Topic 7

Risk Management

Dr Diarmuid Ó Briain

Version: 3.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Dr Diarmuid Ó Briain

Table of Contents

Table of Figures

Index of Tables

1 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.

2 Introduction to Risk Management in OT

Operational technology (OT) is the physical devices and software that control industrial processes, such as power plants, manufacturing facilities, and critical infrastructure. OT systems are increasingly connected to Information Technology (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 basic steps of OT risk management are:

- **Risk Identification**: Identify the potential risks to OT systems, such as cyber attacks, natural disasters, and human error.
- **Risk Assessment**: Assess the likelihood and impact of each risk.
- **Risk Mitigation**: Implement controls to reduce the likelihood or impact of each risk.
- **Control Implementation**: Implement the controls that have been identified.
- **Monitoring**: Monitor the effectiveness of the controls and make adjustments as needed.

Effective OT risk management is essential to protect critical infrastructure and ensure the safety and security of OT systems. Here are some specific risks that need to be considered in OT risk management:

- **Cyber attack**: Cyber attacks are the most common threat to OT systems. These attacks can be used to steal data, disrupt operations, or even cause physical damage.
- **Natural disaster**: Natural disasters, such as floods, earthquakes, and hurricanes, can also pose a serious threat to OT systems. These disasters can damage or destroy OT equipment, disrupt power supplies, and disrupt communication networks.
- **Human error**: Human error is another common cause of OT incidents. This can include mistakes made by operators, technicians, and engineers.

OT risk management is a complex and challenging task. However, it is essential to protect critical infrastructure and ensure the safety and security of OT systems. By following the five steps of OT risk management, organisations can reduce the risks to their OT systems and improve their overall security posture. Each organisation has 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 suitable framework, and approaches they make to managing risk, vary.

3 Risk Management

3.1 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 [1].

3.2 Risk Assessment Process

It is important to emphasise that risk assessment is a process as opposed to a once off event. Because technology and processes change, risk assessments need to be conducted periodically.

- **Phase 1: Preliminary Risk Assessment**
  - In the first phase, it is necessary to perform a preliminary risk assessment and educate upper management about the risks so that they can make informed decisions about where to allocate the necessary resources.

- **Phase 2: Risk Analysis of Critical Areas and Processes**
  - In the second phase a more in-depth set of risk assessments are performed on critical areas and processes identified in the preliminary risk assessment.

- **Phase 3: Organisation-Wide Risk Assessment**
  - The goal of the third phase is to perform a thorough, wide risk assessment.
  - This phase focuses on IT issues relating to risk assessment with the understanding that this is only part of the process. Ultimately, risk assessment must take into account natural disasters, fire, and other events that can make a system unavailable.

3.3 Risk Terminology

Figure 1: Linking Risk Terminology

- **Asset**: Anything within the environment that should be protected.
- **Asset Valuation**: Monitory value of an asset. This value should include not just the physical value of the item but costs associated with development, maintenance, repair and replacement for example.
- **Threats**: Anything that may cause an undesirable outcome for the organisation of a specific asset. This includes any action or in-action that could cause damage, loss, disclosure of assets.
- **Vulnerability**: Absence or weakness of safeguards that protect an organisation or asset.
- **Exposure**: Being susceptible to an asset loss because of a threat. Exposure is not a realised threat but the fact that a vulnerability exists and it could be exposed.
- **Risk**: Possibility that a threat will exploit a vulnerability to cause harm to an asset.
- **Safeguards**: A safeguard is a countermeasure that removes a vulnerability or protects an asset from all or specific threats.
- **Attack**: The actual exploitation of a vulnerability that may cause damage, loss or disclosure of assets.
- **Breach**: A breach is the occurrence of a security mechanism being bypassed or thwarted.

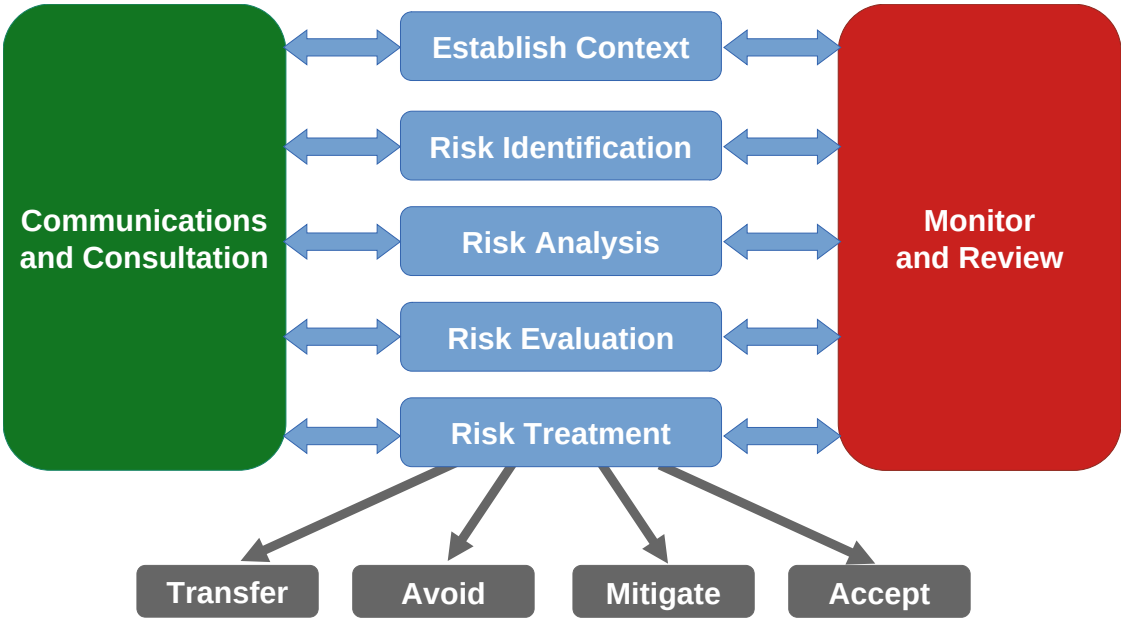


Figure 2: Risk Management Process

Risk Management plays an important role in maintaining the cybersecurity posture of an organisation. It involves identifying, analysing, evaluating, and mitigating potential risks that could impact the objectives or the successful execution of business operations [2].

Risk management is a fundamental practice across various industries, including finance, healthcare, engineering, project management, and more. It is an ongoing process, and as circumstances change, new risks are identified and mitigated. As a result, a proactive and adaptable approach to risk management plays a crucial role in long-term success.

Figure 2 is a good reference for understanding the Risk Management Process. It involves:

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

4 Risk Mitigation and Treatment

Risk mitigation is the process an organisation takes to reduce its exposure to the various risks it might face. Organisations can face many risks, some of which can cause severe disruption or financial loss. Mitigation is a prudent step every organisation should take to avoid such unwanted events.

