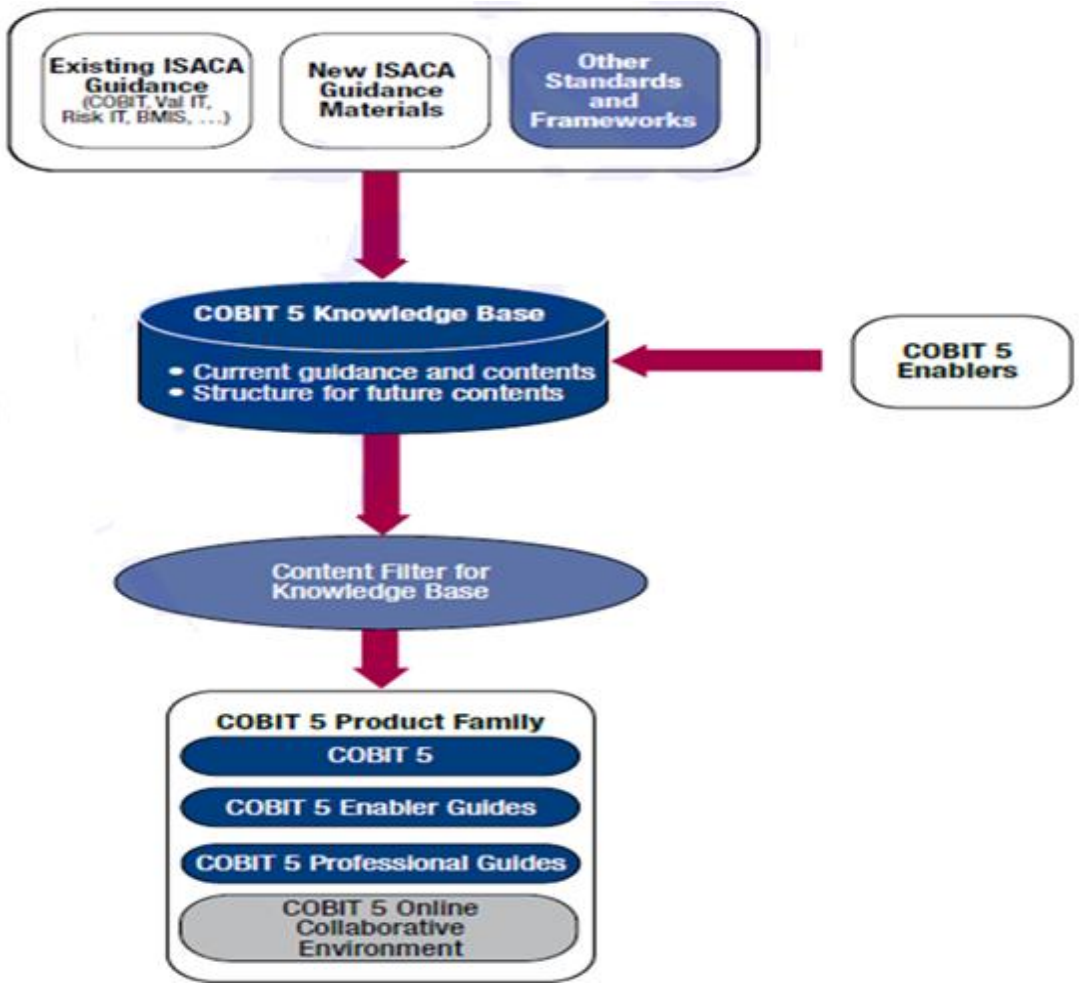


Fig: COBIT 5 Single Integrated Framework

COBIT 5 Principles Cont.

