

# Strategic Governance & Operational Security Frameworks

Dr Diarmuid Ó Briain

12 Oct 2026



## Licence



This work is licenced under a Creative Commons  
Attribution-ShareAlike 4.0 International Licence.  
Full Licence: <http://creativecommons.org/licenses/by-sa/4.0>

## Learning objectives

- At the end of this topic you will be able to:
  - Explain the fundamental purpose and core structures of ITIL, COSO, and CMMI, identifying how each aligns operational maturity and financial controls with security objectives.
  - Compare the unique strengths of various management models and explain how COBIT principles serve as an overarching umbrella to help these systems coexist without corporate redundancy.
  - Detail the structural layout of the updated NIST CSF v2.0 in close depth, explaining how its expanded core functions, categories, and sub-categories function.
  - Assess high-level framework characteristics to determine which models best align with specific regulatory compliance demands and internal board-level risk appetites.

**NIST**



**Management &  
Lifecycle Frameworks**

**COBIT**



# Management Frameworks



***A management system is the framework of processes and procedures used to ensure that an organisation can fulfil all tasks required to achieve its objectives.***



## IT Infrastructure Library (ITIL)

- IT Infrastructure Library (ITIL)
  - Managing IT Service Management and IT Asset Management.
  - Was UK OGC, now PeopleSoft.
- Seven guiding principles:
  - 1) Focus on value
  - 2) Start where you are
  - 3) Progress iteratively with feedback
  - 4) Collaborate and promote visibility
  - 5) Think and work holistically
  - 6) Keep it simple and practical
  - 7) Optimise and automate

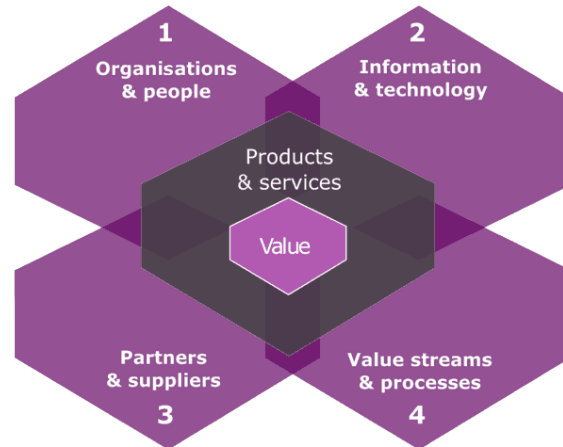


## IT Infrastructure Library (ITIL)

- The core publication scheme for ITIL 5 focuses on key Streams and Modules designed for modern, AI-enabled environments:
  - Foundation
  - Practice Manager (PM)
  - Managing Professional (MP)
  - Strategic Leader (SL)
  - ITIL Transformation
  - AI Governance



## ITIL Dimensions



INSPIRING FUTURES



setu.ie | 9

## Organisations and People

- Culture
- Roles and responsibilities
- Skills and knowledge
- Communication



setu.ie | 10

## Information and Technology

- Data and Information
- Technology Capabilities
- Applications and Infrastructure

INSPIRING FUTURES



setu.ie | 11

## Partners and Suppliers

- Relationships
- Contracts and Agreements
- Dependencies

INSPIRING FUTURES



setu.ie | 12

## Value Streams and Processes

- Value Creation
- Value Streams
- Processes



## Internal Corporate Governance & Financial Controls

**COSO ERM**

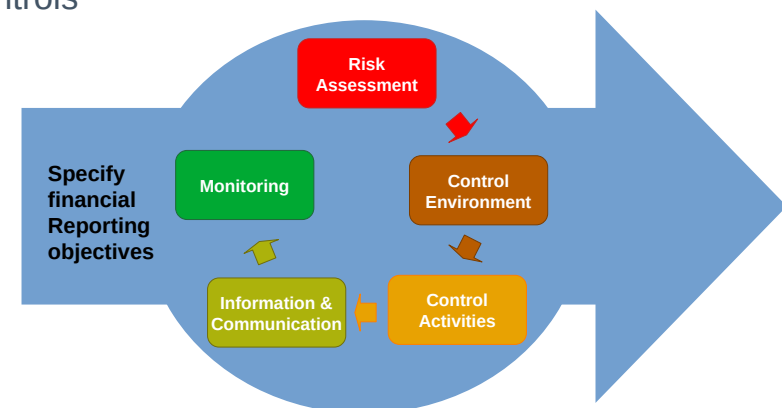
## Committee of Sponsoring Organisations (COSO)

- Treadway Commission: Committee of Sponsoring Organisations (COSO)
- Organisational governance, business ethics, internal control, ERM, fraud, and financial reporting.
  - Internal Control - Integrated Framework
  - ERM Framework
  - Complementary Frameworks.

