Topic 7
Risk Management

Dr Diarmuid Ó Briain

12 Aug 2025

setu.ie
INSPIRING FUTURES

Version: 3.0

Licence

Learning objectives

By the end of this topic you will be able to:

- Understand Foundational Risk Management Concepts.
- Describe and Differentiate Key Risk Management Frameworks.
- Develop a Practical Risk Management Plan (RMP).
- Evaluate Risk Management Frameworks (RMF) for Organisational use.

Risk Management in OT

- OT systems are increasingly connected to IT networks, which exposes them to cyber threats.
- Risk management in OT is the process of identifying, assessing, and mitigating risks to OT systems.
- The five basic steps of OT risk management are:
  - Risk Identification
  - Risk Assessment
  - Risk Mitigation
  - Control Implementation
  - Monitoring.

Risk Management in OT

- Here are some specific risks that need to be considered in OT risk management:
  - Cyber attack
  - Natural disaster
  - Human error.

What is Risk

*Risk is a function of the likelihood of a given **threat-source's** exercising a particular potential **vulnerability**, and the resulting **impact** of that adverse event on the organisation*

Risk Assessment Process

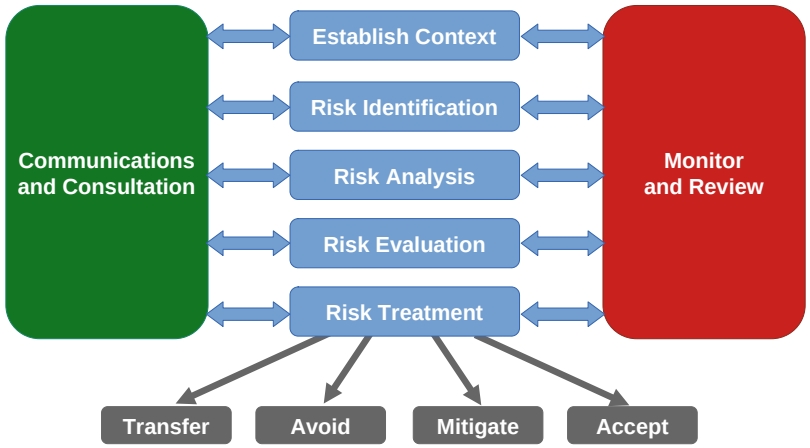
- Phase 1: Preliminary Risk Assessment
- Phase 2: Risk Analysis of Critical Areas and Processes
- Phase 3: Organisation-Wide Risk Assessment

Risk Assessment Process

Risk Assessment Process

- Asset
- Asset Valuation
- Threats
- Vulnerability
- Exposure
- Risk
- Safeguards
- Attack
- Breach

Risk Management Process



ISO 31000:2018 – Risk Management Guidelines

- Establishing the Context
- Risk Identification
- Risk Analysis
- Risk Evaluation
- Risk Treatment
- Continuous Monitoring & Review
- Communication & Consulting.

Risk Appetite

- The level and type of cyber risk an organisation is willing to accept in pursuit of its objectives.
- It is a strategic decision that defines how much risk the organisation is prepared to tolerate before taking action to mitigate it.
- It guides decision-making related to cybersecurity investments and controls.

Risk Appetite Statement

- A statement of the organisations Risk Appetite
- Specific Risk Categories
  - Critical Business Systems and Data
    - Financials, Customer Data, Intellectual Property
  - Operational and Support Systems
    - Internal Communication, HR Systems, Development Environments)
  - Experimental or Non-Production Systems
    - R&D, Sandbox Environments