Principle 3 – Applying a Single, Integrated Framework (Continued):

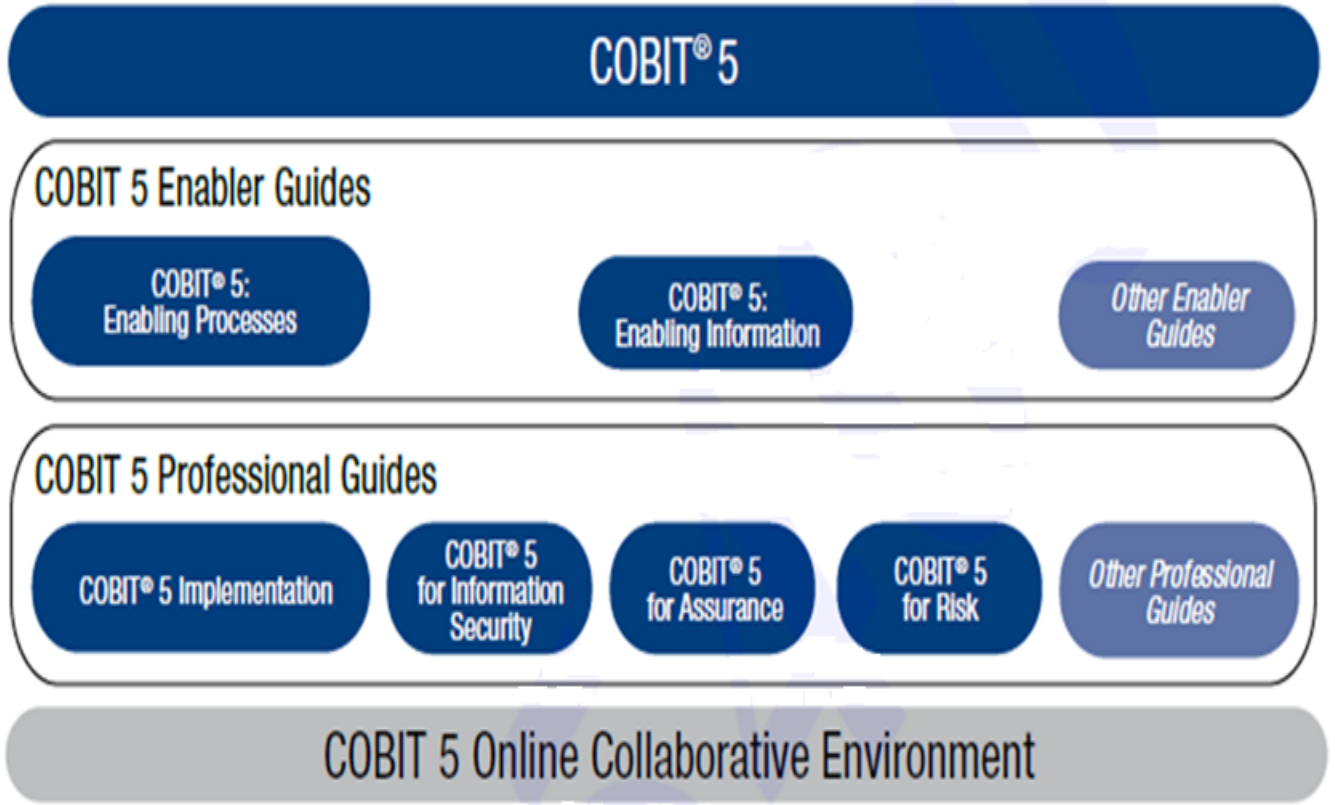


Fig: COBIT 5 Product Family

COBIT 5 Principles Cont.

Principle 4 – Enabling a Holistic Approach:

Efficient and effective governance and management of enterprise IT require a holistic approach, taking into account a number of interacting components. COBIT 5 defines a set of enablers that are broadly defined as anything that can help to achieve the objectives of the enterprise.

COBIT 5 framework defines seven categories of enablers:

- ❑ Principles, policies and frameworks
- ❑ Processes
- ❑ Organizational structures
- ❑ Culture, ethics and behavior
- ❑ Information
- ❑ Services, infrastructure and applications
- ❑ People, skills and competencies

COBIT 5 Principles Cont.