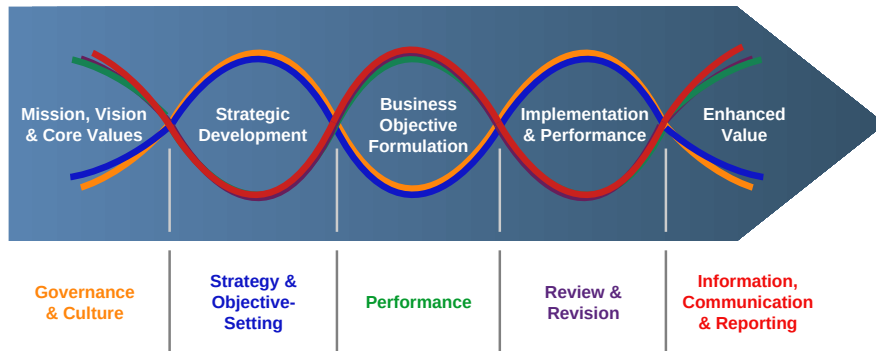


## COSO Internal Control - Integrated Framework

- Design, implement, and assess an organisation's internal controls



## COSO ERM



## COSO ERM

### • 20 Principles grouped as 5 Component Objectives:

- 1) Governance and Culture
- 2) Strategy and Objective-Setting
- 3) Performance
- 4) Review and Revision
- 5) Information, Communication and Reporting

## Key differences between COSO frameworks

| Characteristic    | ICIF                                                                                                | ERM                                                                                                                                                          |
|-------------------|-----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Focus</b>      | Internal controls                                                                                   | Risk management                                                                                                                                              |
| <b>Components</b> | Control environment, risk assessment, control activities, information and communication, monitoring | Internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, monitoring |
| <b>Purpose</b>    | To design, implement, and assess internal controls                                                  | To identify, assess, and manage risks to an organisation's objectives                                                                                        |
| <b>Scope</b>      | More focused on the internal controls that are necessary to achieve an organisation's objectives    | More focused on the overall risk management process                                                                                                          |
| <b>Best for</b>   | Organisations that are looking to improve their internal controls                                   | Organisations that are looking to improve their overall risk management practices                                                                            |



Ollscoil  
Teicneolaíochta  
an Oirdeheiscirt  
South East  
Technological  
University

# Maturity Models & Controls Objectives

## CMM

## COBIT

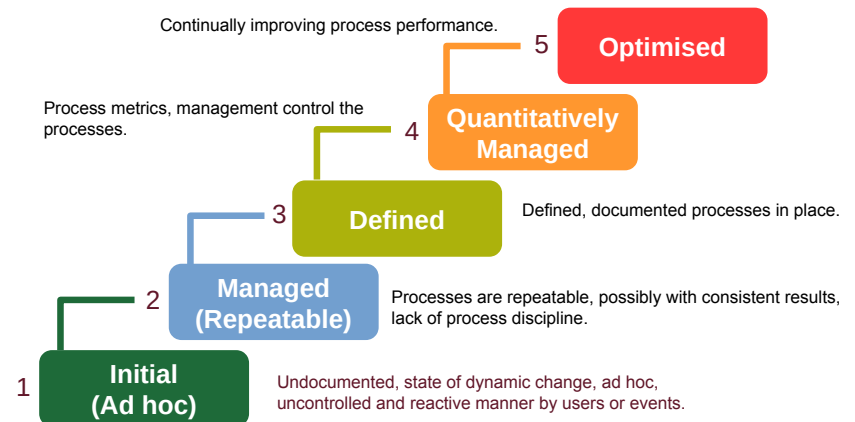
INSPIRING FUTURES

## Capability Maturity Model

- CMM is a useful general theoretical model, to aid in the definition and understanding of an organisation's process capability maturity.
- For software development, the CMM has been superseded by Capability Maturity Model Integration (CMMI).