4.1 Risk Appetite Statement

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

An organisation should develop a formal Risk Appetite statement. For example:

Organisational Risk Appetite Statement

Purpose: This statement defines the organisation's overall attitude towards and tolerance for risk, specifically in the context of information and technology assets. It serves as a guiding principle for all risk management activities, from strategic decision-making to day-to-day operational procedures.

Core Principle: The organisation is committed to a moderate to low-risk appetite for its critical business functions and data. We will actively identify, assess, and manage risks to protect the confidentiality, integrity, and availability of our information systems and data, while enabling business innovation and growth.

Specific Risk Categories

1. **Critical Business Systems and Data**

   (e.g., Financials, Customer Data, Intellectual Property)

   - **Appetite: Very Low.** [ORGANISATION] has a zero-tolerance approach to any risk that could lead to a significant breach of Confidentiality, Integrity, or Availability (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.

2. **Operational and Support Systems**

   (e.g., Internal Communication, HR Systems, Development Environments)

   - **Appetite: Low to Moderate.** [ORGANISATION] are willing to accept a limited level of residual risk, provided that the potential impact does not disrupt core business operations or compromise critical data. We will prioritise cost-effective controls that provide reasonable assurance of security.
   - **Justification:** While important for daily operations, the failure or compromise of these systems would not result in an immediate, catastrophic impact on the organisation. We can tolerate a higher level of risk in these areas to optimise resource allocation.

3. **Experimental or Non-Production Systems**

   (e.g., R&D, Sandbox Environments):

   - **Appetite: Moderate to High.** The [ORGANISATION] is willing to accept a higher level of risk to foster innovation and rapid development. Controls in these environments may be less stringent, and the use of new, unproven technologies may be permitted, provided that:
     - These systems are logically and physically isolated from critical production environments.
     - No sensitive or production data is ever stored or processed within them.
     - A clear and documented process exists for transitioning systems to a more secure state before they are considered for production use.
   - **Justification:** This approach allows for agility and innovation without exposing the organisation to unacceptable risk.

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., General Data Protection Regulations (GDPR), Network & Information Systems (NIS2)) or legal obligations.

4.2 Probability and Impact Matrix tool

Use a Probability and Impact Matrix tool, such as that illustrated in Figure 3, to grade each risk. This is an organisationally agreed impact and probability values that are used to categorise and determine the priority of each risk.

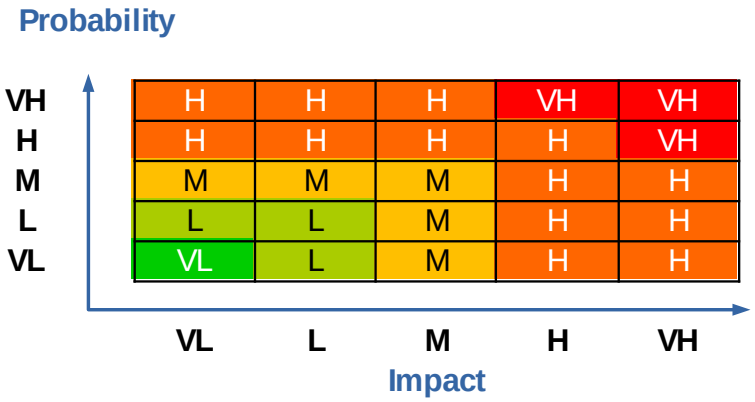


Figure 3: Probability and Impact Matrix Tool

#FF0000	Very High Risk
#FF6600	High Risk
#FFBF00	Medium Risk
#AACC00	Low Risk
#00CC00	Very Low Risk

The Risk Appetite Statement and a risk's specific Priority Rating are fundamental inputs for determining the appropriate Risk Treatment option.

The organisation's Risk Appetite Statement sets the overall tolerance for risk. This high-level policy is then used to establish specific risk tolerance thresholds. The priority rating of an individual risk is then measured against these thresholds.

For example, if an organisation has a Medium risk appetite, it may define its tolerance thresholds as follows:

- Risks with a priority rating of M, L, or VL are generally considered within the organisation's appetite. Therefore, the default risk treatment for these risks would be to *Accept*, provided they are regularly monitored.
- Risks with a priority rating of High or Very High are typically outside of the organisation's appetite. These risks require a more proactive treatment, such as *Mitigate*, *Transfer*, or *Avoid*.

It's important to note that while *Accept* may be the default for lower-priority risks, a conscious decision is still required. Simply accepting a risk without a formal review or ongoing monitoring is a passive approach that could lead to unforeseen consequences.

4.3 Risk Log

The first step is to identify the organisations risks. Once the risks have been logged in a register, such as in Figure 4, take each risk and perform a Qualitative/Quantitative Risk Analysis on each. Then from an informed position plan preventative and contingency actions.

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

Figure 4: Risk Register

4.4 Risk Analysis

4.4.1 Quantitative

Quantitative risk analysis attempts to assign monetary values to the components of the risk assessment and to the assessment of the potential loss.

Asset Value

Asset value or Asset Valuation (AV) is the process of assigning financial value or worth to each information asset. Some of the components of asset valuation include:

1. Value retained from the cost of creating the information asset
2. Value retained from past maintenance of the information asset
3. Value implied by the cost of replacing the information
4. Value from providing the information
5. Value acquired from the cost of protecting the information
6. Value to owners
7. Value of intellectual property
8. Value to adversaries
9. Loss of productivity while the information assets are unavailable
10. Loss of revenue while information assets are unavailable.

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. It is:

$$SLE = AV \; x \; EF$$

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:

$$CBA = (ALE(prior) - ALE(post)) - ACS$$

ALE (prior to control) is the ALE of the risk before the implementation of the control.

ALE (post-control) is the ALE examined after the control has been in place for a period of time.

4.4.2 Performing a quantitative risk analysis

The following is a step by step breakdown of the quantitative risk analysis:

- Create an inventory of assets and assign a value AV.
- Conduct a risk assessment and vulnerability study to determine the risk factors for each asset. For each threat calculate the EF and SLE.
- Perform threat analysis to determine the likelihood of the threat occurring in a single year – ARO.
- Determine the 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 CBA of the countermeasures and choose the most appropriate response to each threat.

Example

A SCADA Server is compromised and becomes unavailable.

The server is valued at €6,000 and the EF is 70% (0.7).

$$SLE = AV \; x \; EF = € \, 6{,}000 \, x \, 0.7 = € \, 4{,}200$$

The cost for a single occurrence of the server being unavailable is €4,200.