Principle 4 – Enabling a Holistic Approach (Continued):

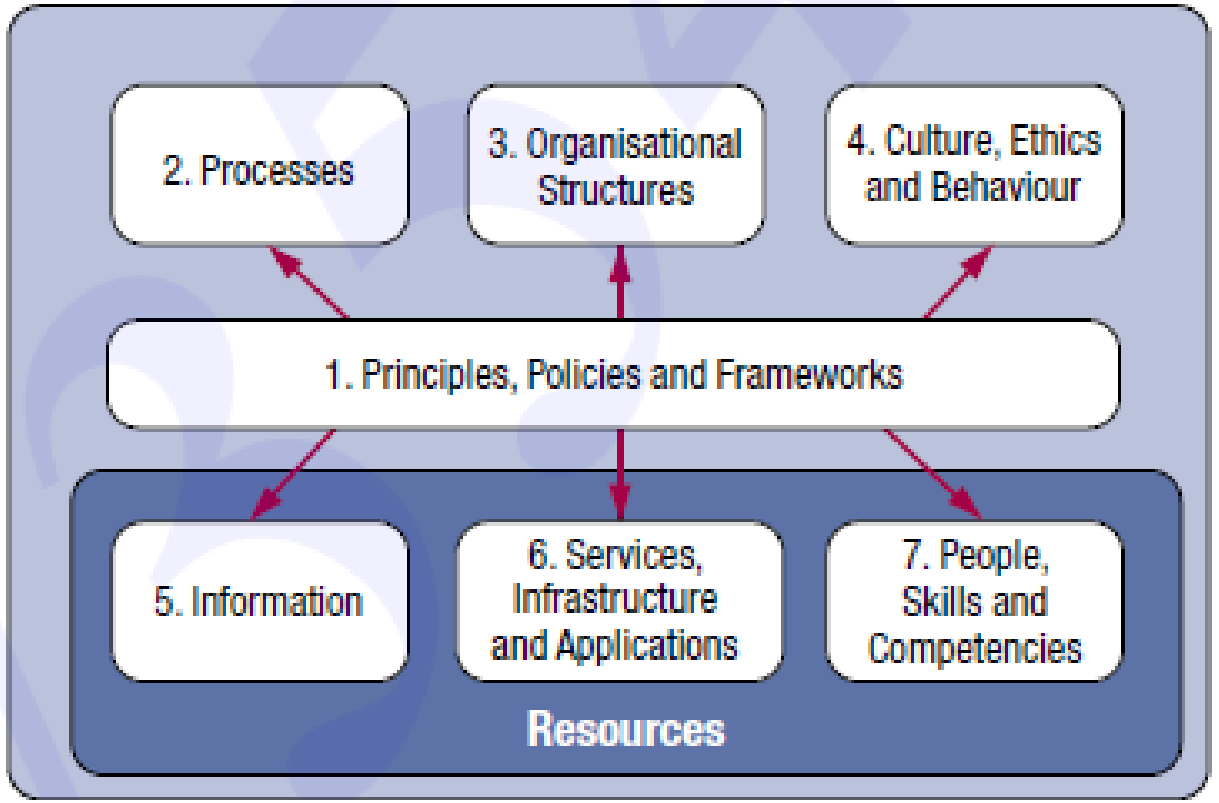


Fig: COBIT 5 Enterprise Enablers

COBIT 5 Principles Cont.

Principle 4 – Enabling a Holistic Approach (Continued)