**CMM**

## Capability Maturity Model



## Capability Maturity Model Integration

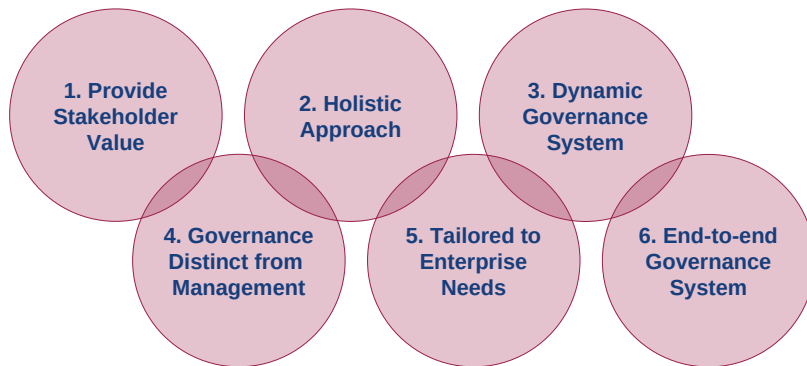
- **CMMI for Acquisition**
  - Designed for businesses that focus on working with suppliers to assemble a product or deliver a service.
- **CMMI for Development**
  - Designed for businesses that focus on developing products and services.
- **CMMI for Services**
  - Designed for businesses that focus on establishing, managing, and delivering services to customers.

SE TU  
Ollscoil Teicneolaíochta an Oirdheiscirt  
South East Technological University

**CQBIT 2019**  
**IT Governance**

setu.ie  
INSPIRING FUTURES

## COBIT<sup>®</sup> 2019 IT Governance



## COBIT<sup>®</sup> 2019 Objectives

### Governance

Evaluate, Direct and Monitor (EDM)

### Management

Align, Plan and Organise (APO)

Build, Acquire and Implement (BAI)

Deliver, Service and Support (DSS)

Monitor, Evaluate and Assess (MEA)

Ensure that the organisation's IT strategy and governance are aligned with its overall business goals. It also includes objectives related to performance and risk management.

## COBIT<sup>®</sup> 2019 Objectives

### Governance

Evaluate, Direct and Monitor (EDM)

### Management

Align, Plan and Organise (APO)

Build, Acquire and Implement (BAI)

Deliver, Service and Support (DSS)

Monitor, Evaluate and Assess (MEA)

Develop and implement an IT strategy that is aligned with the organisation's overall business goals. It also includes objectives related to resource management and project management.

## COBIT<sup>®</sup> 2019 Objectives

### Governance

Evaluate, Direct and Monitor (EDM)

### Management

Align, Plan and Organise (APO)

Build, Acquire and Implement (BAI)

Deliver, Service and Support (DSS)

Monitor, Evaluate and Assess (MEA)

Develop and implement of IT solutions. It includes objectives related to requirements management, change management, and testing.

## COBIT<sup>®</sup> 2019 Objectives

### Governance

Evaluate, Direct and Monitor (EDM)

### Management

Align, Plan and Organise (APO)

Build, Acquire and Implement (BAI)

Deliver, Service and Support (DSS)

Monitor, Evaluate and Assess (MEA)

Delivery and support of IT services. It includes objectives related to service level management, incident management, and problem management.

## COBIT<sup>®</sup> 2019 Objectives

### Governance

Evaluate, Direct and Monitor (EDM)

Align, Plan and Organise (APO)

Build, Acquire and Implement (BAI)

Deliver, Service and Support (DSS)

Monitor, Evaluate and Assess (MEA)

Monitoring and evaluating the performance of IT solutions and services. It also includes objectives related to compliance and risk management.

Performance management in COBIT 2019 is based on the CMMI Performance Management Scheme, in which the capability and maturity levels are measured between 0 and 5.

## COBIT 2019, summary

- COBIT 2019 objectives are designed to help organisations achieve the following benefits:
  - Improved alignment of IT with business goals
  - Enhanced performance and risk management
  - Increased efficiency and effectiveness of IT operations
  - Improved compliance with regulations and standards
  - Reduced costs and improved value for money.

## Implementing Multi-Framework Coexistence

- Identify the organisation's goals and objectives
- Assess the organisation's current state
- Select the right frameworks
- Prioritise the frameworks
- Align the frameworks
- Implement the frameworks
- Monitor and evaluate the frameworks



## Cybersecurity Framework (CSF)

- A Cybersecurity Framework describes essential cybersecurity outcomes that can help an organisation reduce its cybersecurity risk.
  - NIST: Cybersecurity Framework (CSF)
  - ISO/IEC 27001: Information security, cybersecurity and privacy protection
  - ISA/IEC 62443: Industrial communication networks - IT security for networks and systems.



