Topic 6

Frameworks

Dr Diarmuid Ó Briain

Version: 1.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Copyright © 2023 C²S Consulting

Licenced under the EUPL, Version 1.2 or – as soon they will be approved by the European Commission - subsequent versions of the EUPL (the "Licence");

You may not use this work except in compliance with the Licence.

You may obtain a copy of the Licence at:

https://joinup.ec.europa.eu/sites/default/files/custom-page/attachment/eupl_v1.2_en.pdf

Unless required by applicable law or agreed to in writing, software distributed under the Licence is distributed on an "AS IS" basis, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the Licence for the specific language governing permissions and limitations under the Licence.

Dr Diarmuid Ó Briain

Table of Contents

Illustration Index

1 Objectives

By the end of this topic, you will 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.

2 Introduction

As a Cyber Security Professional it is essential that you can critically examine the purpose of frameworks in cybersecurity and the benefits they can provide. You should be able to identify the different types of frameworks available, their strengths and weaknesses, and how they can be used to improve an organisation's cybersecurity posture.

Additionally, in this topic you will learn to evaluate the NIST Cybersecurity Framework 2.0 (CSF) via a critically assessment of the CSF and its effectiveness in reducing cybersecurity risk. You will create a profile to assess, prioritise, and communicate cybersecurity efforts through synthesis of information from the CSF and other sources to create a profile of an organisation's cybersecurity posture. The profile should identify the organisation's risks, its current controls, and its plans for improvement.

From this information you will learn to synthesise a plan to identify and mitigate cybersecurity risks by using knowledge of the CSF and other sources to develop a plan to identify and mitigate cybersecurity risks. The plan should be Specific, Measurable, Achievable, Relevant, and Time-bound (SMART).

3 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.

4 ISO/IEC 27001 Information Security Management System

The ISO/IEC 27000-series, the Information Security Management System (ISMS) Family of Standards (ISO/IEC 27000) comprises information security standards published jointly by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) [1].

The series provides best practice recommendations on information security management, risks and controls within the context of an overall ISMS.

This series consists of six main standards and in excess of 40 documents overall offering standards and guidelines for the implementation, maintenance and auditing of ISMS.

- 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

4.1 ISO/IEC 27001 IT Security techniques ISMS requirements

ISO/IEC 27001 formally specifies an ISMS that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. Organisations that claim to have adopted ISO/IEC 27001 can therefore be formally audited and certified compliant with the standard. ISO/IEC 27001 requires that management:

- Systematically examine the organisation's information security risks, taking account of the threats, vulnerabilities and impacts,
- Designs and implements 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,
- Adopts an overarching management process to ensure that the information security controls continue to meet the organisation's information security needs on an ongoing basis.

4.1.1 Controls points (CP)

The CPs are grouped into four themes:

- **People**: controls focus on the people who work for the organisation, and how they can be a source of security risk or protection.
- **Organisational**: controls focus on the organisation's structure, processes, and procedures, and how they can be used to protect information assets.
- **Technological**: controls focus on the organisation's technology, and how it can be used to protect information assets.
- **Physical**: controls focus on the physical security of the organisation's premises and assets, and how they can be used to protect information assets.

While CPs are not mandatory within ISO27001:2022, but they are considered to be best practices for information security. Organisations can choose to implement the controls that are most appropriate for their needs and risk profile.

These CPs are a comprehensive set of security measures that organisations can implement to protect their information assets. By implementing these controls, organisations can reduce their risk of a security incident and protect their business-critical information.

Figure 1 lists some of the more common CPs from ISO 27001:2022.

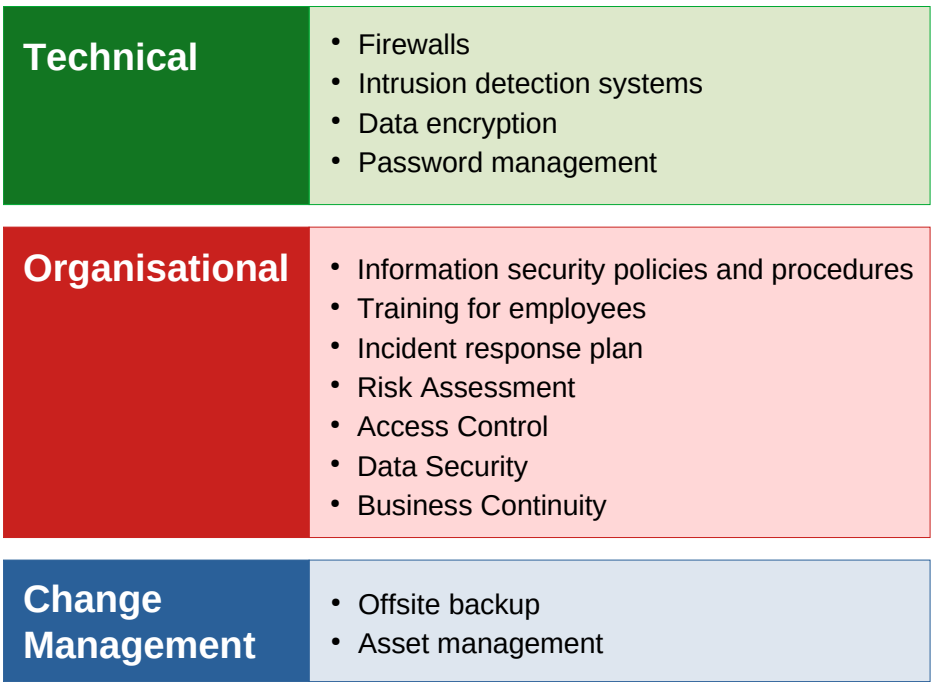

Figure 1: Example Control Points

Considering the key CPs from Figure 1:

- **Technical CPs**
  - **Firewalls:** are a network security devices that monitors and controls incoming and outgoing network traffic. It can be used to block unauthorised access to an organisation's network.
  - **Intrusion Detection Systems (IDS):** are devices or software applications that monitors a network or system for malicious activity. It can be used to detect unauthorised access, malware, and other threats.
  - **Data encryption:** is the process of converting data into a form that cannot be read without a special key. It can be used to protect data from unauthorised access, use, or disclosure.
  - **Password management:** is the process of creating, storing, and managing passwords securely. It can be used to protect access to information assets, such as accounts, files, and applications.