The ARO has been estimated to be four times per year based on types of vulnerabilities and threats that are known and documented that relate to this type of server.

$$ARO = 4 / year$$

This information is obtained from cases around the world, documented publications etc.

$$ALE = SLE \; x \; ARO = € \, 4{,}200 \, x \, 4 = € \, 16{,}800$$

Having completed research into possible safeguards a firewall/IDS was chosen at a cost of €9,000 per year with service contract.

$$ACS = € \, 8{,}000$$

This system estimates a reduction in vulnerability of the system by 80% (0.2).

$$ALE(post) = ALE(prior) \, x \, 0.2 = € \, 16{,}800 \, x \, 0.2 = € \, 3{,}360$$

The CBA of the firewall/IDS can be obtained now.

$$CBA = (ALE(prior) - ALE(post)) - ACS = (€ \, 16{,}800 - € \, 3{,}360) - € \, 8{,}000 = € \, 5{,}440$$

$$CBA = € \, 5{,}440$$

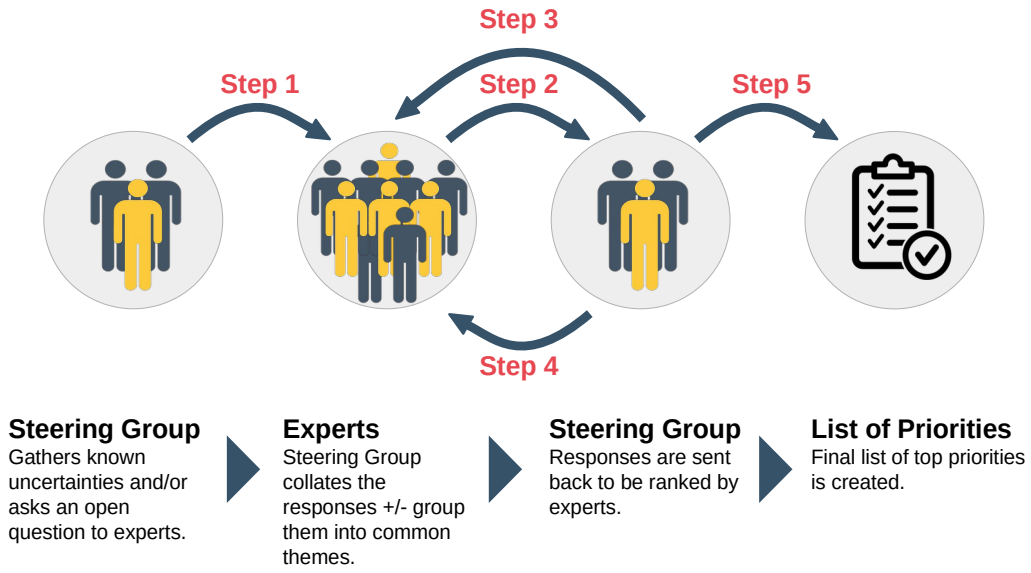
A €8,000 annual expense yields a €5,440 annual cost saving.

4.4.3 Qualitative

Qualitative Risk Analysis is a 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 such as the following are used to assess the risk and produce a Risk Registrar:

- Brainstorming
- Delphi Technique
- Storyboarding
- Focus Groups
- Surveys
- Questionnaires
- Check Lists
- Interviews

Delphi Technique



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

Figure 5: Delphi Technique

The Delphi Technique is a systematic, interactive forecasting method which relies on a panel of experts. The experts answer questionnaires in two or more rounds. After each round, a steering group provides an anonymous summary of the experts' forecasts from the previous round as well as the reasons they provided for their judgements. Thus, experts are encouraged to revise their earlier answers in light of the replies of other members of their panel. It is believed that during this process the range of the answers will decrease and the group will converge towards the "*correct*" answer. Finally, the process is stopped after a pre-defined stop criterion (e.g. number of rounds, achievement of consensus, stability of results) and the mean or median scores of the final rounds determine the results.

5 ISO 31000:2018 — Risk management

ISO 31000:2018, Risk management — Guidelines [2], is a global standard that provides a framework for managing risk. It is a generic standard, which means that it can be applied to any organisation regardless of size, industry, or sector. It provides a comprehensive approach to risk management, including guidance on how to identify, assess, treat, and monitor risks.

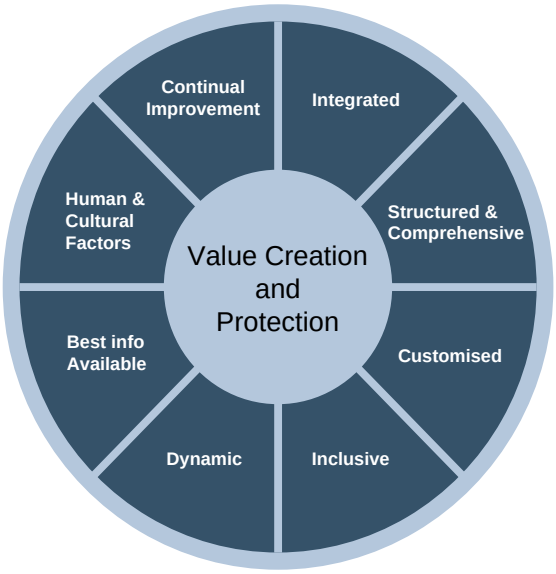


Figure 6: ISO 31000:2018 Risk Management Principles

The standard is based on eight principles:

- **Integrated**: Risk management should be integrated into all organisational processes and activities.
- **Structured & Comprehensive**: Risk management should be systematic and thorough, covering all relevant risks and taking into account all relevant information.
- **Customised**: Risk management should be tailored to the specific needs and circumstances of the organisation.
- **Inclusive**: Risk management should involve all stakeholders, including employees, customers, suppliers, and regulators. This is important because stakeholders can provide valuable insights into the organisation's risks and can help to develop and implement effective risk management strategies.
- **Dynamic**: Risk management should be a dynamic process that is adapted to the changing needs of the organisation. This is important because risks can change over time due to factors such as new technologies, new competitors, and new regulations.
- **Best Information Available**: Risk management should be based on the best available information, including internal data and external sources.
- **Human and Cultural Factors**: Risk management should take into account human and cultural factors, such as the organisation's culture, values, and decision-making processes.
- **Continual improvement**: Risk management should be continually improved.

5.1 Risk Management Framework

Figure 7: ISO 31000:2018 Risk Management Framework

The ISO 31000 framework, as illustrated in Figure 7, consists of fundamental principles that underpin it and provide a guide to its implementation. Management and oversight bodies should ensure that risk management is integrated into all organisational activities and should demonstrate leadership and commitment by:

- Customising and implementing all components of the framework.
- Issuing a statement or policy that establishes a risk management approach, plan, or course of action.
- Ensuring that the necessary resources are allocated to managing risk.
- Assigning authority, responsibility, and accountability at appropriate levels within the organisation.

Leadership and commitment should be considered with these five elements that are interconnected and work together to support the overall goal of risk management, which is to reduce the likelihood and impact of negative events on the organisation's objectives.

- **Integration**: Risk management should be integrated into all organisational processes and activities. This requires support from stakeholders, particularly top management. Framework development encompasses integrating, designing, implementing, evaluating, and improving risk management across the organisation.
- **Design**: The design of the risk management framework should be tailored to the specific needs of the organisation. This includes considering the organisation's size, industry, complexity, and risk appetite.