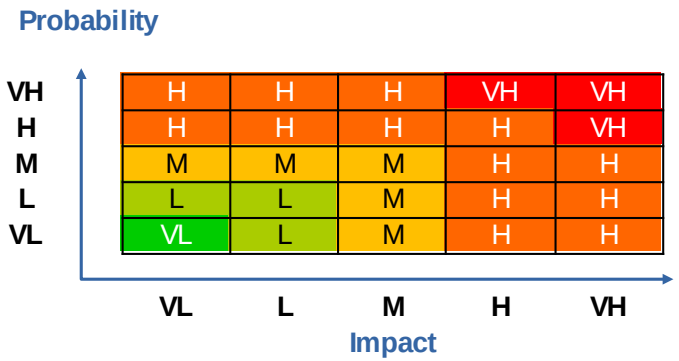
Risk Appetite Statement

- Example:
  - **Critical Business Systems and Data**
    - **Appetite**: **Very Low**. [ORGANISATION] has a zero-tolerance approach to any risk that could lead to a significant breach of CIA of these assets. The organisation will invest in robust security controls, continuous monitoring, and proven technologies to mitigate these risks to the lowest possible level.
    - **Justification**: The loss, corruption, or unauthorised disclosure of these assets would have a catastrophic impact on our reputation, legal standing, and financial viability.

Risk Appetite Statement

- **Risk Tolerance and Thresholds**
  - **Financial Impact**: [ORGANISATION] will not accept a single event with a potential financial loss exceeding €1 million without explicit, senior-level approval.
  - **Reputational Damage**: [ORGANISATION] will not accept any risk that could lead to a public data breach notification or significant negative media coverage.
  - **Regulatory/Legal**: [ORGANISATION] will not accept any risk that could result in a violation of major regulatory requirements (e.g., GDPR, NIS2) or legal obligations.

Probability and Impact Matrix Tool



Risk Log

- Identify Risks.
- Perform Qualitative/Quantitative Risk Analysis.
- Plan Risk Responses.

Project: <Project Title>

Summary				Description				Preventative Actions			Contingency Actions		
ID	Date Raised	Raised By	Description of Risk	Description of Impact	Probability Rating	Impact Rating	Priority Rating	Action	Resource	Date	Actions	Resource	Date

VL = Very Low | L = Low | M = Medium | H = High | VH = Very High

Quantitative Risk Analysis

- Quantitative risk analysis attempts to **assign monetary values** to the components of the risk assessment and to the assessment of the potential loss.
- Asset valuation
  - Value retained from the cost of creating the information asset
  - Value retained from past maintenance of the information asset
  - Value implied by the cost of replacing the information
  - Value from providing the information
  - Value acquired from the cost of protecting the information
  - Value to owners
  - Value of intellectual property
  - Value to adversaries
  - Loss of productivity while the information assets are unavailable
  - Loss of revenue while information assets are unavailable

Asset valuation

- An organisation must be able to place a dollar value on each information asset it owns, based on:
  - How much did it cost to create or acquire?
  - How much would it cost to recreate or recover?
  - How much does it cost to maintain?
  - How much is it worth to the organisation?
  - How much is it worth to the competition?

Exposure factor (EF)

- **Loss Potential** or the percentage of loss an organisation would realise if a risk was realised.
- **Single Loss Expectancy (SLE)**
  - The monetary value expected from the occurrence of a risk on an asset.
  - SLE = AV x EF
- **Annualised Rate of Occurrence (ARO)**
  - An estimate based on the data of how often a threat would be successful in exploiting a vulnerability.
- **Annualised Loss Expectancy (ALE)**
  - A calculation of the single loss expectancy multiplied the annual rate of occurrence, or how much an organisation could estimate to lose from an asset based on the risks, threats, and vulnerabilities. It is:
  - ALE = SLE x ARO
- **Annual Cost of Safeguard (ACS)**
  - This is the cost of the researched safeguard.
- **Cost Benefit Analysis (CBA)**
  - CBA determines whether or not a control alternative is worth its associated cost. CBAs may be calculated before a control or safeguard is implemented, to determine if the control is worth implementing, or calculated after controls have been implemented and have been functioning for a time:
  - CBA = (ALE(prior) – ALE(post)) – ACS

