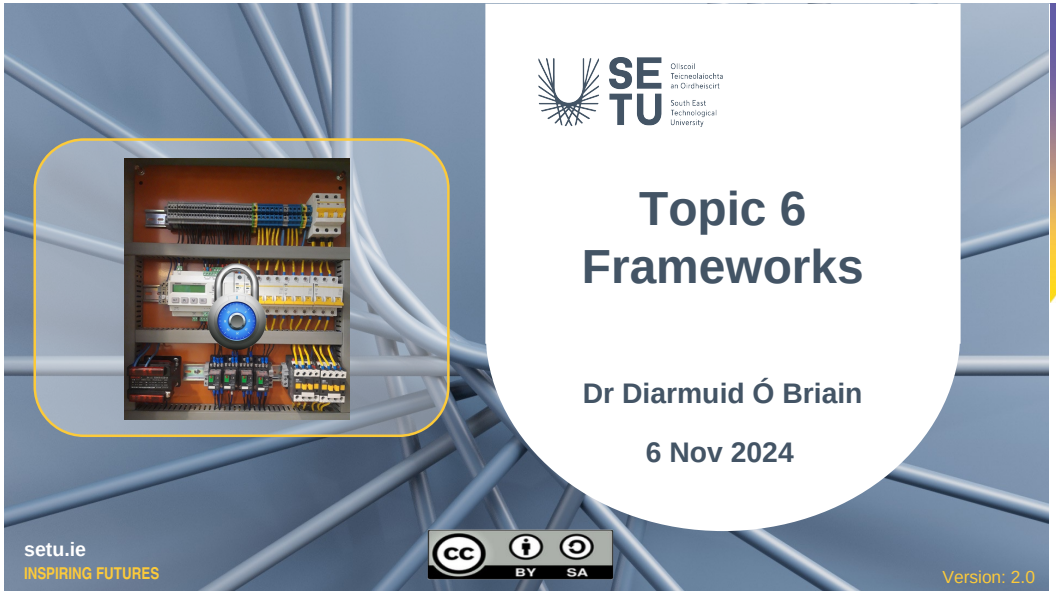


Topic 6 Frameworks

Dr Diarmuid Ó Briain

6 Nov 2024

setu.ie
INSPIRING FUTURES

Version: 2.0

Licence

Learning objectives

- By the end of this topic, you will be able to:
  - Define the framework and explain its purpose.
  - Describe the key components of the framework.
  - Explain how the framework can be used to improve IT security.
  - Identify the benefits of using the framework.
  - Discuss the challenges of implementing the framework.

NIST

ISO 27000

ITIL

COBIT

OGC

Management Frameworks

setu.ie
INSPIRING FUTURES

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.

ISO/IEC 27000

- Information Security Management System (ISMS):
  - ISO/IEC 27000-series

Standard	Function
ISO/IEC 27001	Information Security Management Systems
ISO/IEC 27002	Information Security Controls
ISO/IEC 27003	ISMS implementation guidance
ISO/IEC 27004	Monitoring, measurement, analysis and evaluation
ISO/IEC 27005	Guidance on managing information security risks
ISO/IEC 27006	Requirements for bodies providing audit and certification of ISMS

- This is an evolving list with new 27000 series standards being added to take account of changing needs, for example 27017 covers Information security management for cloud systems.

ISO/IEC 27001 – Management Requirement

- Systematic examination of the organisation's information security risks, taking account of the threats, vulnerabilities and impacts.

  Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that it deems unacceptable.

  Adopt an overarching management process to ensure that the information security controls continue to meet the organisation's information security needs on an ongoing basis.