- **Implementation**: The implementation of the risk management framework should be carried out in a way that is effective and efficient. This includes developing and implementing risk management processes, tools, and resources.
- **Evaluation**: The risk management framework should be evaluated on a regular basis to ensure that it is effective and efficient. This includes assessing the performance of the risk management processes, tools, and resources.
- **Improvement**: The risk management framework should be continually improved to ensure that it remains effective and efficient. This includes learning from experience and adopting new best practices.

Consider some examples of how the framework elements can be applied in practice. Management should establish a risk management committee and allocate the necessary resources to support the risk management programme.

- **Integration**: The risk management framework could be integrated into the organisation's strategic planning process and into the day-to-day operations of all departments.
- **Design**: The risk management framework could be designed to be flexible and adaptable to the changing needs of the organisation.
- **Implementation**: The risk management framework could be implemented through a phased approach, starting with the most critical areas.
- **Evaluation**: The risk management framework could be evaluated annually or more often, as needed.
- **Improvement**: The risk management framework could be improved by regularly reviewing and updating the risk management processes, tools, and resources.

Figure 8: ISO 31000:2018 Risk Management Process

5.2 Risk Management Process

The *ISO 31000:2018 Risk Management Process* is a five-step process that is used to identify, assess, treat, and monitor risks. Figure 8 illustrates the following steps, and the relationship between the steps, in the process:

- **Scope, Context, and Criteria**: The first step is to define the scope of the risk assessment, the context in which the risks are to be assessed, and the criteria that will be used to evaluate the risks. The scope should be defined based on the organisation's objectives and the risks that could impact those objectives. The context should include the organisation's internal and external environment, as well as its values and culture. The criteria should be used to evaluate the likelihood and impact of each risk, as well as its importance to the organisation.
- **Risk Assessment**: The risk assessment process involves identification, analysis, and evaluation of risks. This can be achieved using a variety of methods, such as brainstorming, risk checklists, and scenario analysis.
- **Risk Treatment**: Once the risks have been assessed, the organisation needs to decide how to treat them. There are a variety of risk treatment options available, such as avoidance, reduction, transfer, and acceptance. The organisation should choose the treatment option that is most appropriate for each risk, considering the cost, benefits, and other factors.

Through each of these steps there is the importance of communication, consultation, monitoring and review:

- **Communication and Consultation**: Communicate and consult with stakeholders to identify risks and understand their concerns. This can be done through interviews, workshops, surveys, or other methods. It is important to communicate and consult with stakeholders at all stages of the process to ensure that everyone is involved and informed. This will help to ensure that the risk management process is effective and that the risks are managed in a way that is acceptable to all stakeholders.
- **Monitoring and Review**: The risk management process is an ongoing process, so it is important to monitor and review risks on a regular basis. This will help to ensure that the organisation is aware of new risks and that the existing risks are being managed effectively.

5.3 ISO/IEC 31000:2018 Summary

The *ISO/IEC 31000:2018 Risk Management Process* is a flexible and adaptable framework that can be used by organisations of all sizes and in all industries. It can help organisations to identify, assess, treat, and monitor risks in a systematic and effective way.. Some of the benefits of using ISO 31000 are that it:

- helps organisations to identify and manage all of their risks, including those that are not immediately obvious.
- helps organisations to make more informed decisions about risk.
- help organisations to reduce the likelihood and impact of negative events.
- help organisations to achieve their objectives.
- It can improve the organisation's reputation and credibility.
- It can make the organisation more attractive to investors and customers.

ISO/IEC 31000 is a voluntary standard, but it is widely accepted and used by organisations worldwide. It is also recognised by many regulators and accreditation bodies.

6 Risk Management — NIST

The US National Institute of Standards and Technology have a number of documents that relate to Risk Management.

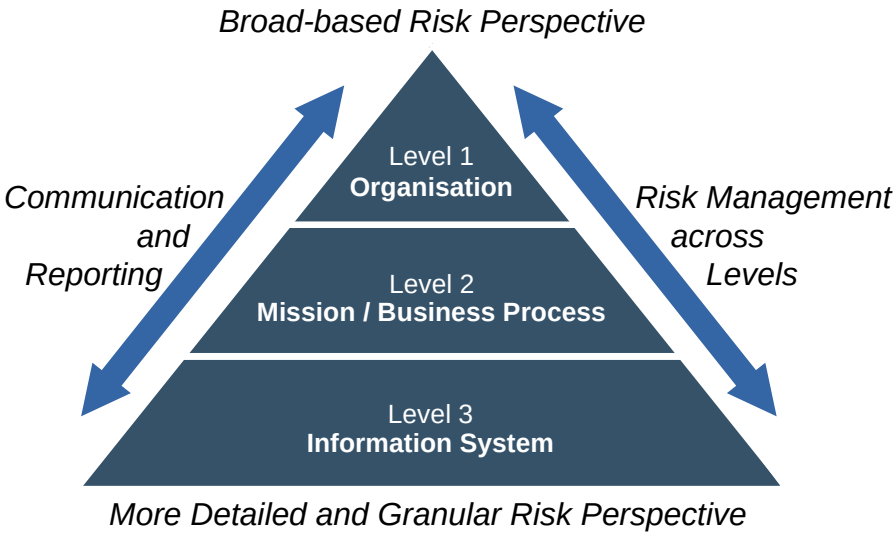


Figure 9: Organisation-wide Risk Management Approach

NIST SP 800-39: Managing Information Security Risk [3]: This publication is the foundational document. As illustrated in Figure 9, this document establishes the strategic framework and core principles for managing information security risk at three key levels:

- the organisational level,
- the mission/business process level, and
- the information system level.

It answers the *what* and *why* of risk management, defining the fundamental components and the hierarchy of risk.

NIST SP 800-30: Guide for Conducting Risk Assessments [4]**:** This document focuses on one specific, critical component of the overall risk management process: the risk assessment. It provides the detailed methodology, steps, and techniques for identifying, analysing, and evaluating risks. It acts as a *how-to* guide for a specific activity within the broader framework.

NIST SP 800-37r2: Risk Management Framework (RMF) [5]: This publication provides the end-to-end, comprehensive process for managing security and privacy risk throughout a system's life cycle. The RMF is the operational element that ties the strategic guidance of SP 800-39 with the detailed risk assessment methodology of SP 800-30 and other related publications.

From here this topic will focus on the third document, the NIST RMF.

6.1 NIST Risk Management Framework

The RMF [5] is a structured, seven-step process developed to guide federal agencies and other organisations in managing security and privacy risks for their information systems.