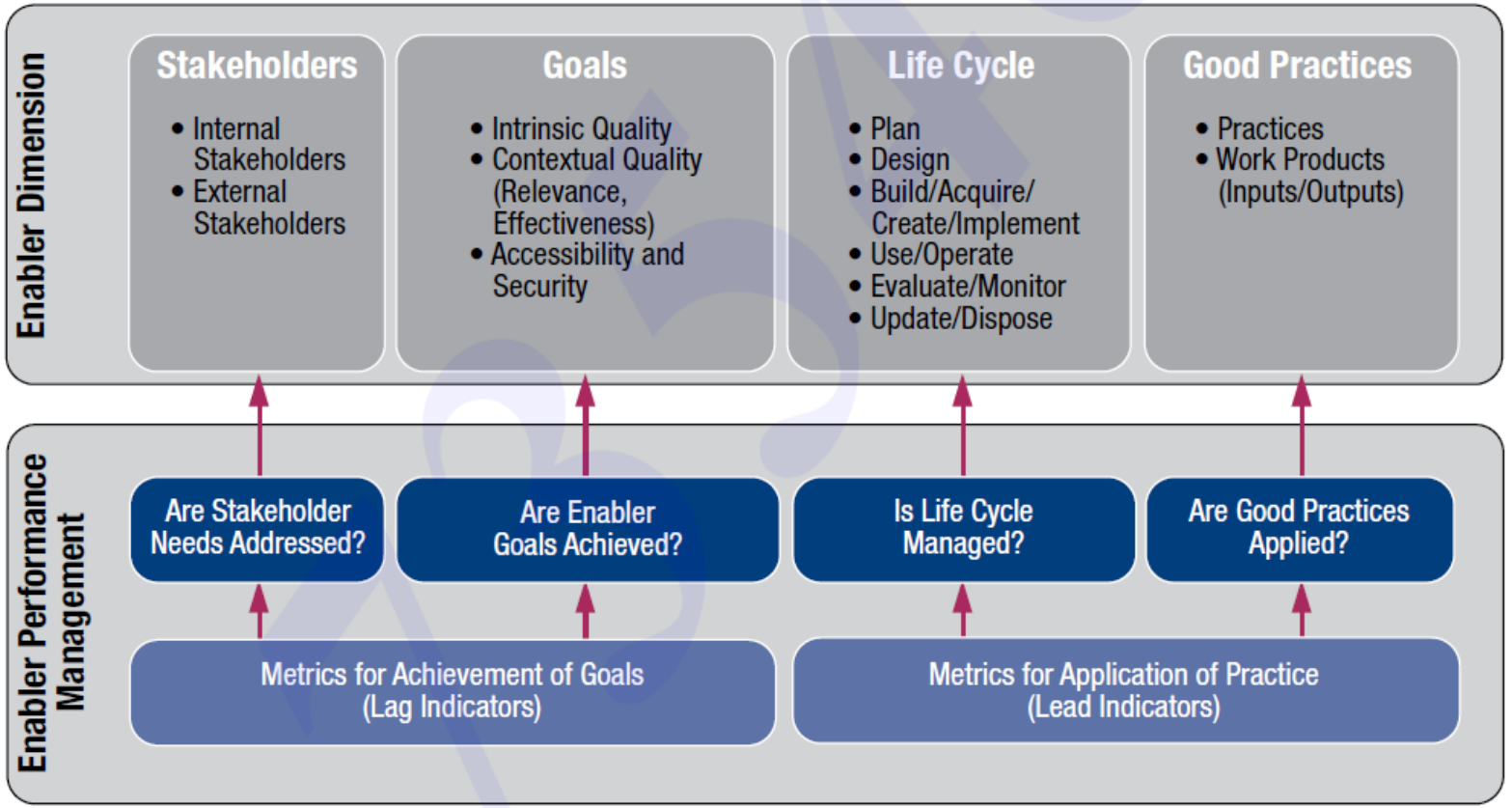


Fig: COBIT 5 Enablers – Generic

COBIT 5 Principles Cont.