Control Points in ISO27001:2022

- *A CP, in ISO/IEC 27001, is a specific activity or measure that can be implemented to mitigate a security risk. Control points can be technical, organisational, or procedural. They can be implemented at the individual, departmental, or organisational level.*
- CPs are grouped into four themes:
  - People
  - Organisational
  - Technological
  - Physical

Control Points examples

Technical	• Firewalls • Intrusion detection systems • Data encryption • Password management
Organisational	• Information security policies and procedures • Training for employees • Incident response plan • Risk Assessment • Access Control • Data Security • Business Continuity
Change Management	• Offsite backup • Asset management

Key characteristics of a CP

- It should be relevant to the specific risk that it is intended to mitigate
- It should be measurable, so that the organisation can assess its effectiveness
- It should be affordable and achievable for the organisation
- It should be integrated with other controls in the organisation's ISMS

Implementation stages for ISMS

- Planning
- Implementation
- Operation
- Improvement

Systematic approach to implementation of ISMS

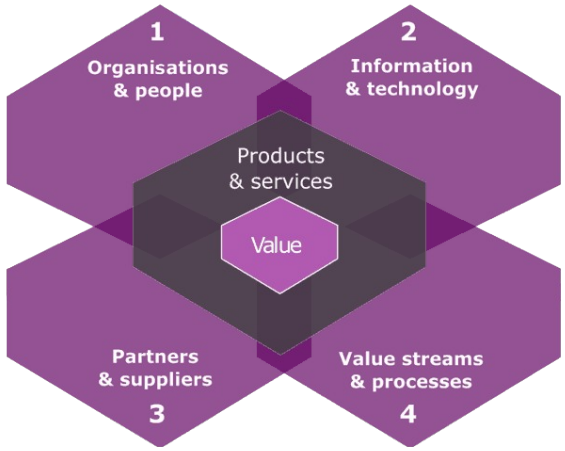
- Get top management commitment and support.
- Involve all stakeholders in the implementation process.
- Use a risk-based approach to identify and mitigate risks.
- Choose the right tools and technologies to support the ISMS.
- Monitor and review the ISMS on an ongoing basis.
- Make continuous improvement a part of the ISMS.

setu.ie
INSPIRING FUTURES

IT Infrastructure Library (ITIL)

- IT Infrastructure Library (ITIL)
  - Managing IT Service Management and IT Asset Management.
  - UK Office of Government Commerce (OGC).
- Five guiding principles:
  1) Focus on value
  2) Create a service value system
  3) Work together
  4) Be open
  5) Be continual

ITIL Dimensions



Organisations and People

- **Culture**: The culture of the organisation, which includes its values, beliefs, and norms.
- **Roles and responsibilities**: The roles and responsibilities of the people who work in the organisation, including those who are responsible for IT service management.
- **Skills and knowledge**: The skills and knowledge that are needed to deliver IT services effectively.
- **Communication**: The way that people communicate with each other, both within the organisation and with customers and stakeholders.

Information and Technology

- **Data**: The data that is used to deliver IT services, including its quality, accuracy, and security.
- **Technology**: The technology that is used to deliver IT services, including its capabilities, limitations, and risks.
- **Applications**: The applications that are used to deliver IT services, including their functionality, usability, and security.

Partners and Suppliers

- **Relationships**: The relationships that organisations have with their partners and suppliers, including their trust, communication, and collaboration.
- **Contracts**: The contracts that organisations have with their partners and suppliers, including their terms and conditions.
- **Dependencies**: The dependencies that organisations have on their partners and suppliers, including their criticality and risk.

Value Streams and Processes

- **Value**: The value that is created for customers and stakeholders, including its perceived benefits and costs.
- **Requirements**: The requirements of customers and stakeholders, including their needs, expectations, and priorities.
- **Processes**: The processes that are used to create and deliver value, including their efficiency, effectiveness, and alignment with the organisation's goals.

SETU Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

COSO

ERM

setu.ie
INSPIRING FUTURES

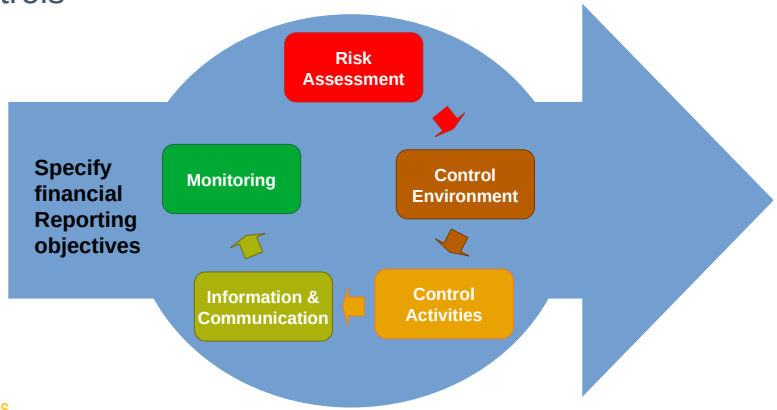
Committee of Sponsoring Organisations (COSO)

- 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.