- **Organisational CPs**
  - **Information security policies and procedures:** Information security policies and procedures are documents that define the organisation's security requirements and how they will be met. They can be used to guide employees in their security practices and to help the organisation comply with regulations.
  - **Training for employees:** Training for employees is essential for ensuring that they are aware of the organisation's security policies and procedures and how to follow them. It can also help employees to identify and report security threats.
  - **Incident response plan:** An incident response plan is a document that describes how the organisation will respond to a security incident. It should include steps for identifying, containing, and recovering from an incident.
  - **Risk assessment:** A risk assessment is a process for identifying and assessing the risks to an organisation's information assets. It can be used to identify the most critical assets and the threats that they face.
  - **Access control:** Access control is the process of controlling who has access to information assets. It can be used to restrict access to sensitive information to authorised users only.
  - **Data security:** Data security is the protection of data from unauthorised access, use, disclosure, disruption, modification, or destruction. It is a broad concept that includes a variety of controls, such as access control, data encryption, and data backup.
  - **Business continuity:** Business continuity is the ability of an organisation to continue to operate its critical business functions in the event of a disruption. It includes a variety of controls, such as disaster recovery plans, business impact analysis, and risk management.

- **Change Management CPs**
  - **Offsite backup:** is the process of storing backup copies of data in a remote location. This can help to protect data from unauthorised access, use, or destruction.
  - **Asset management:** is the process of tracking and managing an organisation's information assets. It can help to identify and protect critical assets and to ensure that they are properly secured.

4.1.2 Key Characteristics of a CP

By implementing appropriate CPs, organisations can reduce their risk of a security incident and protect their information assets. Key characteristics of CPs in ISO27001:2022 are:

- relevance to the specific risk that it is intended to mitigate.
- 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.

4.2 Implementation stages for ISMS

The implementation stages for the ISO 27001:2022 ISMS are:

- **Planning**
  - Define the scope of the ISMS.
  - Identify the organisation's information assets.
  - Assess the organisation's risks to information security.
  - Develop an ISMS implementation plan.
- **Implementation**
  - Develop and implement the organisation's ISMS controls.
  - Train employees on the ISMS controls.
  - Communicate the ISMS to employees and stakeholders.
- **Operation**
  - Monitor and review the effectiveness of the ISMS controls.
  - Make necessary changes to the ISMS controls.
  - Conduct internal audits of the ISMS.
- **Improvement**
  - Identify and implement new ISMS controls as needed.
  - Conduct management reviews of the ISMS.

4.3 Systematic approach to implementation

The implementation stages can be customised to fit the specific needs of the organisation; however, it is important to follow a systematic approach to ensure that the ISMS is implemented effectively. By following the following steps, organisations can successfully implement the ISMS and improve their information security posture:

- 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.

5 IT Infrastructure Library

The IT Infrastructure Library (ITIL) is a set of concepts and practices for managing IT Service Management (ITSM) and IT Asset Management (ITAM) that focus on the alignment of IT services with the needs of the business.

ITIL gives detailed descriptions of a number of important IT practices and provides comprehensive check lists, tasks and procedures that any IT organisation can tailor to its needs. ITIL is published in a series of books, each of which covers an IT management topic. The names ITIL and IT Infrastructure Library are registered trademarks of the United Kingdom's Office of Government Commerce (OGC). The latest version at the time of writing is ITIL version 4, released in 2019.

ITIL takes a principles-based approach with a set of five principles:

1. **Focus on value**: ITIL organisations should focus on delivering value to their customers and stakeholders.
2. **Create a service value system**: ITIL organisations should create a service value system that aligns their IT services with their business goals.
3. **Work together**: ITIL organisations should work together across the organisation to deliver IT services.
4. **Be open**: ITIL organisations should be open to new ideas and approaches to ITSM.
5. **Be continual**: ITIL organisations should continuously improve their ITSM practices.

Five volumes comprise the ITIL 4, published in 2019 [2]:

- **Part 1: Foundations**: provide an overview of ITIL 4 and its five principles.
- **Part 2: Practices**: provide detailed guidance on the practices that organisations can use to implement ITIL 4.
- **Part 3: Digital and IT Strategy**: provides guidance on how organisations can use ITIL 4 to align their IT services with their digital and business strategies.
- **Part 4: Continual Service Improvement**: provides guidance on how organisations can continuously improve their ITSM practices.

5.1 ITIL Dimensions

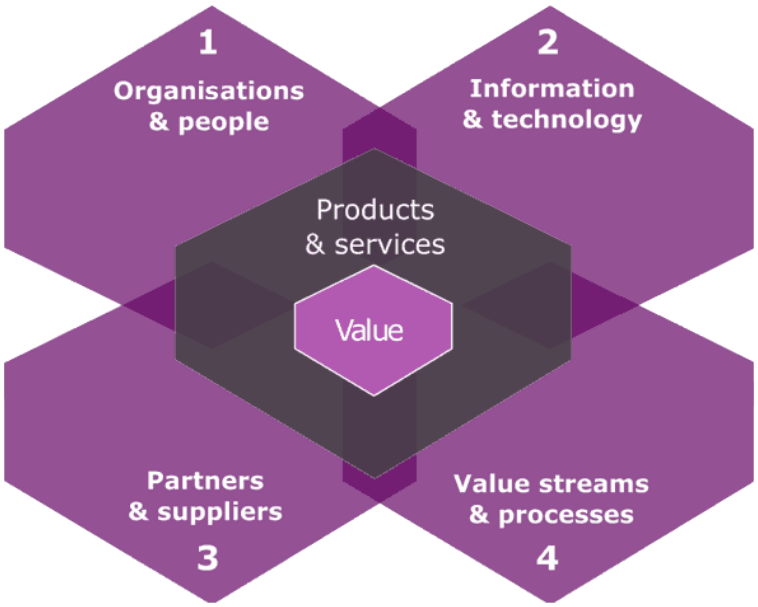

Figure 2: ITIL Dimensions

ITIL defines four dimensions that organisations should consider when implementing ITSM. The four dimensions of ITIL provide a holistic view of ITSM. By considering all four dimensions, organisations can ensure that they are implementing ITSM in a way that is effective and sustainable. The 4 dimensions are illustrated in Figure 2.

5.1.1 Organisations and people

This dimension focuses on the people who work in the organisation and the way they interact with each other and with IT services. It includes the following aspects:

- **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 ITSM.
- **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.

5.1.2 Information and technology

This dimension focuses on the IT that are used to deliver IT services. It includes the following aspects:

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

5.1.3 Partners and suppliers

This dimension focuses on the relationships that organisations have with their partners and suppliers. It includes the following aspects:

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

5.1.4 Value streams and processes

This dimension focuses on the way that value is created and delivered to customers and stakeholders. It includes the following aspects:

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

6 Committee of Sponsoring Organisations

The US Treadway Commission was established in 1985 to provide guidance on prevention of fraud or abuse of public trust by public officials, non-profit organisations, for-profit organisations, and others who are charged with upholding the law.

