CATAPULT
High Value Manufacturing

High Value Manufacturing Catapult

Summer 2022

Cyber Security Risk Assessment for Advanced Manufacturing

Authors

The following centres were directly involved in the creation and assembly of the Cyber Security Risk Assessment for Advanced Manufacturing:

- University of Sheffield Advanced Manufacturing Research Centre – AMRC
  Lead author: Narcisa Pinzariu
- Nuclear Advanced Manufacturing Research Centre – NAMRC
  Contributor: Dimitrios Anagnostakis

Acknowledgments

The project team would like to express their gratitude to all the representatives from the following centres of the High Value Manufacturing Catapult for taking the time to read through the work presented herein and provide invaluable feedback for its improvement:

- Advanced Forming Research Centre – AFRC
- Centre for Process Innovation – CPI
- Manufacturing Technology Centre – MTC
- National Composites Centre – NCC
- Warwick Manufacturing Group - WMG

Nomenclature

APT	Advanced Persistent Threats
BPCS	Basic Process Control System
CIA	Confidentiality, Integrity, Availability
CVE	Common Vulnerability and Exposure
DCS	Distributed Control System
DoS	Denial of Service
HIPAA	Health Insurance Portability and Accountability Act
I/O	Input/Output
IACS	Industrial Automation Control System
ICS	Industrial Control System
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention Systems
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
OT	Operation Technology
PIPEDA	Personal Information Protection and Electronic Documents Act
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information & Event Management
SIS	Safety Instrumented System
SUC	System Under Consideration
TTP	Tactics, Techniques and Procedures
USB	Universal Serial Bus
WLAN	Wireless Local Area Network