INSPIRING FUTURES

setu.ie | 34

## Cybersecurity Framework (CSF)

The CSF is collection of cybersecurity outcomes that can be used to:

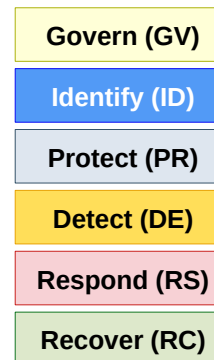
- Understand and Assess
- Prioritise
- Communicate.



INSPIRING FUTURES

setu.ie | 35

## CSF Functions



INSPIRING FUTURES

setu.ie | 36

## CSF Functions

|                      |                                                                                                           |
|----------------------|-----------------------------------------------------------------------------------------------------------|
| <b>Govern (GV)</b>   | Establish and monitor the organisation's cybersecurity risk management strategy, expectations, and policy |
| <b>Identify (ID)</b> | Help determine the current cybersecurity risk to the organisation                                         |
| <b>Protect (PR)</b>  | Use safeguards to prevent or reduce cybersecurity risk                                                    |
| <b>Detect (DE)</b>   | Find and analyse possible cybersecurity attacks and compromises                                           |
| <b>Respond (RS)</b>  | Take action regarding a detected cybersecurity incident                                                   |
| <b>Recover (RC)</b>  | Restore assets and operations that were impacted by a cybersecurity incident                              |

## Categories and Sub-categories



| Function             | Category                                                | Category ID |
|----------------------|---------------------------------------------------------|-------------|
| <b>Govern (GV)</b>   | Organisational Context                                  | GV.OC       |
|                      | Risk Management Strategy                                | GV.RM       |
|                      | Cybersecurity Supply Chain Risk Management              | GV.SC       |
|                      | Roles, Responsibilities, and Authorities                | GV.RR       |
|                      | Policies, Processes, and Procedures                     | GV.PO       |
|                      | Oversight                                               | GV.OV       |
| <b>Identify (ID)</b> | Asset Management                                        | ID.AM       |
|                      | Risk Assessment                                         | ID.RA       |
|                      | Improvement                                             | ID.IM       |
| <b>Protect (PR)</b>  | Identity Management, Authentication, and Access Control | PR.AA       |
|                      | Awareness and Training                                  | PR.AT       |
|                      | Data Security                                           | PR.DS       |
|                      | Platform Security                                       | PR.PS       |
|                      | Technology Infrastructure Resilience                    | PR.IR       |
| <b>Detect (DE)</b>   | Continuous Monitoring                                   | DE.CM       |
|                      | Adverse Event Analysis                                  | DE.AE       |
| <b>Respond (RS)</b>  | Incident Management                                     | RS.MA       |
|                      | Incident Analysis                                       | RS.AN       |
|                      | Incident Response Reporting and Communication           | RS.CO       |
|                      | Incident Mitigation                                     | RS.MI       |
| <b>Recover (RC)</b>  | Incident Recovery Plan Execution                        | RC.RP       |
|                      | Incident Recovery Communication                         | RC.CO       |

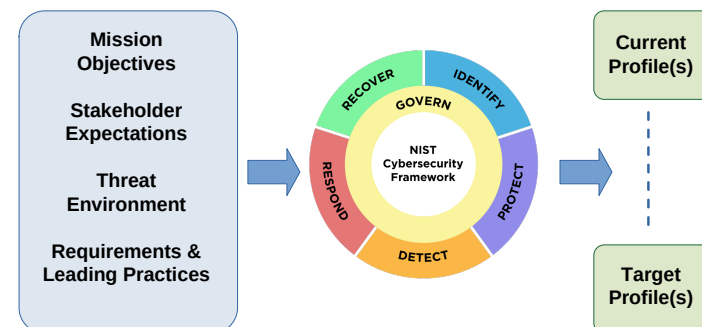
## Implementing the CSF – Handling Risk

Organisations can choose to handle risk in different ways;