One output of the commission is the Committee of Sponsoring Organisations (COSO), a voluntary private-sector organisation, dedicated to providing guidance to executive management and governance entities on critical aspects of organisational governance, business ethics, internal control, Enterprise Risk Management (ERM), fraud, and financial reporting. COSO established a common internal control model against which companies and organisations may assess their control systems.

6.1 Internal Control - Integrated Framework

COSO's most well-known framework is the Internal Control - Integrated Framework (ICIF) [3], which is a set of principles and concepts that organisations can use to design, implement, and assess their internal controls. The framework is based on five interrelated components as illustrated in Figure 3.

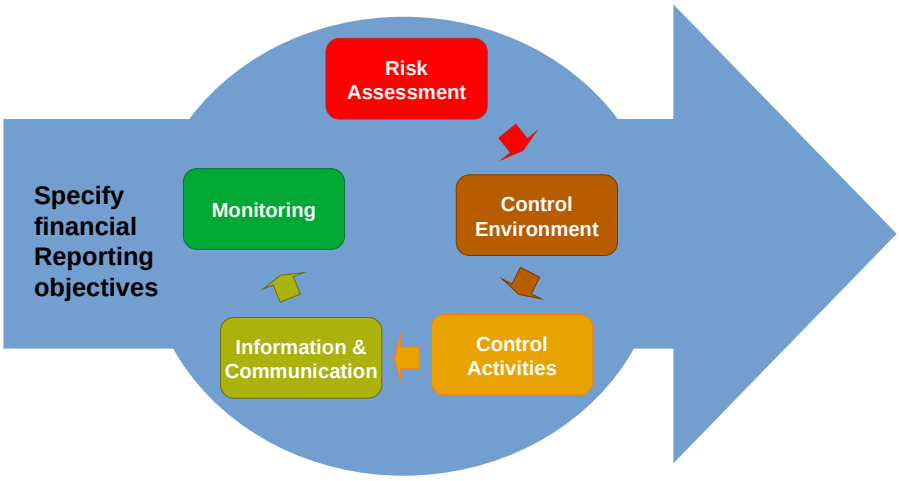

Figure 3: COSO Interrelated Components

The ICIF framework is widely accepted by organisations around the world, and it is used by regulators, auditors, and internal auditors to assess the effectiveness of internal controls.

In addition to the ICIF, COSO also publishes frameworks on ERM and fraud deterrence. The ERM framework provides guidance on how organisations can identify, assess, and manage risks to their objectives. The fraud deterrence framework provides guidance on how organisations can prevent and detect fraud.

The current version of the ICIF is version 2013. It is defined by three volumes:

- **Volume 1**: Executive Summary provides an overview of the framework and its key concepts.
- **Volume 2**: Framework provides a detailed explanation of the five components of internal control and the 17 principles that support them.
- **Volume 3**: Application Tools and Examples provides practical guidance on how to implement the framework in organisations of all sizes and industries.

6.2 COSO ERM Framework

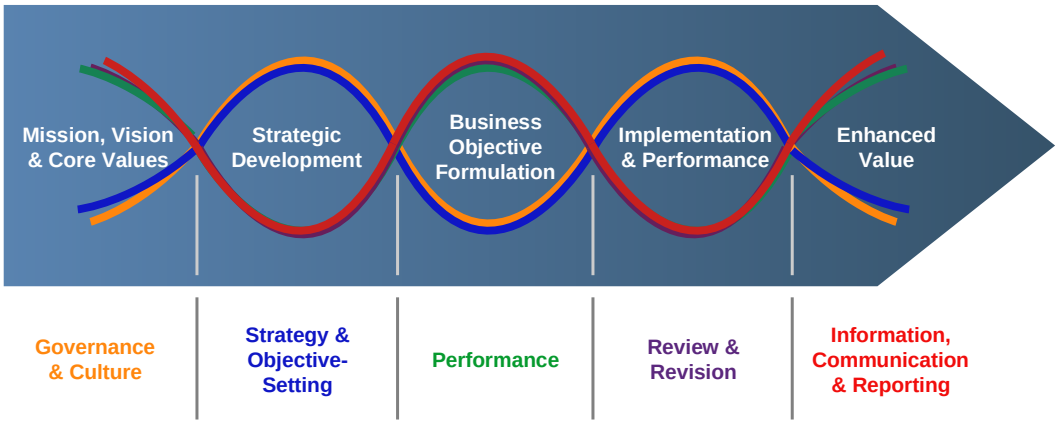

Figure 4: ERM Framework

The COSO ERM Framework has five component objectives and 20 principles across them [4]. The five objectives are:

1. **Governance and Culture**

   Governance and culture form a basis for all other components of ERM. Risk governance sets the entity's tone, reinforces the importance of and establishes oversight responsibilities for ERM. Culture pertains to ethical values, desired behaviours, and understanding of risk in the organisation. Culture is reflected in decision-making. An entity's board of directors plays an important role in governance and significantly influences ERM. There are five principles relating to this component:

   - Principle 1: Exercises Board Risk Oversight
   - Principle 2: Establishes Operating Structures
   - Principle 3: Defines Desired Organisational Behaviours
   - Principle 4: Demonstrates Commitment to Core Values
   - Principle 5 : Attracts, Develops and Retains Capable Individuals.

2. Strategy and Objective-Setting

ERM is integrated into the entity's strategic plan through the process of setting strategy and business objectives. With and understanding of business context, the organisation can gain insight into internal and external factors and their effect on risk. Risk appetite is established and aligned with strategy. The business objectives allow strategy to be put into practice and shape the entity's day-to-day operations and priorities. Four principles have been set relating to this component:

- Principle 6: Analyses Business Context
- Principle 7: Defines Risk Appetite
- Principle 8: Evaluates Alternative Strategies
- Principle 9: Formulates Business Objectives.

3. Performance

An organisation identifies and assesses risks that may affect the entity's ability to achieve its strategy and business objectives. Risks are prioritised according to their severity and considering the entity's risk appetite. The organisation then selects risk responses and monitors performance for change. The organisation determines a portfolio view of the amount of risk the entity has assumed in the pursuit of its strategy and business objectives. There are five principles relating to this component:

- Principle 10: Identifies Risk
- Principle 11: Assesses Severity of Risk
- Principle 12: Prioritises Risk
- Principle 13: Implements Risk Responses
- Principle 14: Develops Portfolio View.

4. Review and Revision

An entity's strategy or business objectives and ERM practices and capabilities may change over time as the entity adapts to shifting business context. In addition the business context in which the entity operates can also change, resulting in current practices no longer applying or sufficient to support the achievement of current or updated business objectives. As necessary, the organisation revises its practices or supplements it capabilities. This component has three principles:

- Principle 15: Assesses Substantial Change
- Principle 16: Reviews Risk and Performance
- Principle 17: Pursues Improvement in ERM.