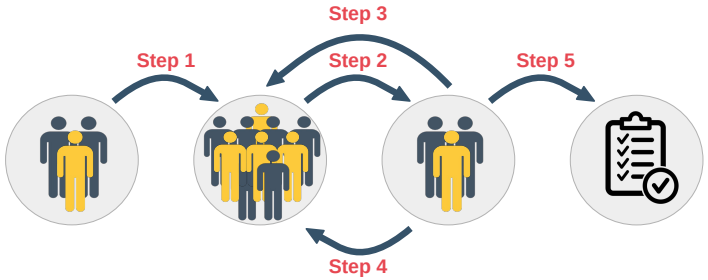
Performing a quantitative risk analysis

- Create an inventory of assets and assign a value [**Asset Value (AV)**].
- Conduct a risk assessment and vulnerability study to determine the risk factors for each asset. For each threat calculate the **Exposure Factor (EF)** and **Single Loss Expectancy (SLE)**.
- Perform threat analysis to determine the likelihood of the threat occurring in a single year – **Annualised Rate of Occurrence (ARO)**.
- Determine the **Annualised Loss Expectancy (ALE)** for each risk factor.
- Research **countermeasures** for each threat and calculate the change to the ARO and ALE if they were deployed.
- Perform a **Cost/Benefit Analysis (CBA)** of the countermeasures and choose the most appropriate response to each threat.

Qualitative Risk Analysis

- Relative measure of risk or asset value based on ranking or separation into descriptive categories such as low, medium, high; not important, important, very important; or on a scale from 1 to 10.
- Techniques used to assess the risk and produce a Risk Registrar.
  - Brainstorming
  - Delphi Technique
  - Storyboarding
  - Focus Groups
  - Surveys
  - Questionnaires
  - Check Lists
  - Interviews.

Delphi Technique



Steering Group
Gathers known uncertainties and/or asks an open question to experts.

Experts
Steering Group collates the responses +/- group them into common themes.

Steering Group
Responses are sent back to be ranked by experts.

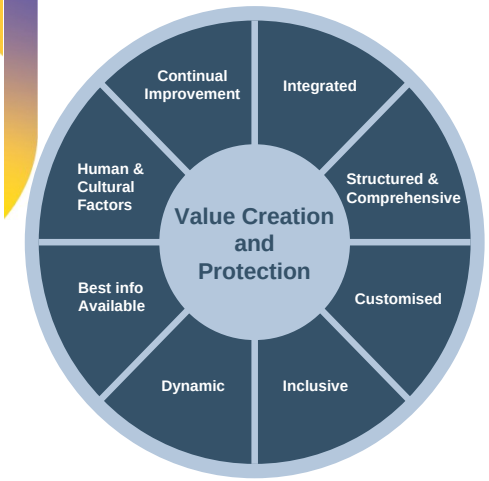
List of Priorities
Final list of top priorities is created.

Note: Steps 3 and 4 can be repeated additional times as deemed necessary.

ISO/IEC 31000 Risk Management

- Global standard that provides a framework and guidelines for managing risk.
- A generic standard, applicable to any organisation, regardless of size, sector, or industry.
- Not intended for certification, giving organisations the flexibility to customise their own approach.
- Its ultimate goal is to create and protect value.
- Provides a comprehensive approach covering the full risk management process, from identifying to monitoring risks.
- Emphasises the importance of leadership commitment and a continual improvement cycle.

ISO/IEC 31000 - Risk Management Principles

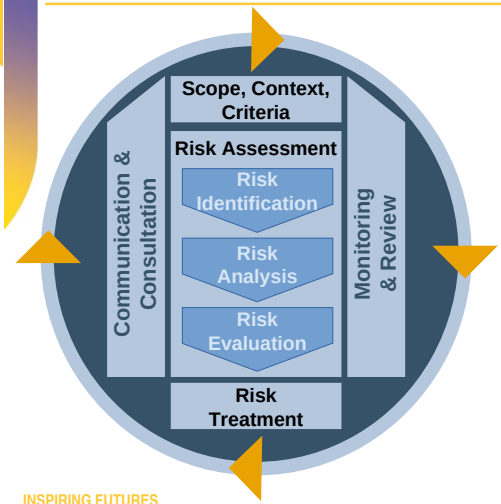


- Part of all processes.
- A systematic approach.
- Tailored to the organisation.
- Involves all stakeholders.
- Responsive to change.
- Based on reliable information.
- Considers people and culture.
- Constantly enhanced.