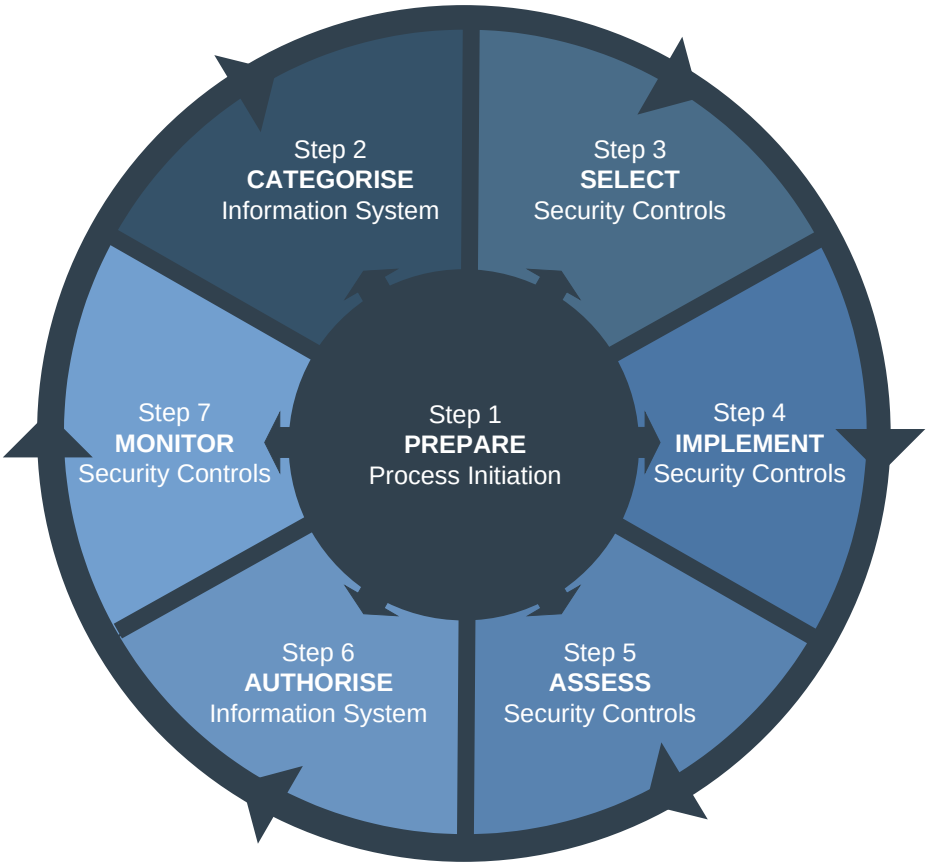


Figure 10: NIST SP 800-53r5 RMF Steps

The RMF is a **comprehensive, flexible, and repeatable approach** that integrates security and privacy into the system development life cycle. It's designed to help organisations make informed, risk-based decisions about which systems to authorise for operation.

The seven steps of the RMF, as illustrated in Figure 10, are:

1. **Prepare:** Establishes a foundation for managing security and privacy risks at an organisational and system level.
2. **Categorise:** Classifies the information system and the data it processes based on a potential impact analysis.
3. **Select:** Chooses a baseline set of security and privacy controls from NIST's extensive catalogue (NIST SP 800-53 [6]) and customises them to the specific needs of the system.
4. **Implement:** Puts the selected controls into practice and documents how they are deployed.
5. **Assess:** Evaluates the controls to determine if they are implemented correctly, operating as intended, and producing the desired security outcomes.

6. **Authorise:** A senior official makes a risk-based decision to authorise the system to operate, accepting the remaining (residual) risk.
7. **Monitor:** Continuously tracks the security and privacy posture of the system, including its controls and risks, and makes ongoing adjustments as needed.

While the RMF was initially developed for US federal agencies, its systematic and risk-based approach has made it a widely adopted standard for cybersecurity and privacy risk management across various sectors and organisations of all sizes.

6.2 PREPARE Tasks

These tasks, listed in Table 1, are essential activities at the organisational level to help prepare the organisation to manage its security and privacy risks using the RMF.

Table 1: PREPARE Tasks and Outcomes — Organisational Level

Nr.	Task	Outcomes	CSF ID
P-1	Risk Management Roles	Individuals are identified and assigned key roles for executing the RMF.	ID.AM-6; ID.GV-2
P-2	Risk Management Strategy	A risk management strategy for the organisation that includes a determination and expression of organisational risk tolerance is established.	ID.RM; ID.SC
P-3	Risk Assessment — Organisation	An organisation-wide risk assessment is completed or an existing risk assessment is updated.	ID.RA; ID.SC-2
P-4	Organisationally-Tailored Control, Baselines and CSF, Profiles (Optional)	Organisationally-tailored control baselines and/or CSF Profiles are established and made available.	Profile
P-5	Common Control Identification	Common controls that are available for inheritance by organisational systems are identified, documented, and published.	
P-6	Impact-Level Prioritisation (Optional)	A prioritisation of organisational systems with the same impact level is conducted.	ID.AM-5
P-7	Continuous Monitoring Strategy — Organisation	An organisation-wide strategy for monitoring control effectiveness is developed and implemented.	DE.CM; ID.SC-4

RMF PREPARE Systems level tasks and expected outcomes are listed in Table 2.

Table 2: PREPARE Tasks and Outcomes — Systems Level

Nr.	Task	Outcomes	CSF ID
P-8	Mission or Business Focus	Missions, business functions, and mission/business processes that the system is intended to support are identified.	Profile; Implementation Tiers; ID.BE
P-9	System Stakeholders	The stakeholders having an interest in the system are identified.	ID.AM; ID.BE
P-10	Asset Identification	Stakeholder assets are identified and prioritised.	ID.AM
P-11	Authorisation Boundary	The authorisation boundary (i.e., system) is determined.	
P-12	Information Types	The types of information processed, stored, and transmitted by the system are identified.	ID.AM-5
P-13	Information Lifecycle	All stages of the information life cycle are identified and understood for each information type processed, stored, or transmitted by the system.	ID.AM-3; ID.AM-4
P-14	Risk Assessment — System	A system-level risk assessment is completed or an existing risk assessment is updated.	ID.RA; ID.SC-2
P-15	Requirements Definition	Security and privacy requirements are defined and prioritised.	ID.GV; PR.IP
P-16	Enterprise Architecture	The placement of the system within the enterprise architecture is determined.	
P-17	Requirements Allocation	Security and privacy requirements are allocated to the system and to the environment in which the system operates.	ID.GV
P-18	System Registration	The system is registered for purposes of management, accountability, coordination, and oversight.	ID.GV

6.3 CATEGORISE Tasks

These tasks, listed in Table 3, inform organisational risk management processes and tasks by determining the adverse impact to organisational operations and assets, individuals, other organisations, and the state with respect to the loss of CIA of organisational systems and the information processed, stored, and transmitted by those systems.