5. **Information, Communication and Reporting**

   Communication is the continual, iterative process of providing, sharing and obtaining information, which flows throughout the entity. Management uses relevant information from both internal and external sources to support ERM. The organisation reports on risk, culture, and performance at multiple levels of the entity. There are three principles regarding this component:

   - Principle 18: Leverages Information and Technology
   - Principle 19: Communicates Risk Information
   - Principle 20: Reports on Risk, Culture, and Performance.

The current version is the 2017 COSO ERM Framework, and it is defined by two volumes:

- **Volume 1**: Executive Summary provides an overview of the framework and its key concepts.
- **Volume 2**: Framework provides a detailed explanation of the five objective components of ERM and the 20 principles that support them.

6.3 COSO Complementary frameworks

The ICIF and the ERM are complementary frameworks. The ICIF can be used to implement the ERM by providing guidance on how to design and implement control activities to mitigate risks.

The ICIF is more focused on the internal controls that are necessary to achieve an organisation's objectives, while the ERM is more focused on the overall risk management process.

Organisations can use either framework, or both frameworks, to improve their risk management practices. The best framework for an organisation will depend on its specific needs and objectives.

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

Figure 5: Key differences between the COSO ICIF and the ERMF

7 Capability Maturity Model

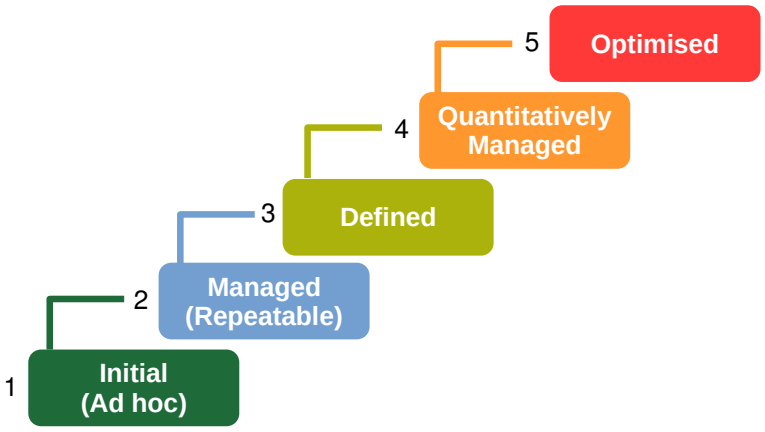

Figure 6: CMM Levels

The Capability Maturity Model (CMM) is a service mark and a model for understanding the capability maturity of an organisation's software development business processes. Because the CMM is about process maturity, it differs from more common maturity models that provide a structured collection of elements that describe certain aspects of maturity in an organisation. The CMM is useful as a general theoretical model, to aid in the definition and understanding of an organisation's process capability maturity.

Level 1 – Initial / Ad-Hoc

- It is characteristic of processes at this level that they are (typically) undocumented and in a state of dynamic change, tending to be driven in an ad hoc, uncontrolled and reactive manner by users or events.
- This provides a chaotic or unstable environment for the processes.

Level 2 - Repeatable

- It is characteristic of processes at this level that some processes are repeatable, possibly with consistent results.
- Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress.

Level 3 - Defined

- It is characteristic of processes at this level that there are sets of defined and documented standard processes established and subject to some degree of improvement over time.
- These standard processes are in place and are used to establish consistency of process performance across the organisation.

Level 4 - Managed

- It is characteristic of processes at this level that, using process metrics, management can effectively control the process.
- In particular, management can identify ways to adjust and adapt the process without measurable loss of quality or deviations from specifications.
- Process Capability is established from this level.

Level 5 - Optimised

- It is characteristic of processes at this level that the focus is on continually improving process performance through both incremental and innovative technological changes/improvements.

For software development, the CMM has been superseded by Capability Maturity Model Integration (CMMI). The CMMI is a proven methodology for Performance Management managed by the Software Engineering Institute (SEI). It comes in three models:

CMMI for Acquisition

- Designed for businesses that focus on working with suppliers to assemble a product or deliver a service.
- This model delves into creating effective solicitations and supplier agreements, effectively gathering and communicating requirements to suppliers, monitoring supplier activities and artefacts, and ensuring the results of supplier work meet the needs of end users.

CMMI for Development

- Designed for businesses that focus on developing products and services.
- This model delves into detail about converting customer requirements into requirements used by developers, effectively integrating product components into the final product or service, performing the technical analysis and development work to design the product or service, and ensuring that development work meets the needs of the end users and the specifications formulated during design.

CMMI for Services

- Designed for businesses that focus on working with suppliers to assemble a product or deliver a service.
- This model delves into the creation of effective solicitations and supplier agreements, effectively gathering and communicating requirements to suppliers, monitoring supplier activities and artefacts, and ensuring the results of supplier work meet the needs of end users.