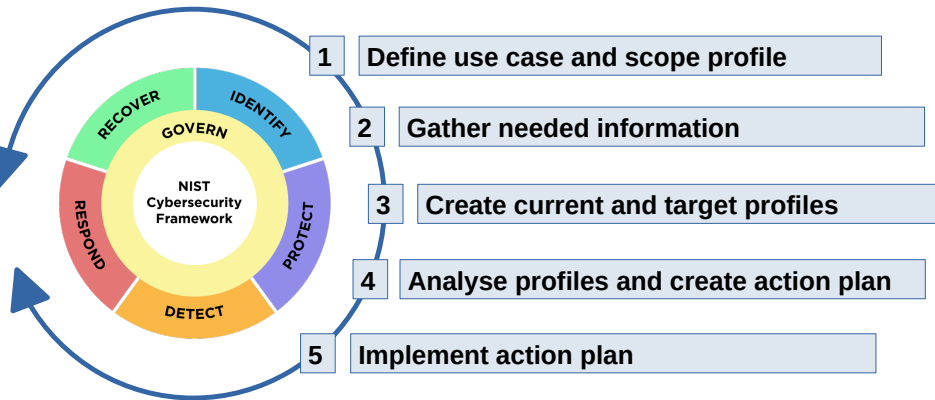
- Mitigation
- Transfer
- Avoidance
- Acceptance.

## CSF Profiles

- Understand, assess, and communicate the organisation's current or target cybersecurity posture and to prioritise outcomes.



## Create CSF Profiles



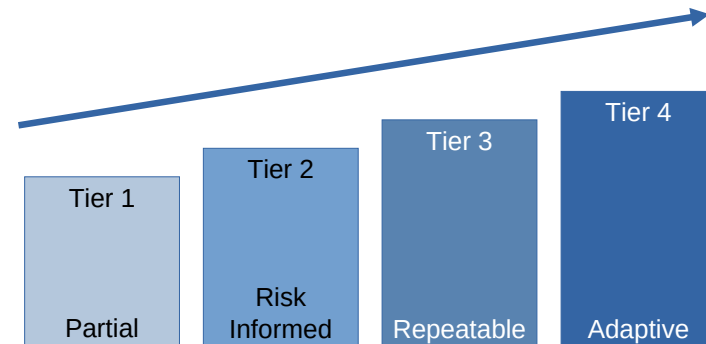
## Organisational profile template

| Selected Framework Outcomes (Functions, Categories, or Subcategories) | Current Policies, Processes, and Procedures                                  | Current Internal Practices                                                                        | Target Priority | Target Policies, Processes, and Procedures                                                                     | Target Roles and Responsibilities                                                          | Target Selected Informative References          | Notes                                                                                           |
|-----------------------------------------------------------------------|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------|----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|-------------------------------------------------|-------------------------------------------------------------------------------------------------|
| GV.AM-01: Asset management strategy is in place. (GOVERN)             | Documented Asset Management Policy and Procedure for Asset Inventory.        | Manual, quarterly spreadsheet inventory; only covers IT assets; little oversight from leadership. | High            | Implement automated Asset Discovery Tool and update policy to include all OT.                                  | CISO to own the policy; Asset Manager to oversee inventory process.                        | ISO 27001: A.8.1; CIS Control 1; COBIT GOV05.01 | Need to purchase and integrate new asset discovery software within 6 months.                    |
| ID.SC-01: System components are identified. (IDENTIFY)                | Process for system registration in Configuration Management Database (CMDB). | CMDB data is often incomplete, missing non-production servers and cloud instances.                | Medium          | Mandate automated cloud discovery agent deployment for all new deployments; Quarterly CMDB Data Quality Audit. | Cloud Operations Team to ensure agent deployment; Configuration Manager to conduct audits. | NIST SP 800-53: CM-8; ISO 27001: A.8.1.1        | Focus on improving accuracy of cloud-based assets first, then expand to container environments. |
|                                                                       |                                                                              |                                                                                                   |                 |                                                                                                                |                                                                                            |                                                 |                                                                                                 |
|                                                                       |                                                                              |                                                                                                   |                 |                                                                                                                |                                                                                            |                                                 |                                                                                                 |
|                                                                       |                                                                              |                                                                                                   |                 |                                                                                                                |                                                                                            |                                                 |                                                                                                 |