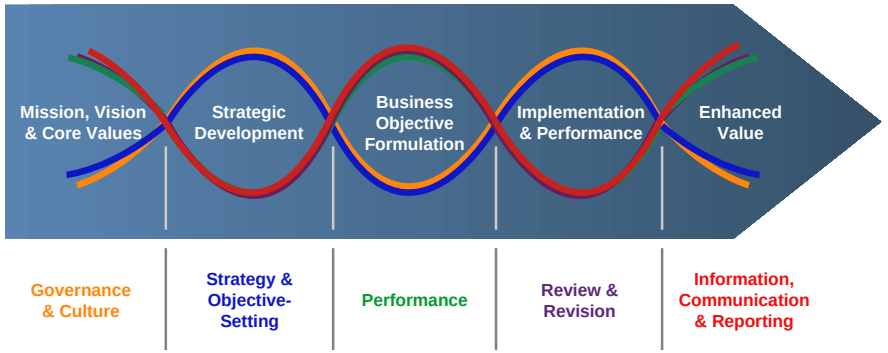
COSO

COSO Internal Control - Integrated Framework

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



COSO ERM



COSO ERM

- **Governance and Culture**
  - 1: Exercises Board Risk Oversight
  - 2: Establishes Operating Structures
  - 3: Defines Desired Organisational Behaviours
  - 4: Demonstrates Commitment to Core Values
  - 5 : Attracts, Develops & Retains Capable Individuals
- **Strategy and Objective-Setting**
  - 6: Analyses Business Context
  - 7: Defines Risk Appetite
  - 8: Evaluates Alternative Strategies
  - 9: Formulates Business Objectives
- **Performance**
  - 10: Identifies Risk
  - 11: Assesses Severity of Risk
  - 12: Prioritises Risk
  - 13: Implements Risk Responses
  - 14: Develops Portfolio View
- **Review and Revision**
  - 15: Assesses Substantial Change
  - 16: Reviews Risk & Performance
  - 17: Pursues Improvement in ERM
- **Information, Communication and Reporting**
  - 18: Leverages Information & Technology
  - 19: Communicates Risk Information
  - 20: Reports on Risk, Culture & Performance

Key differences between COSO frameworks

Characteristic	ICIF	ERM
Focus	Internal controls	Risk management
Components	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
Purpose	To design, implement, and assess internal controls	To identify, assess, and manage risks to an organisation's objectives
Scope	More focused on the internal controls that are necessary to achieve an organisation's objectives	More focused on the overall risk management process
Best for	Organisations that are looking to improve their internal controls	Organisations that are looking to improve their overall risk management practices