8 Control Objectives for Information and Related Technology

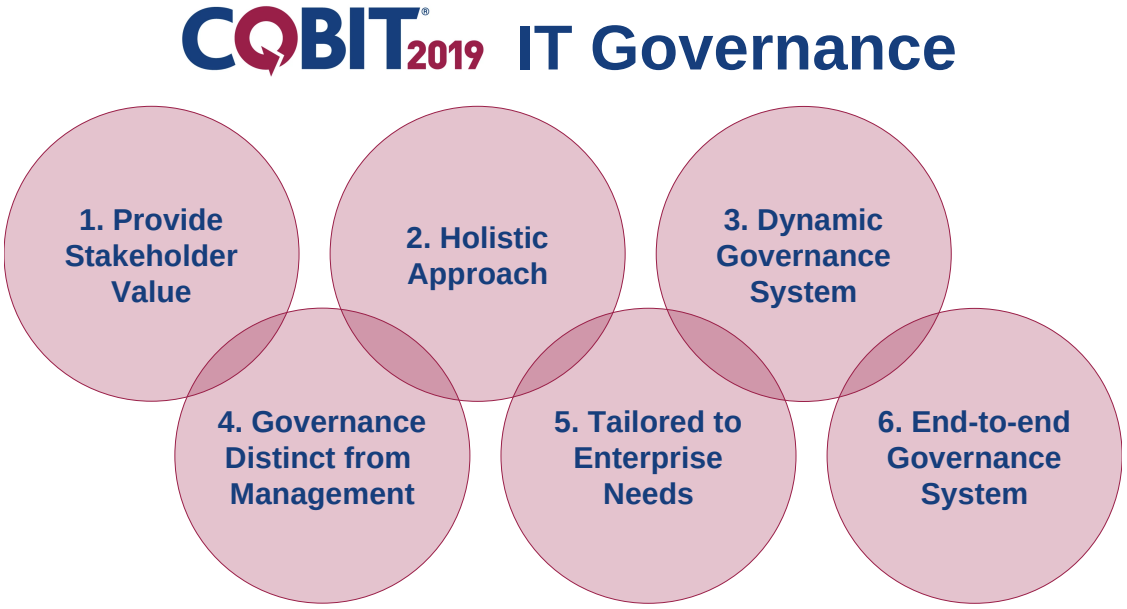

Figure 7: COBIT 2019 IT Governance

Developed by the Information Systems Audit and Control Association (ISACA), Control Objectives for Information and Related Technology (COBIT) 2019, is a comprehensive framework for IT governance and management that helps organisations align their IT investments with their business goals [5]. COBIT covers all aspects of IT governance, from strategy and planning to risk management and compliance.

8.1 COBIT Principles

The COBIT framework is based on six principles:

1. **Provide Stakeholder Value.** The governance system should be designed to meet the needs of all stakeholders, including customers, employees, investors, and regulators. This means that the governance system should be focused on helping the organisation achieve its goals and objectives, while also protecting the interests of all stakeholders.
2. **Holistic Approach.** The governance system should consider all aspects of IT, including strategy, architecture, development, delivery, and support. This means that the governance system should be integrated with other enterprise governance frameworks, such as ERM and compliance.
3. **Dynamic Governance System.** The governance system should be flexible and adaptable to change. This is because the business landscape is constantly changing, and the governance system needs to be able to keep up. The governance system should also be able to respond to new risks and opportunities.

4. **Governance Distinct from Management.** The governance system should be responsible for setting direction and overseeing management's performance, but it should not be involved in the day-to-day management of IT. This is because governance is about setting the rules of the game, while management is about playing the game.
5. **Tailored to Enterprise Needs.** The governance system should be tailored to the specific needs of the enterprise, taking into account its size, complexity, industry, and risk profile. This means that there is no one-size-fits-all approach to governance. The governance system should be customised to meet the specific needs of the organisation.
6. **End-to-end Governance System.** The governance system should cover all aspects of IT, from planning and design to delivery and support. This means that the governance system should be integrated across all business units and functions.

8.2 COBIT Objectives

Figure 8: COBIT 2019 Objective Domains

COBIT 2019 defines 40 governance and management objectives, which are grouped into five domains:

1. **Evaluate, Direct and Monitor (EDM)**: is concerned with ensuring 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.
2. **Align, Plan and Organise (APO)**: is concerned with developing and implementing an IT strategy that is aligned with the organisation's overall business goals. It also includes objectives related to resource management and project management.
3. **Build, Acquire and Implement (BAI)**: is concerned with the development and implementation of IT solutions. It includes objectives related to requirements management, change management, and testing.
4. **Deliver, Service and Support (DSS)**: is concerned with the delivery and support of IT services. It includes objectives related to service level management, incident management, and problem management.

5. **Monitor, Evaluate and Assess (MEA)**: is concerned with 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.

Consider some examples of COBIT 2019 objectives:

- **EDM01: Establish and maintain a strategic vision for IT**
  - Ensures that the organisation has a clear and well-defined vision for its IT. The vision should be aligned with the organisation's overall business goals and objectives, and it should be communicated to all stakeholders.
- **APO01: Align the IT strategy with the enterprise strategy**
  - Ensures that the IT strategy is aligned with the organisation's overall business strategy. The IT strategy should support the organisation's goals and objectives, and it should be flexible enough to adapt to change.
- **BAI01: Manage the IT investment portfolio**
  - Ensures that the organisation's IT investments are aligned with its business goals and objectives, and that they are delivering the value that the business needs.
- **DSS01: Ensure the availability and performance of IT services**
  - Ensures that the organisation's IT services are available and performant when needed. This includes managing capacity, performance, and availability.
- **MEA01: Monitor and evaluate the performance of IT solutions and services**
  - Monitors and evaluates the performance of the organisation's IT solutions and services. This includes monitoring IT costs, benefits, and risks.

These are just a few examples of COBIT 2019 objectives. Organisations can use COBIT 2019 objectives to assess their current IT governance and management practices, and to identify areas for improvement. COBIT 2019 objectives can also be used to develop and implement a plan to improve IT governance and management. 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.

9 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**. What are the organisation's top risks? What are its most important priorities? Once the organisation's goals and objectives are clear, it can then select the frameworks that are most relevant to achieving those goals.
- **Assess the organisation's current state**. What are the organisation's current risk management practices? What are its strengths and weaknesses? This assessment will help the organisation to identify where it needs to improve and how the frameworks can be used to achieve those improvements.
- **Select the right frameworks**. Not all frameworks are created equal. Some frameworks are more comprehensive than others, and some are more focused on specific areas of risk management. The organisation should select the frameworks that are most appropriate for its needs.
- **Prioritise the frameworks**. Not all frameworks need to be implemented at the same time. The organisation should prioritise the frameworks based on its goals and objectives.
- **Align the frameworks**. Once the frameworks have been selected, they need to be aligned with each other. This means ensuring that the frameworks are compatible and that they work together to achieve the organisation's goals.
- **Implement the frameworks**. The frameworks should be implemented in a coordinated and efficient manner. This may involve creating a roadmap or timeline for implementation.
- **Monitor and evaluate the frameworks**. Once the frameworks have been implemented, they should be monitored and evaluated to ensure that they are effective. This may involve conducting regular audits or reviews.

By following these pointers, organisations can implement multiple frameworks in a way that is coordinated and efficient. This can help organisations to improve their risk management practices and achieve their goals. Some additional points of consideration when implementing multiple frameworks are:

- **The organisation's size and complexity**: Larger and more complex organisations may need to implement more frameworks than smaller and simpler organisations.
- **The organisation's industry**: Some industries are more regulated than others, and this may affect the need for certain frameworks.
- **The organisation's culture**: The organisation's culture can also affect the success of implementing multiple frameworks. If the organisation is not open to change, it may be more difficult to implement new frameworks.