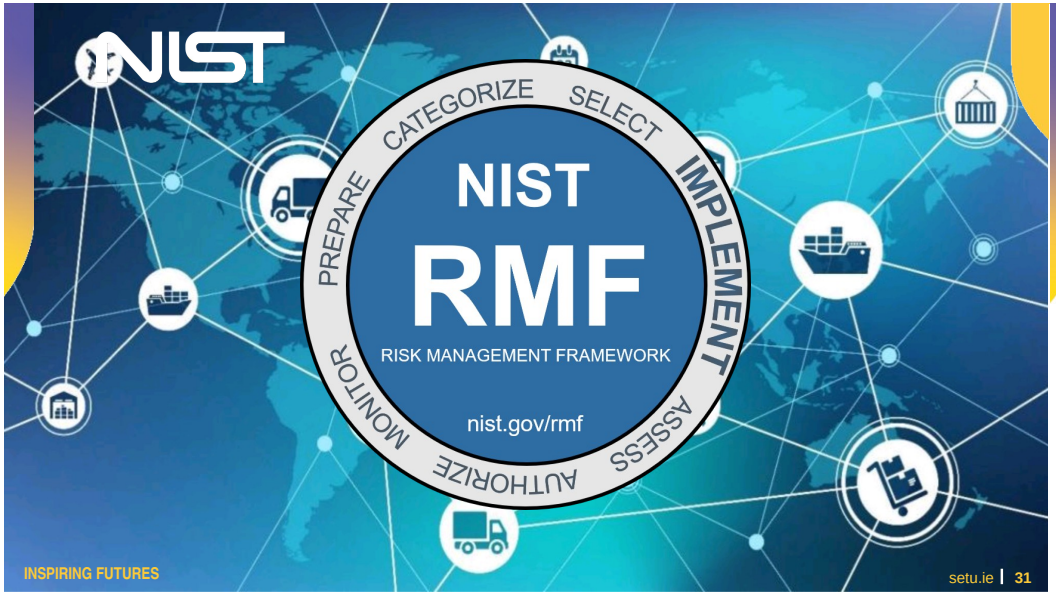
ISO/IEC 31000 - Risk Management Framework

- The foundation of the entire process, driven by top management.
- Embedding the framework into all organisational functions and decisions.
- Planning the framework and its specific components.
- Putting the designed framework into action.
- Measuring and assessing the framework's performance.
- Enhancing the framework based on evaluation results.

ISO/IEC 31000 - Risk Management Process



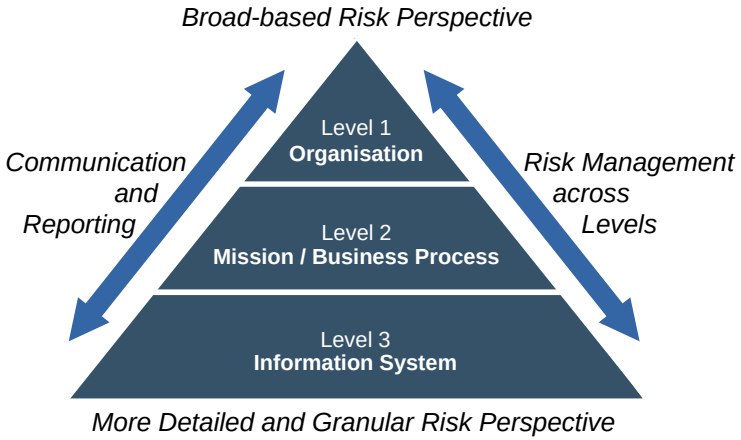
- Defining the scope, environment, and criteria for managing risk.
- Risk Assessment
  - Identification of the risks
  - Analysis of the nature and level of risks
  - Evaluation if/what risk treatment.
- Risk Treatment
  - Modifying risks based on the evaluation.
- Ongoing Activities:
  - Continuous stakeholder engagement.
  - Monitoring & Review: Regular checking and updating of the process.



NIST SP 800-39: Managing Information Security Risk

- Foundational document.
- Establishes the strategic framework and core principles for managing information security risk at:
  - Organisational level
  - Mission /Business Process level
  - Information System level
- It answers the what and why of risk management, defining the fundamental components and the hierarchy of risk.

