Topic 5

Risk Management

Dr Diarmuid Ó Briain

Version: 2.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Dr Diarmuid Ó Briain

Table of Contents

Illustration Index

1 Objectives

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

- Understand the nature of Risk Management in Operational Technology (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.

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 five 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.

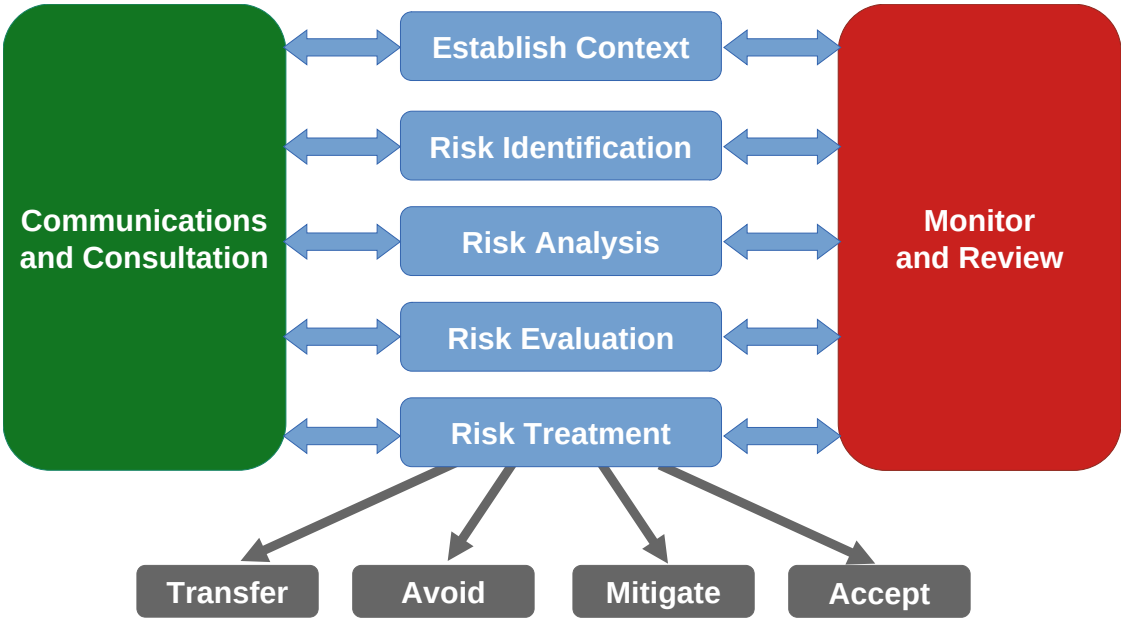

Figure 2: Risk Management Process

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.

Another source for a definition is *NIST SP 800-30 - Guide for Conducting Risk Assessments* [1] which defines a risk assessment as the determination of quantitative or qualitative value of risk related to a concrete situation and a recognised threat. It further outlines the Risk Assessment and Analysis process through the following steps:

- System Characterisation
- Thread Identification
- Vulnerability Identification
- Control Analysis
- Likelihood Determination
- Impact Analysis
- Risk Determination
- Control Recommendations
- Results Documentation.

4 Risk Mitigation

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 Log

The first step is to identify the organisations risks. Once the risks have been logged in a register, such as in Figure 3, 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 3: Risk Register

Use a Probability and Impact Matrix tool, such as that illustrated in Figure 4, 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.

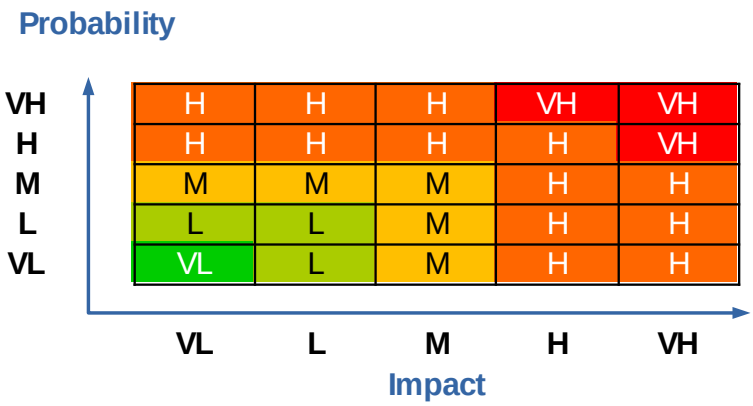

Figure 4: Probability and Impact Matrix Tool

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

4.2 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.

4.2.1 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?

4.2.2 Exposure Factor (EF)

Loss Potential or the percentage of loss an organisation would realise if a risk was realised.

4.2.3 Single Loss Expectancy (SLE)

The monetary value expected from the occurrence of a risk on an asset. It is:

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

4.2.4 Annualised Rate of Occurrence (ARO)

An estimate based on the data of how often a threat would be successful in exploiting a vulnerability.

4.2.5 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:

$$ALE = SLE \; x \; ARO$$

4.2.6 Annual Cost of Safeguard (ACS)

This is the cost of the researched safeguard.

4.2.7 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.

4.3 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.

4.3.1 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 Qualitative Risk Analysis

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

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 facilitator 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 Risk management — Guidelines

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.