Some examples of the type of organisations that implement a combination of two or more frameworks, such as ISO27000, ITIL, COSO and COBIT are:

- **Financial Institutions**: Banks are required to comply with a number of regulations, including the Payment Card Industry Data Security Standard (PCI DSS), which is based on ISO/IEC 27001. Banks also use ITIL to manage their IT services and COSO to manage their overall risk.
- **Healthcare organisations**: Healthcare organisations are required to comply with a number of regulations, including the General Data Protection Regulation (GDPR). Healthcare organisations also use ITIL to manage their IT services and COSO to manage their overall risk.
- **Government agencies**: Government agencies are required to comply with a number of regulations, including the EU Cybersecurity Act [6]. Government agencies also use ITIL to manage their IT services and COSO to manage their overall risk.
- **Critical infrastructure organisations**: Critical infrastructure organisations, such as power plants and telecommunications providers, are required to comply the Network Information Systems (NIS) directives [7] [8]. Critical infrastructure organisations also use ITIL to manage their IT services and COSO to manage their overall risk.
- **Technology companies**: Technology companies use ISO/IEC 27001 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.

These are just a few examples of organisations that implement a combination of two or more of ISO/IEC 27000, ITIL, COSO and COBIT. The specific frameworks that an organisation uses will depend on its specific needs and objectives.

10 NIST Cybersecurity Framework

10.1 Introduction to CSF

A Cybersecurity Framework, such as the US National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) [9], describes essential cybersecurity outcomes that can help an organisation reduce its cybersecurity risk. Frameworks are not necessarily a one size fits all approach to managing cybersecurity risks and, depending on circumstances, it maybe necessary to take elements from two or more. An example that will be explored later is the ISO International Electrotechnical Commission (IEC) 27001 [10] and International Society of Automation (ISA)/IEC 62443 [11], together to deal with a particular set of circumstances in Operational Technology (OT) environments. Organisations have unique risks, including different threats, vulnerabilities, and risk tolerances, as well as unique mission objectives and requirements across sectors. Thus, each organisations' implementation of a Framework, and approaches they make to managing risk, vary.

This topic will focus on the NIST CSF v2.0 as a basis for understanding Cybersecurity Frameworks and later in the module other frameworks will be discussed.

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

- **Understand and Assess**:
  - Describe an organisation's current or target cybersecurity posture within and across organisations, sectors, or business units.
  - Determine where an organisation may have cybersecurity gaps, including with respect to existing or emerging threats or technologies, and assess progress toward addressing those gaps.
  - Align policy, business, and technological approaches to managing cybersecurity risks across an entire organisation or in a more focused area, such as a portion of the organisation, a specific technology, or technology suppliers.
- **Prioritise**:
  - Prioritise opportunities to improve cybersecurity risk management.
  - Identify, organise, and prioritise actions for reducing cybersecurity risks that align with the organisation's mission, legal and regulatory requirements, and risk management and governance expectations.
  - Inform decisions about cybersecurity-related workforce needs and capabilities.

- **Communicate**:
  - Provide a common language for communicating with internal and external parties about cybersecurity risks, capabilities, needs, and expectations.
  - Complement an organisation's risk management process by presenting a concise way for executives and others to distil the fundamental concepts of cybersecurity risk so that they express at a high level risks to be managed and how their organisation uses cybersecurity standards, guidelines, and practices.

10.2 Framework Core

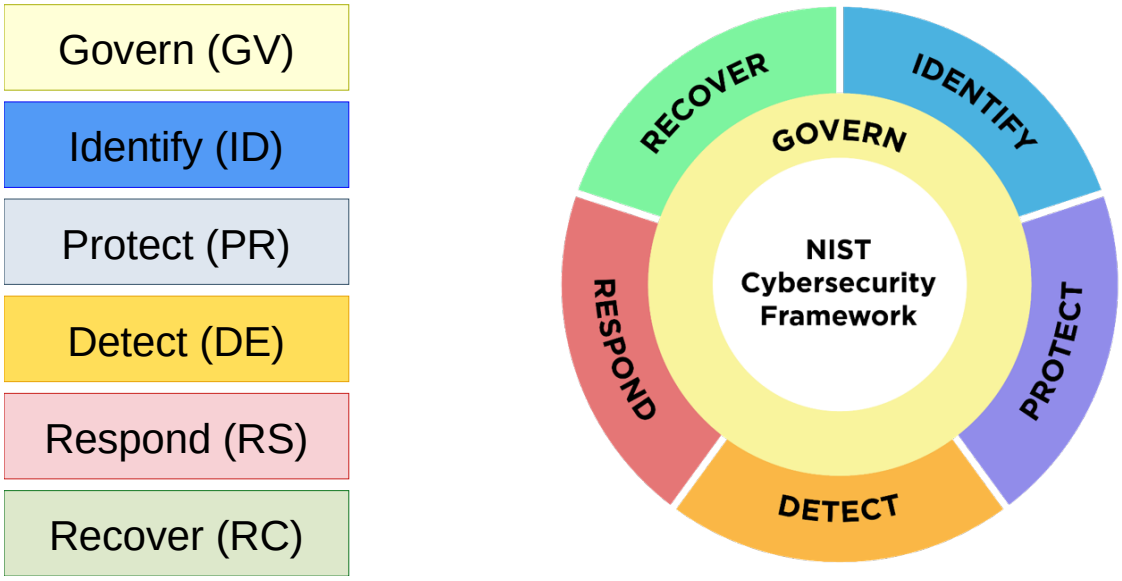

Figure 9: Framework Functions

The Framework Core provides a set of cybersecurity outcomes, arranged by Function, Category, and Subcategory, implementation examples of how those outcomes might be achieved as well as references to additional guidance on how to achieve those outcomes.

10.2.1 Functions

Govern (GV)

Establish and monitor the organisation's cybersecurity risk management strategy, expectations, and policy. This is a cross-cutting function and provides outcomes to inform how an organisation will achieve and prioritise the outcomes of the other five functions in the context of its mission and stakeholder expectations. GV directs the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policies, processes, and procedures; and the oversight of cybersecurity strategy.

Identify (ID)

A function to determine the current cybersecurity risk to the organisation. Understanding the assets as well as the related cybersecurity risks enables an organisation to focus and prioritise effort in a manner consistent with its risk management strategy and the mission needs identified under GV. This function includes the identification of improvements needed for the organisation's policies, processes, procedures, and practices supporting cybersecurity risk management to inform efforts under all six functions.

Protect (PR)

Use safeguards to prevent or reduce cybersecurity risk. Once assets and risks are identified and prioritised, PR supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events. This function includes outcomes such as awareness and training; data security; identity management, authentication, and access control; platform security as well as the resilience of technology infrastructure.

Detect (DE)

Find and analyse possible cybersecurity attacks and compromises. DE enables timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse cybersecurity events that may indicate that cybersecurity attacks and incidents are occurring.

Respond (RS)

Action related to a detected cybersecurity incident. RS supports the ability to contain the impact of cybersecurity incidents and outcomes include incident management, analysis, mitigation, reporting, and communication.