Organisation-wide Risk Management Approach



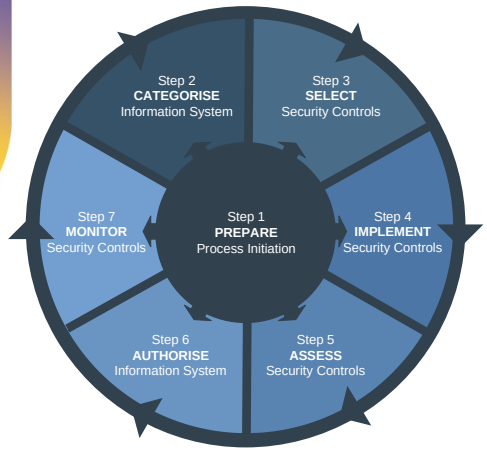
NIST SP 800-30: Guide for Conducting Risk Assessments

- Focuses on the risk assessment process.
- Provides the detailed methodology, steps, and techniques for identifying, analysing, and evaluating risks.
- A how-to guide for a specific activity within the broader framework.

NIST SP 800-37 Rev2: Risk Management Framework

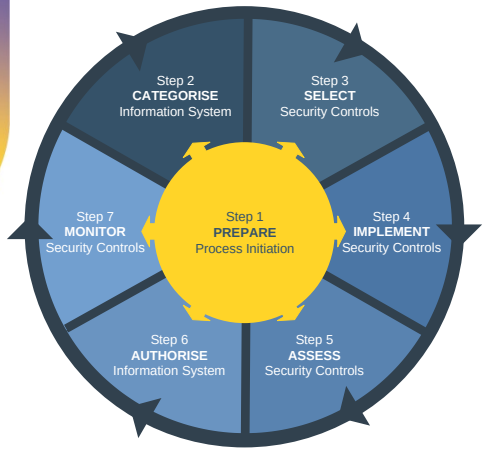
- Provides the end-to-end, comprehensive process for managing security and privacy risk throughout a system's life cycle.
- The operational document that ties:
  - The strategic guidance of SP 800-39
  - The detailed risk assessment methodology of SP 800-30
  - The SP 800-53 Rev. 5 Security and Privacy Controls
  - Other related publications
- This is the focus of this section of the topic.

RMF Steps and Structure



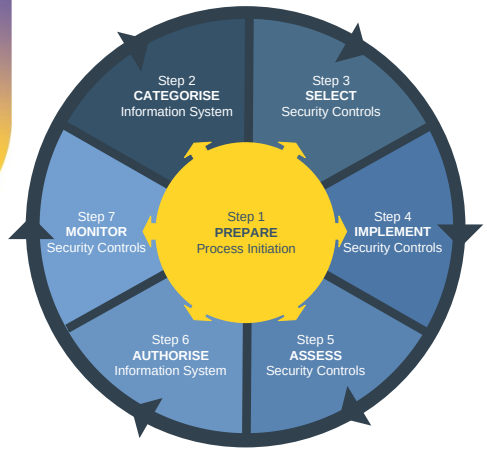
- A comprehensive, flexible, and repeatable, 7-step, process.
- Integrates security and privacy throughout a system's life cycle.
- Helps organisations make informed, risk-based decisions.
- Authorises systems for operation based on an acceptable risk posture.

RMF PREPARE — Organisational level tasks



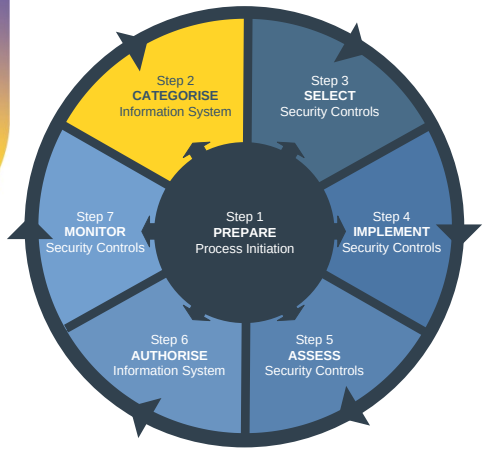
Nr.	Task
P-1	Risk Management Roles
P-2	Risk Management Strategy
P-3	Risk Assessment — Organisation
P-4	Organisationally-Tailored Control, Baselines and CSF, Profiles (Optional)
P-5	Common Control Identification
P-6	Impact-Level Prioritisation (Optional)
P-7	Continuous Monitoring Strategy — Organisation