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

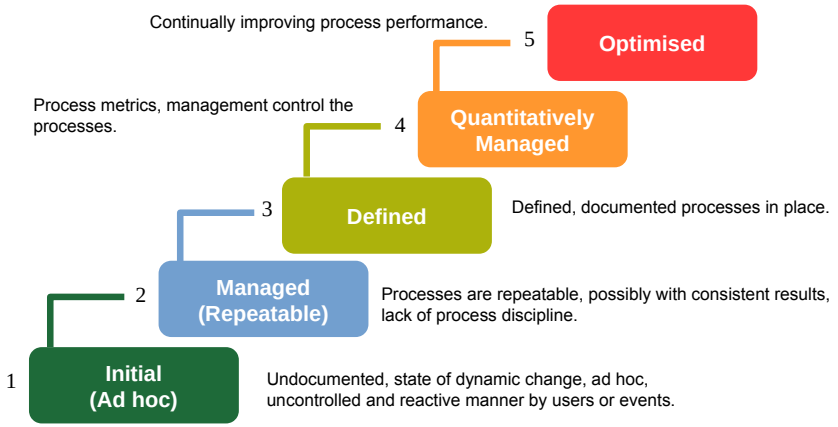
CMM
Capability Maturity Model

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

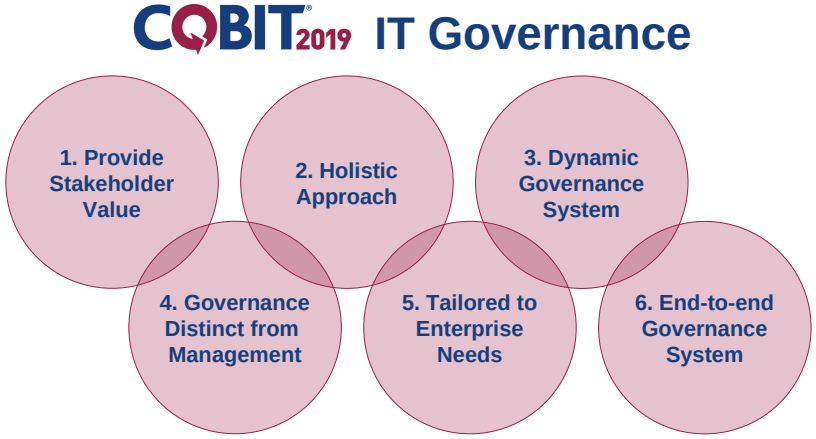
- **CMMI for Acquisition**
  - Designed for businesses that focus on working with suppliers to assemble a product or deliver a service.
- **CMMI for Development**
  - Designed for businesses that focus on developing products and services.
- **CMMI for Services**
  - Designed for businesses that focus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

SETU Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

COBIT 2019 IT Governance

setu.ie
INSPIRING FUTURES

COBIT 2019



COBIT 2019 Objectives

Governance

Management

- 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**)

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 2019 Objectives

Governance

Management

- 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**)

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 2019 Objectives

Governance

Management

- 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**)

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

COBIT 2019 Objectives

Governance

Management

- 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**)

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

COBIT 2019

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 multiple Frameworks

setu.ie
INSPIRING FUTURES

Implementing Multiple Frameworks

- Organisations can implement multiple frameworks, such as ISO27000, ITIL, COSO and COBIT, but it is important to do so in a way that is coordinated and efficient.
- Here are some pointers for implementing multiple frameworks:
  - 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.

Examples

- **Financial Institutions**
  - Banks are required to comply with a number of regulations, including the PCI DSS, which is based on ISO27001.
  - Banks also use ITIL to manage their IT services and COSO to manage their overall risk.
- **Healthcare organisations**
  - Required to comply with a number of regulations, including the GDPR
  - Healthcare organisations also use ITIL to manage their IT services and COSO to manage their overall risk.
- **Government agencies**
  - Required to comply with a number of regulations, such as EU Cybersecurity Act
  - Also use ITIL to manage their IT services and COSO to manage their overall risk.

Examples

- **Critical infrastructure organisations**
  - Organisations such as power plants and telecommunications providers, are required to comply the Network Information Systems (NIS) directives
  - Critical infrastructure organisations also use ITIL to manage their IT services and COSO to manage their overall risk.
- **Technology companies**
  - Such organisations use ISO27001 to protect their data and ITIL to manage their IT services.
  - They may also use COSO to manage their overall risk, especially if they are publicly traded companies.

Ollscoil Teicneolaíochta an Oirdheisceart
South East Technological University

NIST

Cybersecurity Framework (CSF)

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.

NIST

Cybersecurity Framework (CSF)

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

- Understand and Assess
- Prioritise
- Communicate.

CSF Functions

- Govern (GV)
- Identify (ID)
- Protect (PR)
- Detect (DE)
- Respond (RS)
- Recover (RC)

CSF Functions

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

Categories and Sub-categories

Function	Category	Category ID
Govern (GV)	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
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	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
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

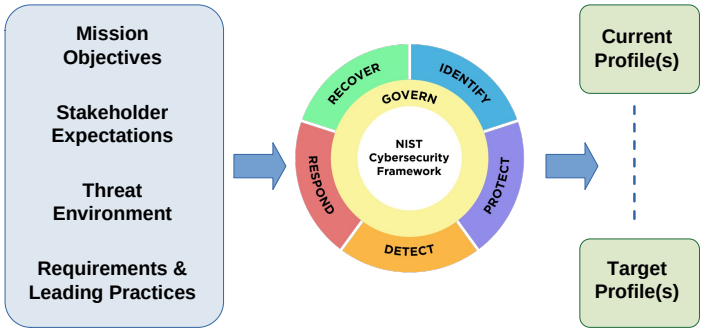
Implementing the CSF – Handling Risk

Organisations can choose to handle risk in different ways;