Recover (RC)

Restore assets and operations that were impacted by a cybersecurity incident. RC supports timely restoration of normal operations to reduce the impact of cybersecurity incidents and enable appropriate communication during recovery efforts.

Figure 9 illustrates the CSF Functions in a wheel as all framework functions are related to each other. GV is in the centre of the wheel considering how it informs the organisation on the implementation of the other five functions.

10.3 Categories and Sub-categories

Functions are subdivided into categories of related outcomes and Subcategories are a further division of a Category into specific outcomes of technical and management activities.

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

Figure 10: Categories and their identifiers

11 Implementing the CSF

Organisations can choose to handle risk in different ways;

- Mitigation
- Transfer
- Avoidance
- Acceptance.

The organisation can also use the framework both internally and to oversee third parties.

11.1 CSF Profiles

CSF Profiles are developed to understand, assess, and communicate the organisation's current or target cybersecurity posture and to prioritise outcomes for achieving the target cybersecurity posture.

These profiles:

- Assess the organisation's achievement in terms of cybersecurity outcomes.
- Characterise cybersecurity risk management outcomes within framework tiers.
- Improve cybersecurity communication with internal and external stakeholders.
- Manage cybersecurity risk throughout supply chains.

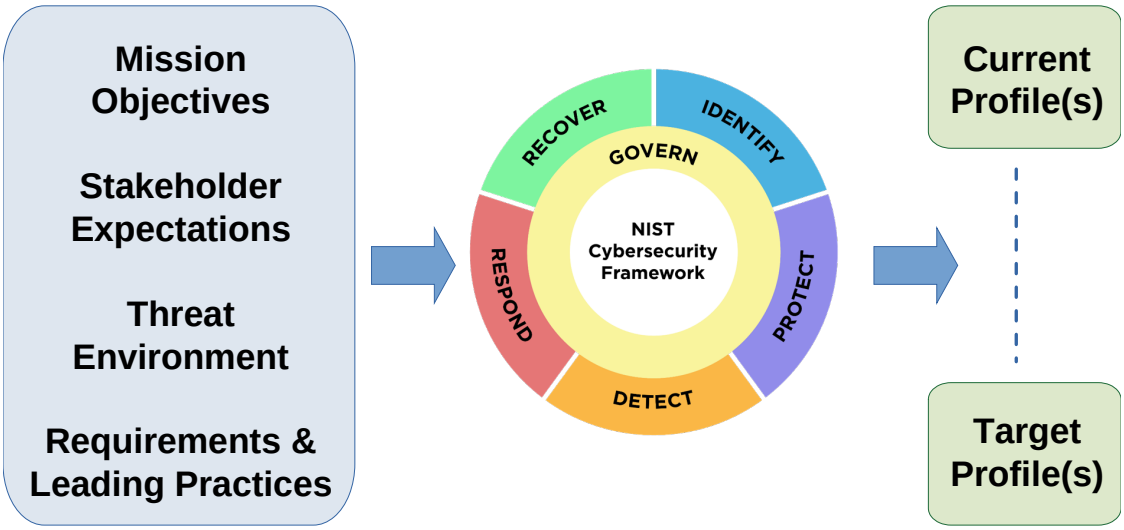

Figure 11: CSF Target Profiles

As illustrated in Figure 11, there are two types of profiles:

- **Current Profile**
  - Covers the Core outcomes that an organisation is currently achieving (or attempting to achieve) and characterises how or to what extent each outcome is being achieved.
- **Target Profile**
  - Covers the desired outcomes that an organisation has selected and prioritised from the Core for achieving its cybersecurity risk management objectives.
  - A Target Profile takes into account anticipated changes to the organisation's cybersecurity posture, such as new requirements, new technology adoption, and cybersecurity threat intelligence trends.

Some organisations prefer to create a Current Profile first. An organisation may want to review its current efforts first and then consider areas for improvement. Others prefer to start with a Target Profile and work toward it.

11.1.1 Create CSF Profiles

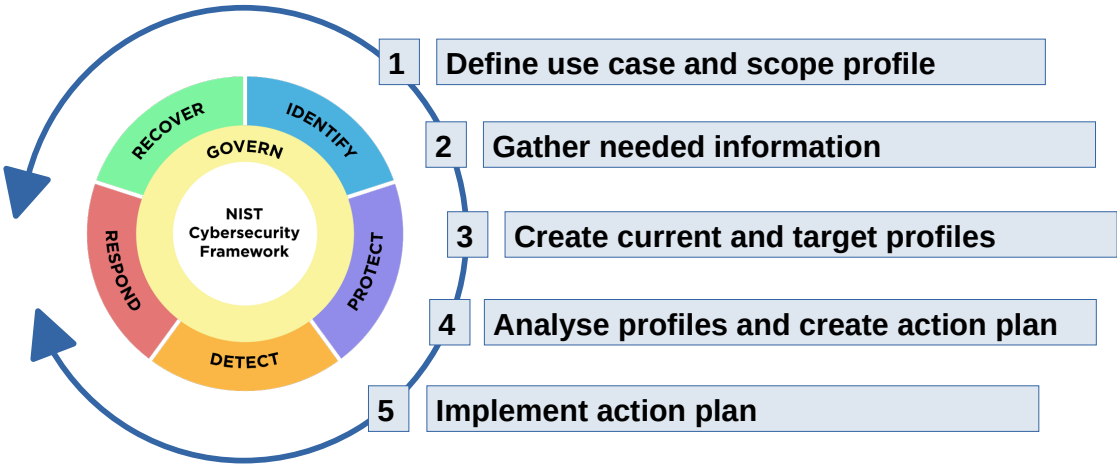

Figure 12: Create CSF Profiles

1. **Define the use case for the Profiles**
   - The use case defines the high-level facts and assumptions on which the Profiles will be based, as a way of scoping the Profiles.
   - This can include:
     - The reason for creating the Profiles
     - The organisation's divisions, IT assets, services, and other elements that are in scope for these Profiles
     - Those who will develop, review, and operationalise the Profiles
     - The individuals who will set expectations for actions to achieve the cybersecurity outcomes.

2. **Gather the information needed to prepare the Profiles**
    - An organisation can gather relevant resources prior to preparing the Profiles, such as organisational policies, risk management priorities and resources, cybersecurity requirements and standards followed by the organisation, and work roles.

3. **Create Current and Target Profiles**
    - Determine what types of supporting information each Profile should include for each of the selected Framework outcomes, and fill in the elements for each selected outcome. Consider the risk implications of the current state to inform target state planning and prioritisation.

4. **Analyse the Profiles and create an action plan**
    - Identify and analyse the differences between the Current and Target Profiles is a great way for the organisation to identify gaps and develop a prioritised action plan for addressing those gaps to improve cybersecurity.