Principle 4 – Enabling a Holistic Approach (Continued)

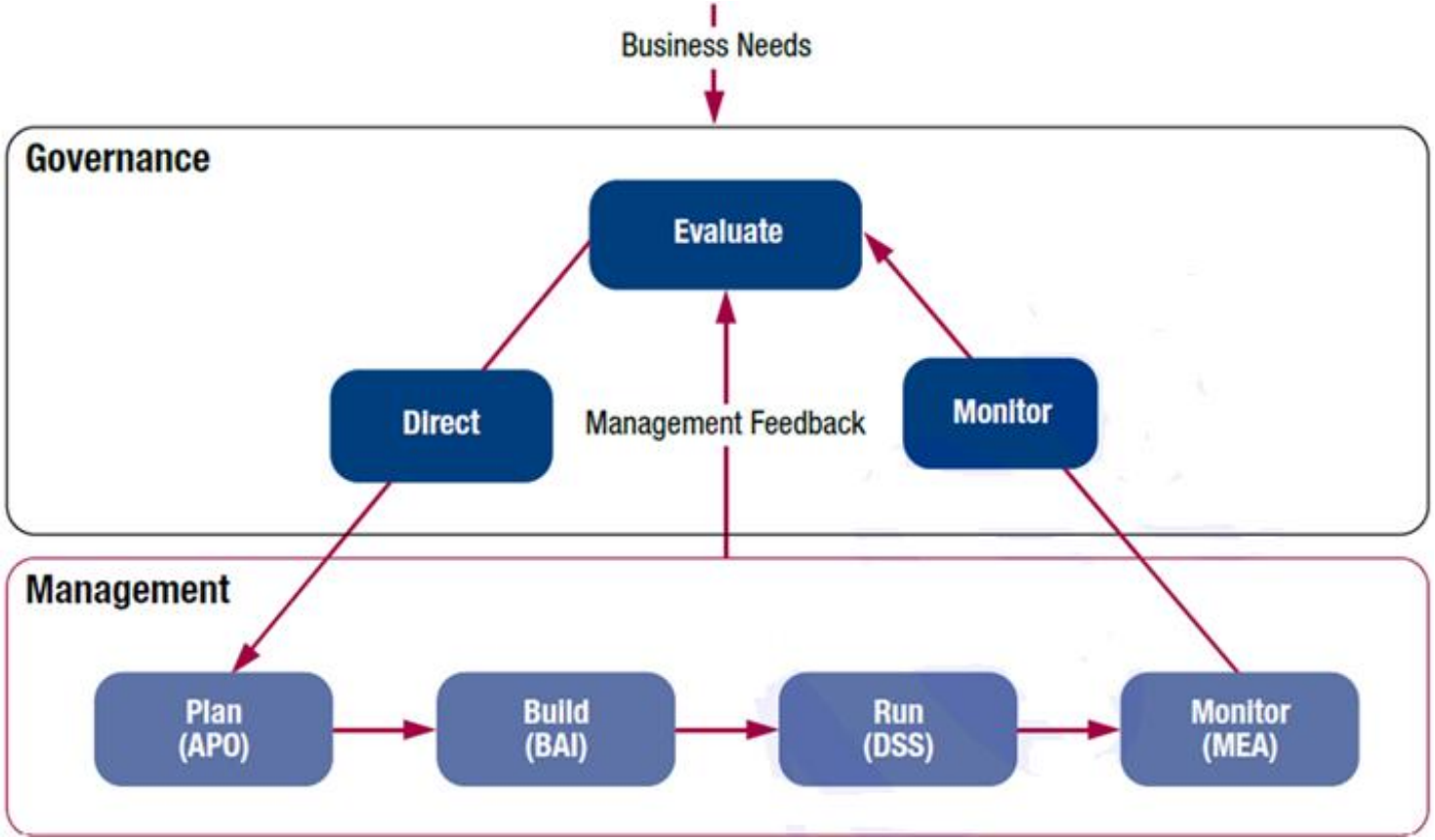


Fig: COBIT 5 Governance and Management Key Areas

COBIT 5 Principles Cont.