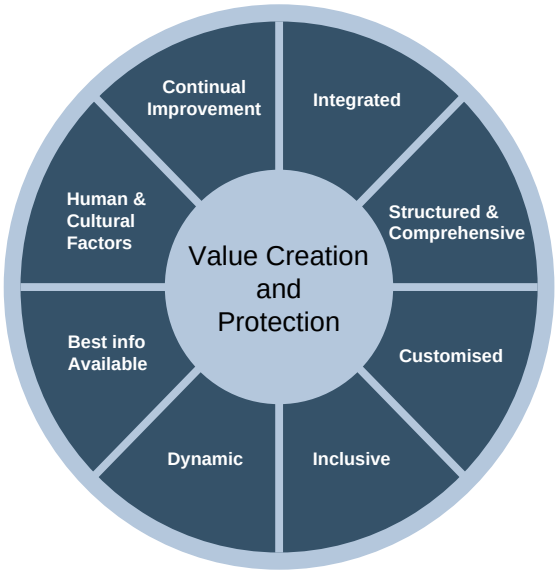

Figure 5: ISO 31000:2018 Risk Management Principles

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 6: ISO 31000:2018 Risk Management Framework

The ISO 31000 framework, as illustrated in Figure 6, 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 7: 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 7 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 ISO31000:2018 Summary

The *ISO 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 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 Plan (RMP)

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 such as:

- **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.

6.1 Simplified Risk Management Plan

Here is a simplified example of a RMP for a manufacturing company with an assembly line:

Risk Identification

- **Safety hazards**:
  - Machinery accidents
  - Ergonomic injuries
  - Exposure to hazardous materials
- **Quality hazards**:
  - Defects in products
  - Product recalls
- **Production hazards**:
  - Equipment failures
  - Material shortages
  - Supply chain disruptions

Assembly Line Specific Risks

In addition to the general risks listed above, there are some specific risks that are associated with assembly lines. These risks include:

- **Repetitive motion injuries**: Assembly line workers often perform the same repetitive tasks over and over again, which can lead to repetitive motion injuries.
- **Ergonomic hazards**: Assembly line workers may have to work in awkward or uncomfortable positions, which can lead to ergonomic hazards.
- **Exposure to hazardous materials**: Assembly line workers may be exposed to hazardous materials, such as chemicals, fumes, and dust.

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, while the risk of a product recall may be considered to be low probability and high impact.

Risk Mitigation

For each risk, a risk mitigation strategy should be developed. 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.

For example, to reduce the risk of a machinery accident, the company could implement machine guarding, provide training to employees on safety procedures, and have a plan in place to respond to accidents.

To mitigate the specific risks, the company could implement the following measures:

- Provide training to employees on ergonomics and how to prevent repetitive motion injuries.
- Implement engineering controls to reduce the risk of exposure to hazardous materials.
- Provide Personal Protective Equipment (PPE) to employees to protect them from exposure to hazardous materials.
- By identifying, assessing, and responding to risks, the manufacturing company can reduce the likelihood and impact of negative events. This can help to protect the safety of employees, ensure the quality of products, and maintain production schedules.

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.

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.

6.2 OT Risk Management Plan

The following **Risk Management Plan (RMP)** is proposed for the OT security programme:

Step 1: Asset Identification

The first step is to identify all of the assets that are part of the OT system. This includes people, processes and technology. For example what personnel are involved, what policies and procedures are in place to operate the wind farms and hardware, software and data are essential to running the the wind farms.

Step 2: Risk Identification

Once the assets have been identified, the next step is to identify the threats that could potentially impact those assets. Threats can be internal or external, and they can be intentional or unintentional.

Step 3: Risk Assessment

Once the threats have been identified, the next step is to assess the risks that these threats pose to the OT system. This involves considering the likelihood of each threat occurring and the impact that it would have if it did occur. To do this a Probability and Impact Matrix Tool is employed grading risks similar to the one in Figure 8:

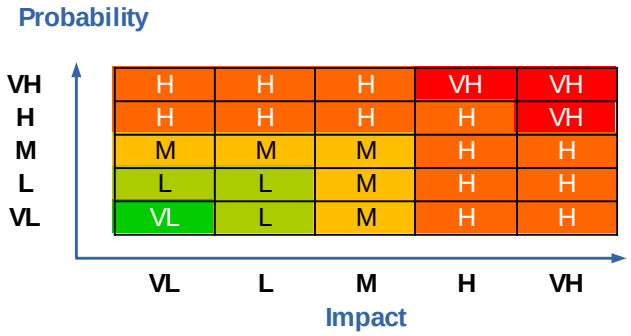

Figure 8: Probability and Impact Matrix Tool

Step 4: Risk Mitigation

Once the risks have been assessed, the next step is to mitigate the risks that are deemed to be unacceptable. This can be achieved by implementing a variety of security controls, such as access control, data encryption, and Intrusion Detection and Prevention Systems (IDS/IPS) and Security Information and Event Management (SIEM).

Step 5: Monitor and Review the RMP

The risk management plan should be monitored and reviewed on a regular basis to ensure that it remains effective against evolving threats.

7 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’. International Standards Organization, Feb. 2018. Accessed: Oct. 10, 2023. [Online]. Available: https://www.iso.org/standard/65694.html

This page is intentionally blank