5. **Implement the action plan and update the Profiles**
    - The organisation follows the action plan to adjust its cybersecurity practices to address gaps and move toward the Target Profile. Improving an organisation's cybersecurity programme is a continuous effort, and implementing an action plan can take months or years. At frequencies defined by the organisation, the Current Profile should be updated to assess progress towards the Target.
    - Profile(s) should be updated to reflect changes in the organisation and its cybersecurity risk.

An organisation may choose to develop multiple profiles that each address a different use case and scope. This can enable better prioritisation of activities and outcomes where there may be differing degrees of cybersecurity risk while still allowing an organisation to use the overarching framework structure for consistency across use cases. Examples include describing a cybersecurity outcome posture for:

- An entire enterprise
- Each of an organisation's major business units
- Business partners or suppliers
- Each of an organisation's most critical systems
- Products or services with cybersecurity requirements.

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

Figure 13: Organisational Profile Template

Figure 13 illustrates a organisational profile template. This could have added elements such as:

- Status
- Priority
- Policies, Processes and Procedures
- Internal Practices
- Roles and Responsibilities
- References
- Measurements/Metrics
- Artefacts and Evidence.

Figure 14 illustrates a possible action plan template that is customisable to an organisations own requirements. Once differences between the Current and Target Profiles are identified, analysed and gaps are identified, an action plan is required to address the gaps to improve cybersecurity. This plan should consider mission drivers, benefits, risks, and necessary resources.

This example template includes rows for the priority of each action item, a description of the action item, the responsible party or department, the target completion date, and the resources required to accomplish the action item, such as personnel, budget, tools. This template can be integrated with the Profiles or maintained separately. The action plan can be based on outcomes at the Function, Category, or Subcategory level or a combination of those levels.

The CSF is designed to be used in conjunction with other cybersecurity frameworks, standards, and guidance. There are many resources that can be tapped into within NIST publications but also with other organisations that will be the subject of future topics in this module.

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

Figure 14: Action Plan Template

11.2 CSF Tiers

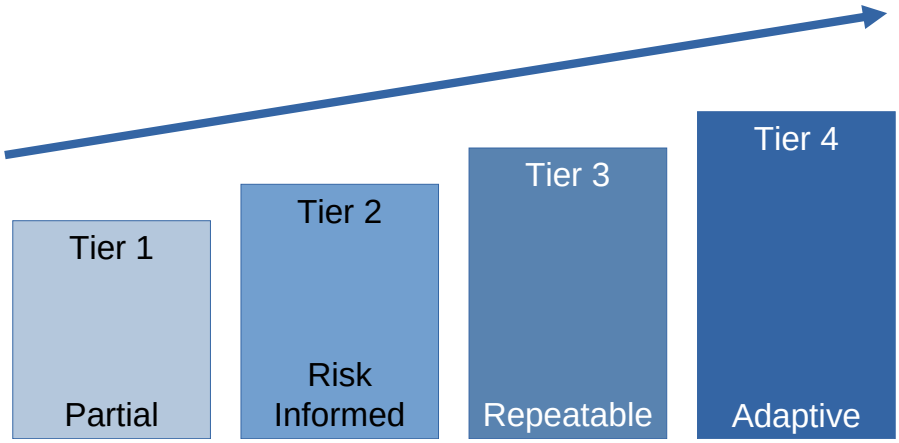

Figure 15: CSF Tiers

CSF Tiers help to set the overall tone for how cybersecurity risks will be managed within the organisation, and determine the effort required to reach a selected Tier. This follows the CMM.

Tier 1

Organisations can start with where they are, perhaps with undocumented processes and in a state of dynamic change, tending to be driven in an ad hoc, uncontrolled and reactive manner by users or events. This provides a chaotic or unstable environment for the processes.

Tier 2

Risk management practices, within the organisation, are approved by management but may not be established as organisational-wide policy. Prioritisation of cybersecurity activities and protection requirements are directly informed by organisational risk objectives, the threat environment, or business/mission requirements.

Tier 3

The organisation's risk management practices are formally approved and expressed as policy. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Organisational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements, threats, and technological landscape.

Tier 4

There is an organisation-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 organisational objectives is clearly understood and considered when making decisions. Senior executives monitor cybersecurity risks in the same context as financial and other organisational risks.

12 Frameworks Summary

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

Figure 16: Frameworks Summary

13 Bibliography

[1] 'ISO/IEC 27001: 2022 Information Security Management Systems'. ISO, Oct. 01, 2022. Accessed: Sep. 10, 2023. [Online]. Available: https://www.iso.org/standard/27001

[2] *ITIL® Foundation: ITIL 4 Edition (2022)*. PeopleCert, 2022.

[3] 'Achieving Effective Internal Control over Sustaibability Reporting (ICSR): Building Trust and Confidence through the COSO Internal Control—Integrated Framework'. COSO, Jun. 28, 2023. Accessed: Sep. 14, 2023. [Online]. Available: https://www.coso.org/_files/ugd/3059fc_a3a66be7a48c47e1a285cef0b1f64c92.pdf

[4] 'COSO Enterprise Risk Management: Integrating with Strategy and Performance'. COSO, Jun. 2017. Accessed: Sep. 14, 2023. [Online]. Available: https://www.aicpa-cima.com/cpe-learning/publication/coso-enterprise-risk-management-integrating-with-strategy-and-performance

[5] Isaca, *COBIT 2019 Framework: Governance and Management Objectives*. Schaumburg, USA: Isaca, 2018.

[6] Regulation (EU) 2019/881, *EU Cybersecurity Act*. 2019, p. 55. Accessed: Oct. 09, 2023. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2019/881/oj

[7] Directive (EU) 2016/1148, *Measures for a high common level of security of network and information systems across the Union*. 2016, p. 30. Accessed: Jun. 09, 2023. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[8] Directive (EU) 2022/2555, *Measures to ensure a high common level of cybersecurity in the Union and amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing the Directive (EU) 2016/1148 (NIS 2 Directive)*. 2022, p. 73. Accessed: Aug. 08, 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[9] NIST, 'Cybersecurity Framework 2.0', National Institute of Standards and Technology, Aug. 2023. Accessed: Aug. 22, 2023. [Online]. Available: https://doi.org/10.6028/NIST.CSWP.29.ipd

[10] ISO/IEC27001, 'Information security, cybersecurity and privacy protection — Information security management systems — Requirements'. Oct. 25, 2022.

[11] ISA/IEC 62443, 'Industrial communication networks - IT security for networks and systems'. International Society of Automation/International Electrotechnical Commission, Jul. 20, 2009.