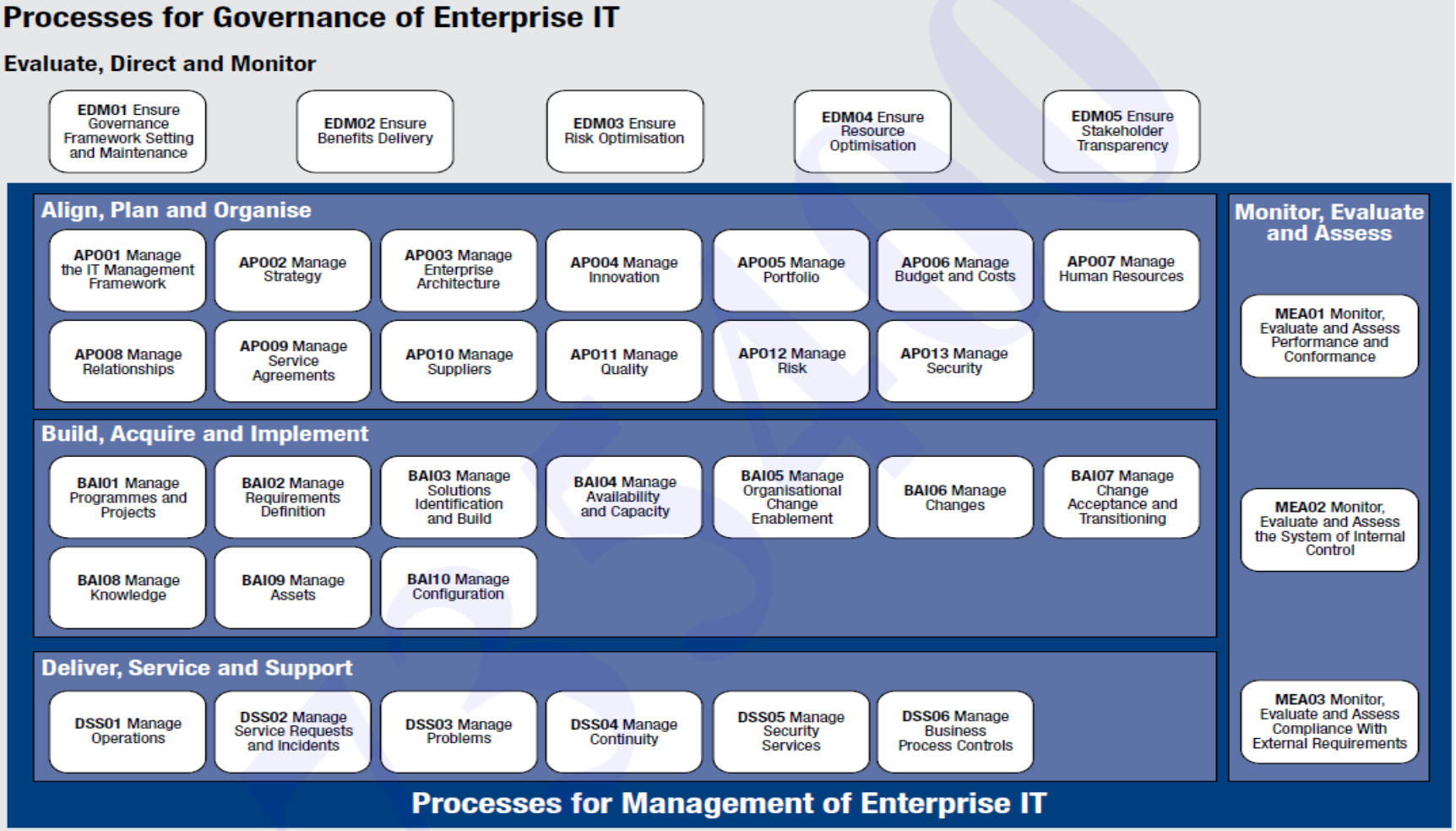
Principle 5 – Separating Governance From Management:

The COBIT 5 framework makes a clear distinction between governance and management.

- **Management** plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives. In most enterprises, this is the responsibility of the senior management under the leadership of the CEO.
- **Governance** ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives. In most enterprises, this is the responsibility of the board of directors. Specific responsibilities may be delegated to special organizational structures at an appropriate level.

COBIT 5 Principles Cont.