RMF PREPARE — System level tasks



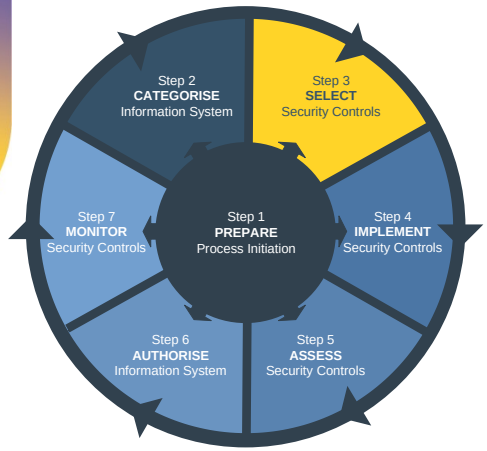
Nr.	Task
P-8	Mission or Business Focus
P-9	System Stakeholders
P-10	Asset Identification
P-11	Authorisation Boundary
P-12	Information Types
P-13	Information Lifecycle
P-14	Risk Assessment — System
P-15	Requirements Definition
P-16	Enterprise Architecture
P-17	Requirements Allocation
P-18	System Registration

RMF CATEGORISE tasks



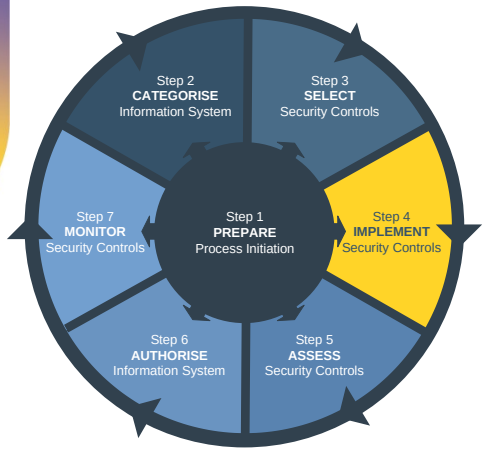
Nr.	Task
C-1	System Description
C-2	Security Categorisation
C-3	Security Categorisation Review and Approval

RMF SELECT tasks



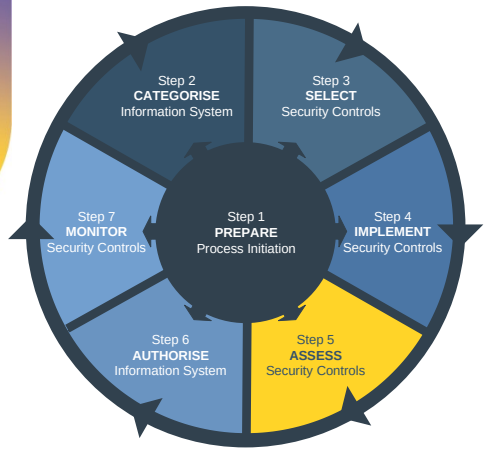
Nr.	Task
S-1	Control Selection
S-2	Control Tailoring
S-3	Control Allocation
S-4	Documentation of Planned Control Implementations
S-5	Continuous Monitoring Strategy — System
S-6	Plan Review and Approval

RMF IMPLEMENT task



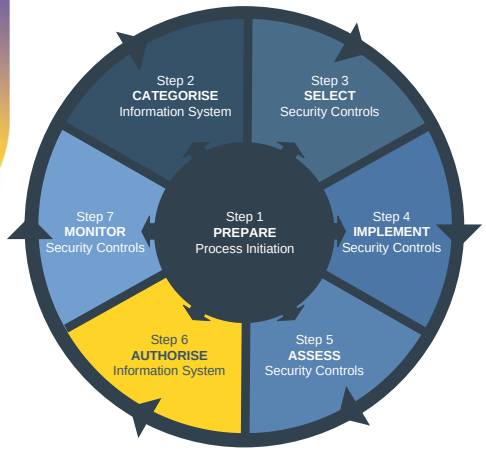
Nr.	Task
I-1	Control Implementation
I-2	Update Control Implementation Information