## Action Plan template

| Selected Framework Outcomes                         | Priority | Action Item                                                                                                           | Responsible Parties                    | Target Completion Date | Resources Required                                                        |
|-----------------------------------------------------|----------|-----------------------------------------------------------------------------------------------------------------------|----------------------------------------|------------------------|---------------------------------------------------------------------------|
| PR.AA-01: MFA implemented for all remote access     | High     | 1. Deploy hardware security keys to critical IT staff.<br>2. Enforce MFA policy on main identity provider (IdP).      | Security Operations, IT Infrastructure | 25 Nov                 | MFA software licenses, key hardware budget, 20 hrs staff deployment time. |
| RS.MA-01: Incident response plan updated and tested | Medium   | 1. Review incident response procedures for ransomware scenarios.<br>2. Conduct tabletop exercise with executive team. | CISO, Incident Response Team           | 15 Dec                 | External facilitator fee, 2 hrs executive time.                           |

## CSF Tiers



## Summary of the Frameworks

| Framework     | Focus                           | Scope                                                                    |
|---------------|---------------------------------|--------------------------------------------------------------------------|
| ITIL          | IT service management           | Entire lifecycle of IT services                                          |
| COSO          | Internal control                | Risk management, control, and governance                                 |
| CMM           | Capability Maturity Model       | Measuring the maturity of an organisation's software development process |
| COBIT         | IT governance and management    | Ensuring that IT delivers value to the organisation                      |
| NIST CSF 2.0  | Cybersecurity framework         | Managing and reducing cybersecurity risks to networks and data           |
| ISO/IEC 27000 | Information security management | Security of information assets                                           |

## NIST CSF2.0 and OT

### GOVERN

- Ensure Compliance
- Review applicable requirements
- Policies and procedures
- Continuous improvement strategy
- Metrics & reporting
- Audit & review

### IDENTIFY

- Determine Scope and Risk
- Asset management
- Risk assessments
- Risk management strategy
- Business alignment
- Budget planning

### PROTECT

- Implement Controls to Limit Risk
- Secure network architecture
- Vulnerability management
- Secure remote access
- Incident response tabletops
- Penetration testing



### DETECT

- Watch for Suspicious Activity
- Threat detection
- Continuous monitoring
- Event correlation
- Threat hunting
- Integrate with IT monitoring

### RESPOND

- Take Action to Limit Damage
- Response team coordination
- Incident triage
- Escalation procedures
- Coordination with key parties
- Reporting requirements

### RECOVER

- Get Back Up & Running
- Rebuild / replace systems
- Restore from backup
- Restore operations safely
- "Lessons learned"

## NIST SP 800-82

- Tailors NIST CSF 2.0 and SP 800-37 RMF to provide a risk-based security framework for OT.
- Covers diverse physical-world systems.
- Adapts NIST SP 800-53 security baselines to IT/OT convergence.
- SP 800-82r4 Draft:
  - Continuous Verification & Identity-First Access (ZTA)
  - Micro-Segmentation
  - Threat Exposure & Supply Chain Risk
  - Converged Security Operations

## Exercise



# Quiz



## The cross-cutting function of the NIST CSF v2.0 core

The NIST CSF v2.0 organises its core outcomes into several distinct functions. Which function occupies the central position of the framework wheel and serves to inform and prioritise the execution of all other functions?

- A) Identify (ID) function.
- B) Protect (PR) function.
- C) Govern (GV) function.
- D) Detect (DE) function.

## The cross-cutting function of the NIST CSF v2.0 core

The NIST CSF v2.0 organises its core outcomes into several distinct functions. Which function occupies the central position of the framework wheel and serves to inform and prioritise the execution of all other functions?

- A) Identify (ID) function.
- B) Protect (PR) function.
- C) **Govern (GV) function.** ✓
- D) Detect (DE) function.

## Dimensions of IT Service Management

When implementing the ITIL framework, organisations must consider four distinct dimensions to ensure a sustainable approach. Which of the following are one of these dimensions?

- A) Value streams and processes.
- B) Strategic financial reporting.
- C) Information and technology.
- D) Partners and suppliers.

## Dimensions of IT Service Management

When implementing the ITIL framework, organisations must consider four distinct dimensions to ensure a sustainable approach. Which of the following are one of these dimensions?

- A) **Value streams and processes.** ✓
- B) Strategic financial reporting.
- C) **Information and technology.** ✓
- D) **Partners and suppliers.** ✓

## Categorisation of COBIT objective domains

COBIT 2019 defines 40 governance and management objectives partitioned into five distinct domains. If an organisation is primarily focused on developing and implementing an IT strategy that manages resources and projects, which domain is it operating within?

- A) Evaluate, Direct and Monitor (EDM).
- B) Align, Plan and Organise (APO).
- C) Build, Acquire and Implement (BAI).
- D) Deliver, Service and Support (DSS).