Principle 5 – Separating Governance From Management (Continued):



COBIT 5 Implementation

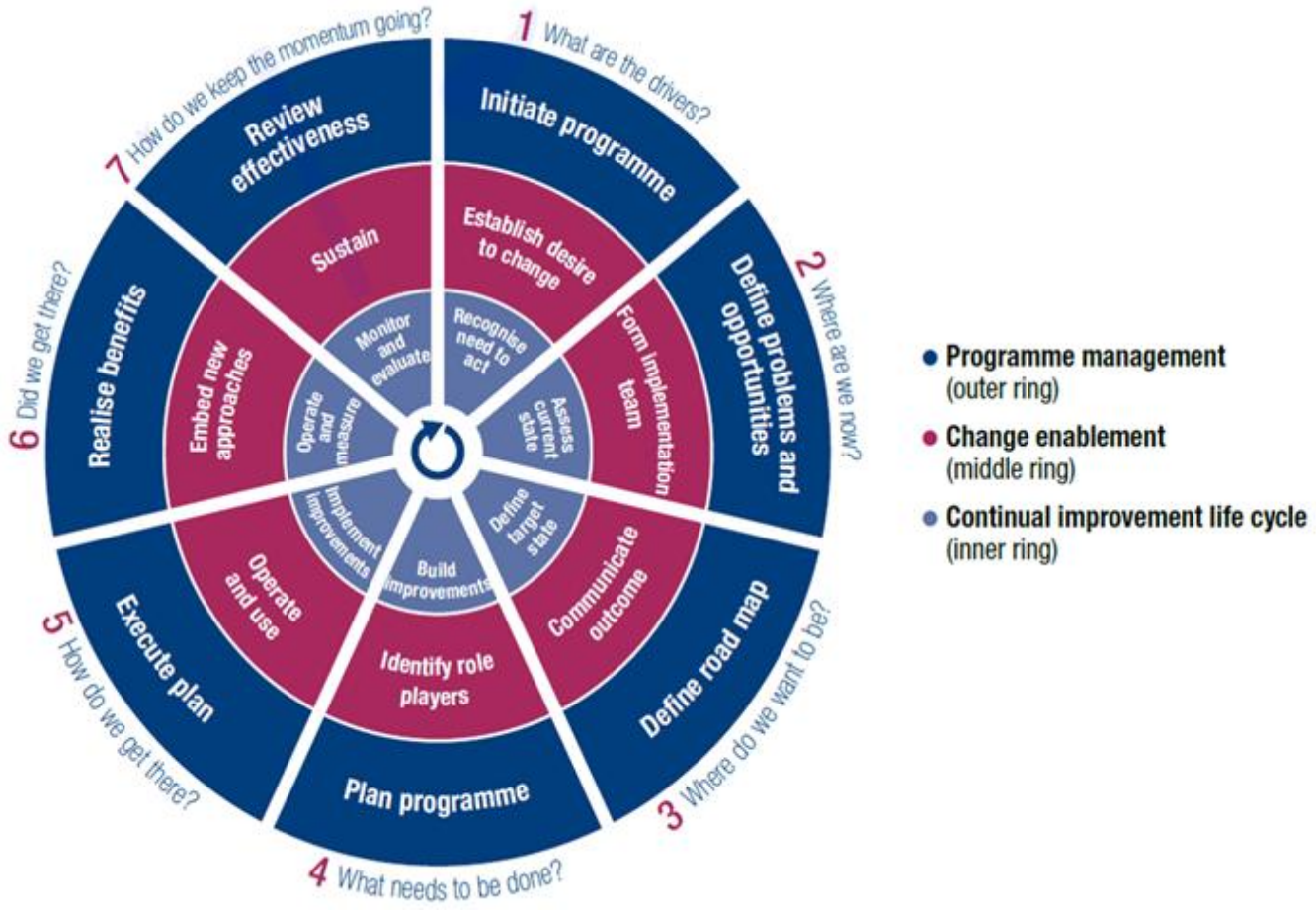


Fig: The Seven Phases of the Implementation Life Cycle

COBIT 5: Overview of the Process Assessment Model