Table 3: CATEGORISE Tasks and Outcomes

Nr.	Task	Outcomes	CSF ID
C-1	System Description	The characteristics of the system are described and documented.	Profile
C-2	Security Categorisation	A security categorisation of the system, including the information processed by the system represented by the organisation-identified information types, is completed.	ID.AM-1; ID.AM-2; ID.AM-3; ID.AM-4; ID.AM-5
		Security categorisation results are documented in the security,privacy, and supply chain risk management plans.	Profile
		Security categorisation results are consistent with the enterprise architecture and commitment to protecting organisational missions, business functions, and mission/business processes.	Profile
		Security categorisation results reflect the organisation's risk management strategy.	
C-3	Security Categorisation Review and Approval	The security categorisation results are reviewed and the categorisation decision is approved by senior leaders in the organisation.	

6.4 SELECT Tasks

These tasks, listed in Table 4, select, tailor, and document the controls necessary to protect the information system and organisation commensurate with risk to organisational operations and assets, individuals, other organisations, and the state.

Table 4: SELECT Tasks and Outcomes

Nr.	Task	Outcomes	CSF ID
S-1	Control Selection	Control baselines necessary to protect the system commensurate with risk are selected.	Profile
S-2	Control Tailoring	Controls are tailored producing tailored control baselines.	Profile
S-3	Control Allocation	Controls are designated as system-specific, hybrid, or common controls.	
		Controls are allocated to the specific system elements (i.e., machine, physical, or human elements).	Profile; PR.IP
S-4	Documentation of Planned Control Implementations	Controls and associated tailoring actions are documented in security and privacy plans or equivalent documents.	Profile
S-5	Continuous Monitoring Strategy — System	A continuous monitoring strategy for the system that reflects the organisational risk management strategy is developed.	ID.GV; DE.CM
S-6	Plan Review and Approval	Security and privacy plans reflecting the selection of controls necessary to protect the system and the environment of operation commensurate with risk are reviewed and approved by the authorising official.	

6.5 IMPLEMENT Tasks

These tasks, listed in Table 5, implement the controls in the security and privacy plans for the system and for the organisation and to document in a baseline configuration, the specific details of the control implementation.

Table 5: IMPLEMENT Tasks and Outcomes

Nr.	Task	Outcomes	CSF ID
I-1	Control Implementation	Controls specified in the security and privacy plans are implemented.	PR.IP-1
		Systems security and privacy engineering methodologies are used to implement the controls in the system security and privacy plans.	PR.IP-2
I-2	Update Control Implementation Information	Changes to the planned implementation of controls are documented.	PR.IP-1
		The security and privacy plans are updated based on information obtained during the implementation of the controls.	Profile

6.6 ASSESS Tasks

These tasks, listed in Table 6, determine if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organisation.

Table 6: ASSESS Tasks and Outcomes

Nr.	Task	Outcomes	CSF ID
A-1	Assessor Selection	An assessor or assessment team is selected to conduct the control assessments.	
		The appropriate level of independence is achieved for the assessor or assessment team selected.	
A-2	Assessment Plan	Documentation needed to conduct the assessments is provided to the assessor or assessment team.	
		Security and privacy assessment plans are developed and documented.	
		Security and privacy assessment plans are reviewed and approved to establish the expectations for the control assessments and the level of effort required.	
A-3	Control Assessments	Control assessments are conducted in accordance with the security and privacy assessment plans.	
		Opportunities to reuse assessment results from previous assessments to make the risk management process timely and cost-effective are considered.	
		Use of automation to conduct control assessments is maximised to increase speed, effectiveness, and efficiency of assessments.	
A-4	Assessment Reports	Security and privacy assessment reports that provide findings and recommendations are completed.	
A-5	Remediation Actions	Remediation actions to address deficiencies in the controls implemented in the system and environment of operation are taken.	
		Security and privacy plans are updated to reflect control implementation changes made based on the assessments and subsequent remediation actions.	Profile
A-6	Plan of Action and Milestones	A plan of action and milestones detailing remediation plans for unacceptable risks identified in security and privacy assessment reports is developed.	ID.RA-6

6.7 AUTHORISE Tasks

These tasks, listed in Table 7, provide organisational accountability by requiring a senior management official to determine if the security and privacy risk (including supply chain risk) to organisational operations and assets, individuals, other organisations, or the State based on the operation of a system or the use of common controls, is acceptable.

Table 7: AUTHORISE Tasks and Outcomes

Nr.	Task	Outcomes	CSF ID
R-1	Authorisation Package	An authorisation package is developed for submission to the authorising official.	
R-2	Risk Analysis and Determination	A risk determination by the authorising official that reflects the risk management strategy including risk tolerance, is rendered.	
R-3	Risk Response	Risk responses for determined risks are provided.	ID.RA-6
R-4	Authorisation Decision	The authorisation for the system or the common controls is approved or denied.	
R-5	Authorisation Reporting	Authorisation decisions, significant vulnerabilities, and risks are reported to organisational officials.	

6.8 MONITOR Tasks

These tasks, listed in Table 8, maintain an ongoing situational awareness about the security and privacy posture of the information system and the organisation in support of risk management decisions.

Table 8: MONITOR Tasks and Outcomes

Nr.	Task	Outcomes	CSF ID
M-1	System and Environment Changes	The information system and environment of operation are monitored in accordance with the continuous monitoring strategy.	DE.CM; ID.GV
M-2	Ongoing Assessments	Ongoing assessments of control effectiveness are conducted in accordance with the continuous monitoring strategy.	ID.SC-4
M-3	Ongoing Risk Response	The output of continuous monitoring activities is analysed and responded to appropriately.	RS.AN
M-4	Authorisation Package Updates	Risk management documents are updated based on continuous monitoring activities.	RS.IM
M-5	Security and Privacy Updates	A process is in place to report the security and privacy posture to the authorising official and other senior leaders and executives.	
M-6	Ongoing Authorisation	Authorising officials conduct ongoing authorisations using the results of continuous monitoring activities and communicate changes in risk determination and acceptance decisions.	
M-7	System Disposal	A system disposal strategy is developed and implemented, as needed.	

6.9 NIST SP 800-37 Rev. 2 Summary

NIST SP 800-37 RMF, provides a structured, flexible, and repeatable process for managing security and privacy risks for information systems and organisations. The framework is designed to be a "system life cycle approach" that integrates security and privacy into every phase of a system's development. It is widely used, particularly by US federal agencies, but can be adapted by organisations of all sizes and types.

Some of the key benefits of using the NIST RMF are that it:

- Provides a disciplined, structured, and flexible process for managing security and privacy risks.
- Encourages a proactive approach by integrating security and privacy into the early stages of a system's lifecycle.
- Promotes near real-time risk management and continuous monitoring, allowing for a more dynamic and responsive security posture.
- Helps organisations make more informed and cost-effective decisions about risk.
- Establishes clear responsibility and accountability for security controls.
- Facilitates compliance with various regulatory requirements and improves an organisation's overall security posture.