## Categorisation of COBIT objective domains

COBIT 2019 defines 40 governance and management objectives partitioned into five distinct domains. If an organisation is primarily focused on developing and implementing an IT strategy that manages resources and projects, which domain is it operating within?

- A) Evaluate, Direct and Monitor (EDM).
- B) **Align, Plan and Organise (APO).** ✓
- C) Build, Acquire and Implement (BAI).
- D) Deliver, Service and Support (DSS).

## Structural differences between COSO ICIF and ERM

COSO provides two key complementary frameworks for enterprise oversight. What is a primary distinguishing characteristic between the ICIF and the ERMF?

- A) The ICIF outlines a framework focused on internal controls, whereas the ERMF outlines a framework for software development maturity.
- B) The ICIF manages technical service value streams, whereas the ERMF establishes explicit guidelines for third-party vendor acquisition.
- C) The ICIF focuses specifically on internal controls, whereas the ERMF focuses on the overarching enterprise risk management process.
- D) The ICIF defines specific capability maturity levels, whereas the ERMF regulates the physical safety requirements of infrastructure.

## Structural differences between COSO ICIF and ERM

COSO provides two key complementary frameworks for enterprise oversight. What is a primary distinguishing characteristic between the ICIF and the ERMF?

- A) The ICIF outlines a framework focused on internal controls, whereas the ERMF outlines a framework for software development maturity.
- B) The ICIF manages technical service value streams, whereas the ERMF establishes explicit guidelines for third-party vendor acquisition.
- C) **The ICIF focuses specifically on internal controls, whereas the ERMF focuses on the overarching enterprise risk management process.** ✓
- D) The ICIF defines specific capability maturity levels, whereas the ERMF regulates the physical safety requirements of infrastructure.

## Characteristics of NIST CSF Tier 3

The NIST CSF v2.0 utilises Tiers to characterise an organisation's risk management practices. Which description accurately depicts the operational environment of an organisation that has successfully achieved Tier 3 (Repeatable)?

- A) Practices are driven in an ad-hoc, uncontrolled, and reactive manner by users or events in a highly unstable environment.
- B) Practices are approved by management but are not yet formally established as a comprehensive organisation-wide policy document. (50%)
- C) Practices are monitored by senior executives in the exact same context as financial risks using a unified enterprise approach.
- D) Practices are formally approved and expressed as policy, with risk-informed processes defined, implemented, and regularly updated.

## Characteristics of NIST CSF Tier 3

The NIST CSF v2.0 utilises Tiers to characterise an organisation's risk management practices. Which description accurately depicts the operational environment of an organisation that has successfully achieved Tier 3 (Repeatable)?

- A) Practices are driven in an ad-hoc, uncontrolled, and reactive manner by users or events in a highly unstable environment.
- B) Practices are approved by management but are not yet formally established as a comprehensive organisation-wide policy document. (50%)
- C) Practices are monitored by senior executives in the exact same context as financial risks using a unified enterprise approach.
- D) **Practices are formally approved and expressed as policy, with risk-informed processes defined, implemented, and regularly updated. ✓**

## Learning Outcomes



## Learning outcomes

You should now be able to:

- Explain the fundamental purpose and core structures of ITIL, COSO, and CMMI, identifying how each aligns operational maturity and financial controls with security objectives. ✓
- Compare the unique strengths of various management models and explain how COBIT principles serve as an overarching umbrella to help these systems coexist without corporate redundancy. ✓
- Detail the structural layout of the updated NIST CSF v2.0 in close depth, explaining how its expanded core functions, categories, and sub-categories function. ✓
- Assess high-level framework characteristics to determine which models best align with specific regulatory compliance demands and internal board-level risk appetites. ✓



Ollscoil  
Teicneolaíochta  
an Oirdheiscirt  
South East  
Technological  
University



EUR ING Dr Diarmuid Ó Briain  
Innealtóir Cairte agus Léachtóir Sinsearach

☎ +353 59 917 5000 | ✉ [diarmuid.obriain@setu.ie](mailto:diarmuid.obriain@setu.ie) | [setu.ie](http://setu.ie)  
Campas Bhóthar Chill Chainnigh, Ceatharlach, R93 V960, Éire



Ollscoil  
Teicneolaíochta  
an Oirdheiscirt  
South East  
Technological  
University

# Thank you

engcore  
advancing technology

INSPIRING FUTURES