RMF ASSESS task



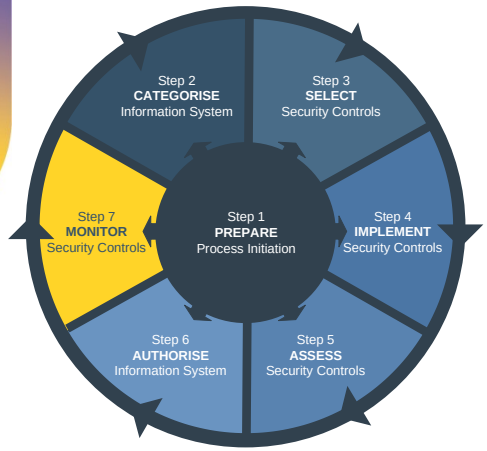
Nr.	Task
A-1	Assessor Selection
A-2	Assessment Plan
A-3	Control Assessments
A-4	Assessment Reports
A-5	Remediation Actions
A-6	Plan of Action and Milestones

RMF AUTHORISE tasks



Nr.	Task
R-1	Authorisation Package
R-2	Risk Analysis and Determination
R-3	Risk Response
R-4	Authorisation Decision
R-5	Authorisation Reporting

RMF MONITOR tasks



Nr.	Task
M-1	System and Environment Changes
M-2	Ongoing Assessments
M-3	Ongoing Risk Response
M-4	Authorisation Package Updates
M-5	Security and Privacy Updates
M-6	Ongoing Authorisation
M-7	System Disposal

Risk Management Summary

Feature	ISO/IEC 31000	NIST SP 800-37, Rev 5
Scope	General, all-encompassing. Applies to all types of risks.	Specific to information systems and managing cybersecurity and privacy risks.
Approach	Principles-based guidelines. Highly flexible and customisable.	Prescriptive, process-oriented framework. Provides a detailed, seven-step process.
Audience	Any organisation, regardless of size, type, or industry.	Designed for US federal agencies and organisations, however widely applicable.
Purpose	To provide a common approach and terminology to effectively manage risk.	To provide a structured methodology for securing information systems and complying with federal mandates.
Core Components	Principles, Framework, and Process.	A seven-step process: Prepare, Categorise, Select, Implement, Assess, Authorise, and Monitor.
Compliance	Not certifiable; an organisation can align with its principles.	Following it is often a mandatory requirement for compliance with US federal laws and regulations.
Integration	Encourages integration of risk management into all organisational activities and decision-making.	Integrates with a suite of other NIST publications (e.g., SP 800-53) for controls and assessment.

Risk Management Plan (RMP)

- Document that describes the risks associated with a product, service, or project, and the actions that will be taken to mitigate those risks
- Commonly used in a variety of industries, including healthcare, OT industries and organisations as well as IT
- An RMP typically includes sections such as:
  - Risk Identification
  - Risk Assessment/Analysis
  - Risk Mitigation/Treatment
  - Risk monitoring
  - Risk review.
- RMPs are living documents that should be updated regularly as new information becomes available and as the product, service, or project changes.

Risk Management Plan (based on ISO/IEC 31000)

- **1. Establish the Context**
  - **Internal Context**
  - **External Context**
  - **Risk Criteria**
    - Risk Appetite
    - Likelihood & Impact scales
    - Risk priority matrix
- **2. Risk Assessment**
  - **Risk Identification**
    - Safety, Quality, Operational & Asset-Specific Risks
  - **Risk Analysis**
    - Determine Likelihood and Impact
    - Review Existing Controls
  - **Risk Evaluation**
    - Prioritise Risks

Risk Management Plan (based on ISO/IEC 31000)

- **3. Risk Treatment**
  - Select Risk Treatment Options
    - Avoid the Risk
    - Modify the Risk (Mitigation)
    - Transfer the Risk
    - Accept the Risk
- **4. Monitoring and Review**
  - Monitor Risks
  - Review the RMP
  - Communicate and Consult

Risk Management Plan (based on SP 80-37r2 RMF)