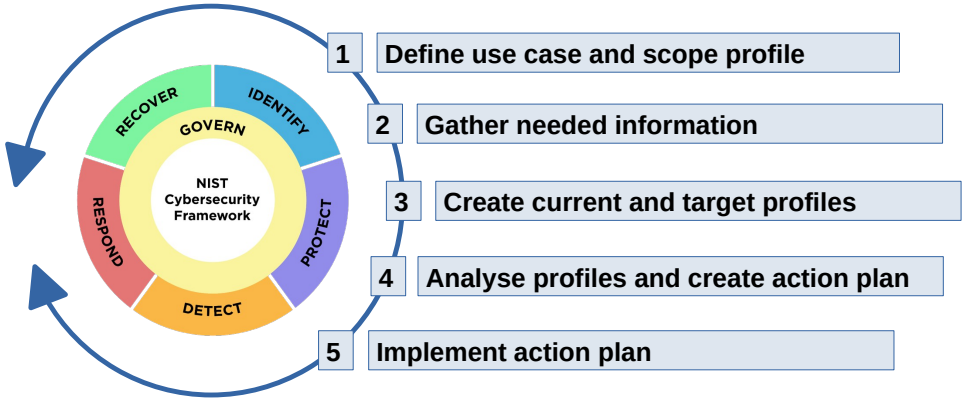
- Mitigation
- Transfer
- Avoidance
- Acceptance.

CSF Profiles

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



Create CSF Profiles



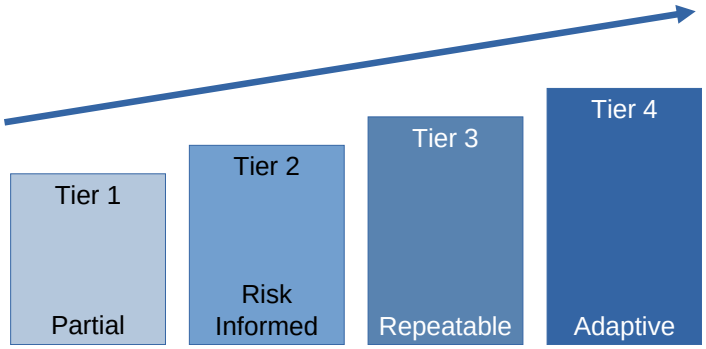
Organisational profile template

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

Action Plan template

Selected Framework Outcomes	Priority	Action Item	Responsible Parties	Target Completion Date	Resources Required

CSF Tiers



Summary of the Frameworks

Framework	Focus	Scope
ISO27000	Information security management	Security of information assets
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	Cybersecurity framework	Managing and reducing cybersecurity risks to networks and data

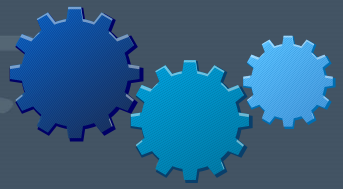
Learning objectives

You should now be able to:

- Analyse the need for frameworks in Information Technology (IT) and cybersecurity ✓
- Describe the key components of typical IT frameworks ✓
- Evaluate the NIST Cybersecurity Framework 2.0 (CSF) ✓
- Create a profile to assess, prioritise, and communicate cybersecurity efforts ✓
- Synthesise a plan to identify and mitigate cybersecurity risks ✓

Exercise #5

Scenario



TUS
Ollscoil Teicneolaíochta na Sionainne: Lár Tíre, An Iarthar Láir
Technological University of the Shannon: Midlands Midwest

EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir Sinsearach

E diarmuid.obriain@tus.ie | W tus.ie
Campas Maoilis, Páirc Maoilis,
Luimneach, V94 EC5T, Éire

CEng, FIEI
CISSP®

Thank you

TUS