The NIST RMF is a seven-step process: Prepare, Categorise, Select, Implement, Assess, Authorise, and Monitor. While not a mandatory standard for all organisations, it is a highly respected framework for any organisation seeking to build a robust and comprehensive risk management programme.

7 Compare Risk Frameworks

ISO/IEC 31000 and NIST SP 800-37, Rev 2, are both widely respected frameworks for managing risk within an organisation, but they are designed for different purposes and audiences. While both aim to help organisations make informed decisions about risk, they do so through distinct approaches. Table 9 highlights the key differences between these two frameworks, from their general scope and approach to their specific core components and compliance requirements.

Table 9: Risk Frameworks comparison

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.

7.1 Other Risk Management Frameworks

There are several other sources of risk management frameworks, particularly in the context of OT. OT environments, such as those found in manufacturing, critical infrastructure, and Automation and Control Systems (ACS), have different priorities than traditional IT, prioritising Safety and Availability above Integrity and Confidentiality. This has led to the development of specialised frameworks.

Here are some of the most notable ones that will be discussed in later topics in some detail:

- **ISA/IEC 62443** [8]: This is a series of internationally recognised standards that address the cybersecurity of ACS. It provides a comprehensive framework for securing these systems throughout their lifecycle. Unlike some other frameworks, it defines requirements for different roles, including asset owners, system integrators, and product suppliers, promoting a shared responsibility model for security. It is highly regarded and often seen as the foundational standard for OT cybersecurity.
- **ISO/IEC 27001** [9]: While ISO/IEC 27001 is a general information security management standard, it can be applied to OT environments. The framework's risk-based approach allows organisations to identify and manage the unique risks associated with OT systems. Organisations can use the ISO 27001 framework to establish a formal Information Security Management System (ISMS) that is tailored to their specific OT environment, integrating security policies, processes, and controls.
- **COBIT** [10]: The Control Objectives for Information and Related Technologies (COBIT) framework is a governance and management framework for enterprise IT. While not specifically an OT framework, its principles of linking business goals to IT goals and providing a structured approach to governance can be adapted for OT. It can be particularly useful for organisations considering bridging the gap between their IT and OT departments to create a unified governance structure.

8 Risk Management Plan

A Risk Management Plan (RMP) is a document that describes the risks associated with a product, service, or project, and the actions that will be taken to mitigate those risks. RMPs are commonly used in a variety of industries, including healthcare, OT industries and organisations as well as IT.

An RMP typically includes sections similar to:

- **Risk Identification**: Identifies the potential risks associated with the product, service, or project. Risks can be identified through brainstorming, interviews, and data analysis.
- **Risk Assessment/Analysis**: Assesses the likelihood and impact of each risk. The likelihood of a risk is the probability that it will occur, and the impact of a risk is the severity of the consequences if it does occur.
- **Risk Mitigation/Treatment**: Describes the actions that will be taken to mitigate each risk. Risk mitigation strategies can include avoiding the risk, reducing the likelihood of the risk, reducing the impact of the risk, and transferring the risk to a third party.
- **Risk monitoring**: Describes how the risks will be monitored and managed over time. This is important because risks can change over time, and new risks may emerge.
- **Risk review**: Describes how the RMP is evaluated for its effectiveness of risk management controls and identifying areas for continual improvement.

RMPs are living documents that should be updated regularly as new information becomes available and as the product, service, or project changes. These headings are generic and will need to be altered depending on the particular RMF that is employed. This can be seen in the following example aligned to NIST RMF.

8.1 Simplified Risk Management Plan

Consider a manufacturing company RMP aligned with ISO/IEC 31000:2018. The framework emphasises an integrated, cyclical, and continual process rather than a linear one. It also introduces the concept of *context* as a foundational element.

Risk Management Process for a Manufacturing Company's Assembly Line

This framework provides a structured approach for managing risks associated with the company's assembly line operations, ensuring the safety of personnel, quality of products, and reliability of production.

1. Establish the Context

Before identifying any risks, the internal and external environment in which the assembly line operates must be understood. This sets the scope and criteria for the entire risk management process.

- **Internal Context:** Define the organisation's objectives for the assembly line (e.g., target production volume, quality standards, safety goals). Identify internal stakeholders, the organisational culture, and the existing policies and procedures.
- **External Context:** Consider external factors such as market demands, regulatory requirements (e.g., Occupational Safety and Health Framework Directive [7], supply chain dependencies, and technological advancements.
- **Risk Criteria:** Define the criteria for evaluating risk. This includes defining the acceptable level of risk (risk appetite), the scales for likelihood and impact, and how risk priority will be determined (e.g., using a probability and impact matrix).

2. Risk Assessment

This phase is a systematic process of identifying, analysing, and evaluating risks.

- **Risk Identification:** Proactively identify all risks that could impact the assembly line's objectives.
    - **Safety Risks:** This includes identifying potential hazards like machinery accidents, ergonomic injuries from repetitive tasks or awkward positions, and exposure to hazardous materials (chemicals, fumes, dust).
    - **Quality Risks:** Identify risks that could lead to product defects or require product recalls.
    - **Operational Risks:** This involves identifying risks to production schedules, such as equipment failures, material shortages, and disruptions in the supply chain.
    - **Asset-Specific Risks:** Identify risks to specific assets, such as the assembly line machinery itself, and the raw materials used.

- **Risk Analysis:** Analyse the identified risks to understand their nature and characteristics.
    - **Determine Likelihood and Impact:** For each risk, estimate the probability of it occurring and the potential consequence if it does.
        - *Example:* The risk of a machinery accident might be analysed as having a **"High"** likelihood and a **"High"** impact on personnel safety and production.
        - *Example:* The risk of a product recall might be analysed as having a **"Low"** likelihood but a **"High"** impact on the company's reputation and finances.
    - **Review Existing Controls:** Analyse the effectiveness of any controls already in place to manage these risks.
- **Risk Evaluation:** Compare the results of the risk analysis against the risk criteria established in the context phase.
    - **Prioritise Risks:** Determine which risks require treatment and which can be accepted based on their priority rating (e.g., High, Medium, Low). The risk of a machinery accident, with a high priority rating, will require immediate and active treatment.

3. Risk Treatment

This phase involves developing and implementing a plan to modify the risks.

- **Select Risk Treatment Options:** For each risk that is not acceptable, choose one or more appropriate treatment options.
    - **Avoid the Risk:** Stop engaging in the activity that causes the risk (e.g., discontinue the use of a particularly dangerous machine).
    - **Modify the Risk (Mitigation):** Implement controls to reduce the likelihood or impact of the risk.
        - *Example:* To mitigate machinery accidents, implement engineering controls like machine guarding, provide mandatory safety training, and develop a clear accident response plan.
        - *Example:* To mitigate ergonomic risks, provide training on proper posture and implement job rotation to reduce repetitive motion.
        - *Example:* To mitigate exposure to hazardous materials, use engineering controls like ventilation systems and provide Personal Protective Equipment (PPE) to all employees.
    - **Transfer the Risk:** Share the risk with another party (e.g., purchase insurance to cover product recall costs).
    - **Accept the Risk:** For risks that fall within the organisation's risk appetite, make a formal decision to accept the residual risk and continue operations.