- **1. PREPARE**
  - Organisational-Level Activities
    - Define the Risk Management Strategy
    - Frame the Risk
    - Establish the Common Control Strategy
  - System-Level Activities (Asset Identification)
    - Identify System Boundaries
    - Identify Key Stakeholders
- **2. CATEGORISE**
  - Categorise the OT System
  - Document the System Description
- **3. SELECT**
  - Select Controls
  - Tailor the Controls
  - Develop the System Security Plan

Risk Management Plan (based on SP 80-37r2 RMF)

- **4. IMPLEMENT**
  - Implement Controls
- **5. ASSESS**
  - Assess Controls
  - Identify Vulnerabilities
- **6. AUTHORISE**
  - Prepare Authorisation package
  - Determine Risk Acceptance
  - Authorise the System
- **7. MONITOR**
  - Monitor Controls and Risk
  - Review and Update the Plan
  - Respond to Events

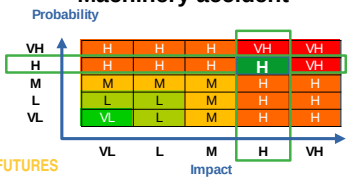
RMP — Risk Identification

- Group exercise
  - Discuss specific risks associated with a Hydro-electrical Power Station

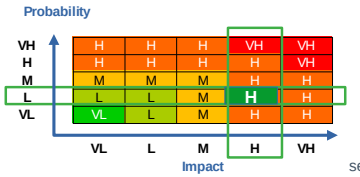
RMP — Risk Assessment

- The likelihood and impact of each risk should be assessed
- For example
  - the risk of a machinery accident may be considered to be high probability and high impact
  - the risk of a product recall may be considered to be low probability and high impact.

Machinery accident



Product Recall



RMP — Risk Assessment

- Individually
  - Assess the risk of a worker in the power station falling into the tailrace of the power station.
- Group
  - Discuss the individual findings and come to an agreed assessment.


2


3

RMP — Risk Mitigation

- For each risk, a risk mitigation strategy should be developed
- Risk mitigation strategies can include:
  - Avoiding the risk
  - Reducing the probability of the risk
  - Reducing the impact of the risk
  - Transferring the risk to a third party.

RMP — Risk Mitigation

- Individually
  - Consider mitigation strategies to the risk.
- Group
  - Discuss the individual strategies and come to an agreed strategy.


2


3

RMP — Risk Monitoring

- The risks should be monitored regularly to ensure that the risk response strategies are effective
- This is important because risks can change over time, and new risks may emerge.

RMP — Risk Review

- The RMP needs to move with changes in the operation of the organisation
- To ensure this happens it is essential that the RMP is evaluated for its effectiveness of risk management controls and identifying areas for continual improvement.

OT RMP

- **Step 1: Asset Identification**
  - What is at risk?
- **Step 2: Risk Identification**
  - What are the threats?
- **Step 3: Risk Assessment**
  - How do the risks expose the OT?
- **Step 4: Risk Mitigation**
  - Access controls, Segmentation, Data Encryption, IDS, IPS, SIEM
- **Step 5: Monitor and Review the RMP**
  - Is the RMP still effective?

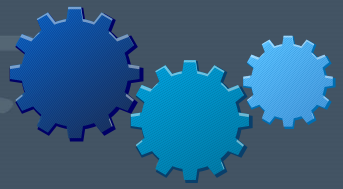
Learning objectives

You should now be able to:

- Understand the nature of Risk Management in OT environments ✓
- Identify the major potential risks to OT systems as cyber attacks, natural disasters, and human error ✓
- Assess the likelihood and impact of each risk using quantitative and qualitative methods ✓
- Define controls to reduce the likelihood or impact of risks ✓
- Implement controls to reduce the likelihood or impact of risks ✓
- Monitor the effectiveness of the controls to reduce the likelihood or impact of risks ✓

Exercise #5

Scenario



EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir Sinsearach

D +353 59 917 5000 | E diarmuid.obriain@setu.ie | **setu.ie**
Campas Bhóthar Chill Chainnigh, Ceatharlach, R93 V960, Éire

engcore
advancing technology