4. Monitoring and Review

This is a continuous and cyclical process that ensures the risk management framework remains effective.

- **Monitor Risks:** Continuously observe the identified risks and the effectiveness of the implemented controls. Track key risk indicators and watch for emerging threats.
- **Review the RMP:** Periodically review the entire risk management process to ensure its continuing suitability, adequacy, and effectiveness. This review should be triggered by significant changes to the assembly line, new products, or a major incident.
- **Communicate and Consult:** Maintain ongoing communication with all stakeholders (e.g., employees, managers, suppliers) to ensure they are aware of the risks and the controls in place, and to gather their feedback for continual improvement.

8.2 OT Risk Management Plan

The following framework outlines the process for managing cybersecurity and privacy risks associated with the organisation's OT systems, such as wind farms. This example is aligned with NIST SP 800-37r2 RMF.

Step 1: PREPARE

This initial step is to prepare for the risk management process at the organisational and system level.

- **Organisational-Level Activities**
  - **Define the Risk Management Strategy:** Establish the organisation's risk appetite, risk tolerance, and overall risk management policy.
  - **Frame the Risk:** Identify the threats, vulnerabilities, and potential impacts that are relevant to the OT environment.
  - **Establish the Common Control Strategy:** Define a strategy for using common security and privacy controls across all OT systems.
- **System-Level Activities (Asset Identification)**
  - **Identify System Boundaries:** Clearly define the assets, people, and processes that are part of the OT system (e.g., wind farm turbines, SCADA systems, remote monitoring stations).
  - **Identify Key Stakeholders:** Determine which personnel are involved in the operation and maintenance of the wind farms and who has responsibility for risk management.

Step 2: CATEGORISE

This step is about categorising the system and the information it processes based on impact.

- **Categorise the OT System:** Determine the potential impact on the organisation's mission, assets, and reputation if the confidentiality, integrity, or availability of the OT system and its data were compromised.
  - *Example:* An OT system for a wind farm might be categorised as having a **"high"** impact on Availability and a **"moderate"** impact on Integrity, as a loss of control could lead to equipment damage and a loss of power generation.
- **Document the System Description:** Formally describe the system's purpose, architecture, and the types of data it handles.

Step 3: SELECT

This step involves selecting the appropriate security and privacy controls to manage the identified risks.

- **Select Controls:** Choose a baseline set of security and privacy controls from NIST SP 800-53, tailored to the system's categorisation level (e.g., High-impact baseline).
- **Tailor the Controls:** Customise the selected controls to fit the specific needs and context of the OT environment, removing controls that are not applicable and adding others where necessary (e.g., specific controls for industrial control systems).
- **Develop the System Security Plan:** Create a formal document that details the selected controls and how they will be implemented.

Step 4: IMPLEMENT

This step focuses on implementing the security controls defined in the System Security Plan.

- **Implement Controls:** Deploy the chosen controls for the OT system. This could include physical security measures, network segmentation, access control policies, data encryption, and installing Intrusion Detection and Prevention Systems (IDS/IPS) and Security Information and Event Management (SIEM) systems where appropriate.

Step 5: ASSESS

This step is about assessing the implemented controls to determine if they are working correctly and effectively.

- **Assess Controls:** Conduct a formal security assessment to determine if the implemented controls are working as intended and meeting the requirements of the System Security Plan.
- **Identify Vulnerabilities:** During the assessment, identify any vulnerabilities or control deficiencies that could lead to an unacceptable level of risk.

Step 6: AUTHORISE

This is the formal decision step where a senior management officer makes a determination about the system's security posture.

- **Prepare the Authorisation Package:** Assemble the necessary documentation, including the System Security Plan, the security assessment results, and a Plan of Action and Milestones (POAM) to address any identified weaknesses.
- **Determine Risk Acceptance:** The authorising officer reviews the package to determine if the residual risk (the risk remaining after controls are implemented) is acceptable based on the organisation's risk appetite.
- **Authorise the System:** The authorising officer formally grants an Authorisation to Operate (ATO), Authorisation to Use (ATU), or a similar decision, indicating that the system can be operated in its current state.

Step 7: MONITOR

This final step is a continuous process to monitor the system's security posture over its entire lifecycle.

- **Monitor Controls and Risk:** Continuously monitor the security controls to ensure they remain effective. This includes analysing data from IDS/IPS and SIEM systems.
- **Review and Update the Plan:** Regularly review the system's security plan, risk assessment, and control implementation to ensure they remain relevant in the face of evolving threats and changes to the system.
- **Respond to Events:** Establish a process to respond to security incidents and to take appropriate actions to mitigate their impact.
- **Update the Authorisation:** At predetermined intervals or after significant changes, the system's authorisation is reviewed and updated to ensure it still operates within the organisation's acceptable risk levels.

9 Bibliography

[1] NIST SP 800-30, 'Guide for Conducting Risk Assessments', National Institute of Standards and Technology, Oct. 2012. Accessed: Aug. 22, 2023. [Online]. Available: https://www.nist.gov/privacy-framework/nist-sp-800-30

[2] ISO 31000:2018, *ISO 31000:2018: Risk management — Guidelines*, Feb. 2018. Accessed: Oct. 10, 2023. [Online]. Available: https://www.iso.org/standard/65694.html

[3] 'NIST SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View', National Institute of Standards and Technology, Initial Public Draft NIST SP 800-39, Mar. 2011. Accessed: June 17, 2025. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-39

[4] 'NIST SP 800-30r1 Guide for Conducting Risk Assessments', National Institute of Standards and Technology, Initial Public Draft NIST SP 800-30 rev 1, Sept. 2012. Accessed: June 17, 2025. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-30r1

[5] 'NIST SP 800-37r2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy', National Institute of Standards and Technology, Initial Public Draft NIST SP 800-37 Rev. 2, Dec. 2018. Accessed: June 17, 2025. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-37r2

[6] 'NIST SP 800-53r5 Security and Privacy Controls for Information Systems and Organizations', National Institute of Standards and Technology, Initial Public Draft NIST SP 800-53 rev 5, Mar. 2025. Accessed: June 17, 2025. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-53r5

[7] Directive 89/391/EEC, *EU measures to encourage improvements in the safety and health of workers at work*. 1989. Accessed: Sept. 20, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:01989L0391-20081211

[8] P. Kobes, *Guideline Industrial Security: IEC 62443 is Easy*. HEYER, 2017. [Online]. Available: https://books.google.ie/books?id=uQEjtAEACAAJ

[9] *ISO/IEC 27001: 2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, Jan. 10, 2022. Accessed: Sept. 10, 2023. [Online]. Available: https://www.iso.org/standard/27001

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

This page is intentionally blank