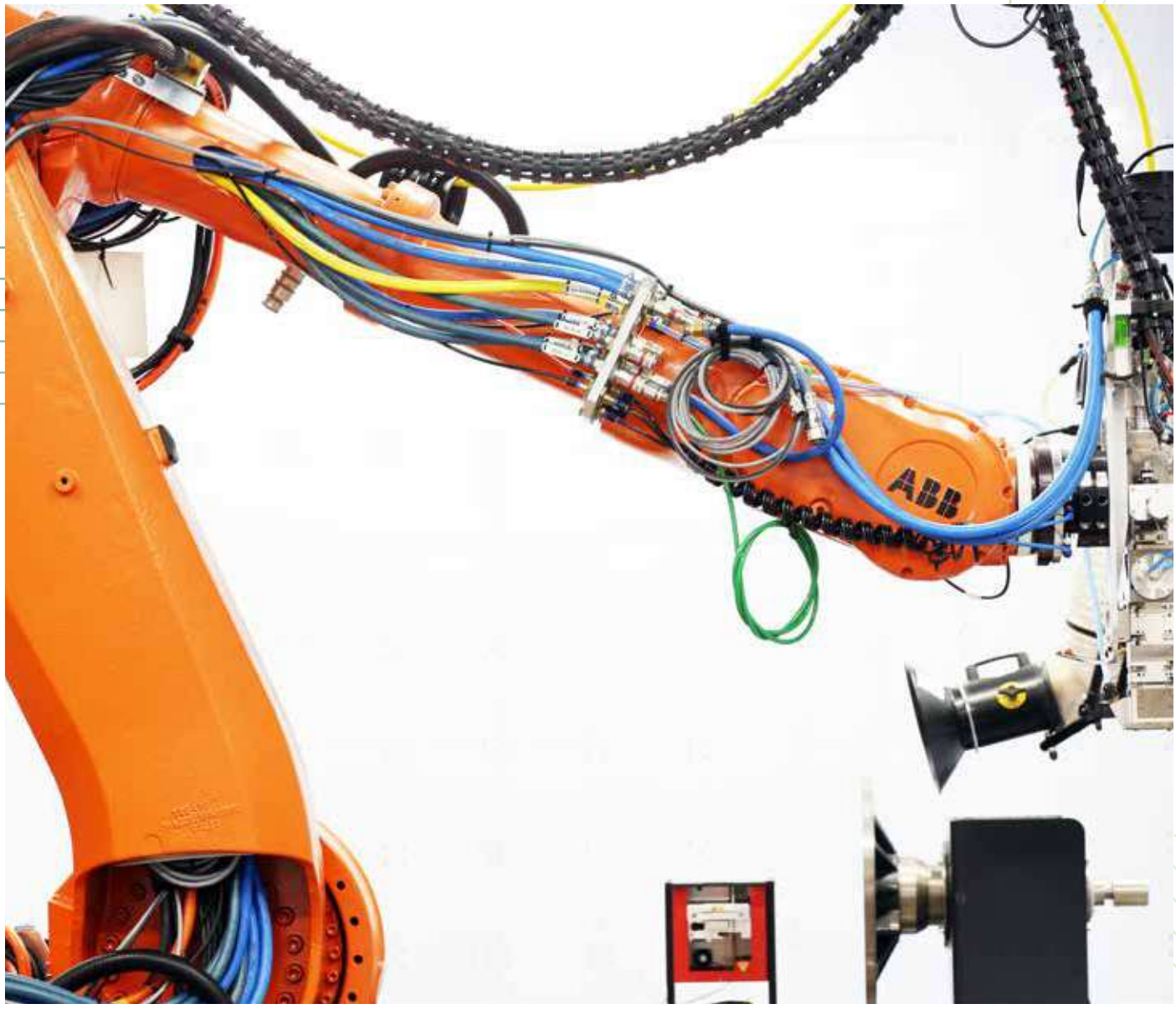


Table of contents

Authors 2
Acknowledgments 2
Nomenclature 3
Table of contents 4
List of figures 7
List of tables 7
1 Preface 8
2 Introduction 9
3 Understanding the system 10
3.1 Identifying the system under consideration 10
3.1.1 Defining the boundaries 11
3.2 Asset Discovery 12
3.3 Cyber Security Status & Baseline Security Criteria 14
3.3.1 Defining a system's baseline security criteria 15
4 Threat identification 17
4.1 Identification of threat sources 17
4.2 Identification of threat events 18
5 Vulnerabilities identification 19
6 Risk quantification 20
6.1 Determine likelihood 20
6.2 Determine severity 21
6.3 Risk calculation 23
7 Threat remediation and risk management 25
7.1 General preventive measures & security practices 25
7.1.1 Risk review 25
7.1.2 Training 26
7.1.3 Passwords & access control 27
7.1.4 Patch management 27
7.1.5 System partitioning & segmentation 27
7.2 Technical controls and countermeasures 28
7.2.1 Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS) 28
7.2.2 Security Information & Event Management (SIEM) 28
7.2.3 Firewalls 28
7.2.4 Malware & antivirus protection 29
7.3 Mitigation strategies & defence-in-depth 29
7.4 Residual risk & acceptable risk 30
7.4.1 Incident response and recovery Plan 30
8 Overview and reporting 31
8.1 Asset list 32
8.2 Asset topology diagrams 32
8.3 Risk registry 33
9 Conclusion 34

Table of contents (continued)

Appendices 35
Appendix 1A - Identifying the system under consideration & defining boundaries 35
Appendix 1B - Asset discovery 36
Appendix 1C - Cyber security status & baseline security criteria - Defining a systems current cyber security status 38
Appendix 2A - Threats identification and assessment 39
Appendix 2B - Threats sources identification 41
Appendix 2C - Threats events identification 45
Appendix 3A - Vulnerabilities and predisposing conditions identification 54
Appendix 3B - Further vulnerabilities assessment methods 58
Gap assessment 58
Penetration testing 59
Active and passive assessment 59
Appendix 4A - Risk quantification 60
Appendix 5A - Risk Review 61
Appendix 5B - Training 61
Appendix 5C - Passwords & access Control 62
Appendix 5D - Patch management 63
Appendix 5E - System partitioning & segmentation 64
Appendix 5F - Technical controls and countermeasures 65
Appendix 5F - Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS) 65
Appendix 5F - Security information & Event Management (SIEM) 65
Appendix 5F - Malware & antivirus protection 66
Appendix 5G - Mitigation strategies & defence-in-depth 66
Appendix 5H - Residual risk & acceptable Risk 66
Appendix 5I - Incident response and recovery plan 67

List of figures

Figure 1 Overview of cyber security risk assessment framework 9
Figure 2 Understanding the system - Identifying the system activity 10
Figure 3 Understanding the system - Setting the boundaries 11
Figure 4 Risk management hierarchy 11
Figure 5 Understanding the system - Asset discovery 12
Figure 6 Understanding the system - Determine the current security status 14
Figure 7 Understanding the system - Define the baseline security criteria 15
Figure 8 A perspective on how high and low cyber-risk tolerances impact technology usage [source] 15
Figure 9 Threats identification - Identify threat sources 17
Figure 10 Threats identification - Identify threat events 18
Figure 11 Vulnerabilities identification - Identify vulnerabilities & predisposing conditions 19
Figure 12 Risk quantification - Determine likelihood of threat/vulnerability 20
Figure 13 Risk quantification - Determine severity of threat/vulnerability 21
Figure 14 Risk quantification - Risk calculation 23
Figure 15 Threat remediation - Preventive measures and security practices 25
Figure 16 Threat remediation - Technical controls and countermeasures 28
Figure 17 Flowchart of the proposed risk assessment framework 31
Figure 18 Asset topology diagram example 32
Figure 19 Example of correct and wrong partitioning and segmentation of assets 64

List of tables

Table 1	Asset list template and relevant details required per item	13
Table 2	Factors to consider when defining the risk tolerance	16
Table 3	Example of a risk likelihood scale	21
Table 4	Example of a risk severity scale	22
Table 5	Example of a risk likelihood – severity matrix	24
Table 6	Recommended solution and strategies for Defence-in-Depth security	29
Table 7	Asset list template and relevant details required per item	32
Table 8	Example of a risk register	33
Table 9	Possible inputs to threat source identification task	41
Table 10	Taxonomy of threat sources	42
Table 11	Threat sources identification - characteristics of adversary capabilities	43
Table 12	Threat sources identification - characteristics of adversary intent	43
Table 13	Threat sources identification - characteristics of adversary targeting	44
Table 14	Threat sources identification - range of effects for non-adversarial sources	44
Table 15	Possible inputs for the threat identification task	46
Table 16	Examples of adversarial threat events	47
Table 17	Examples of non-adversarial threat events	52
Table 18	Identification of relevance of threat events to the organisation	53
Table 19	Possible inputs to the vulnerabilities and predisposing conditions identification	55
Table 20	Assessment scale for vulnerability's severity	56
Table 21	Taxonomy of predisposing conditions relevant to vulnerability	56
Table 22	Pervasiveness of predisposing conditions	57
Table 23	Example of a 3x3 risk matrix	60
Table 24	Example of a 5x5 risk matrix	60
Table 25	Example of a 5x5 risk matrix	61

1 Preface

The advent of Industry 4.0, and the ever-increasing pace of change in Information Technologies (IT) has led to an almost logarithmic increase of digital systems and hardware in global manufacturing and industry. As such the potential for harm, either malicious or accidental, is equally on the rise. Therefore, it is everyone's responsibility to educate themselves around cyber security.

> Cyber security's core function is to protect the devices we all use (smartphones, laptops, tablets and computers), and the services we access - both online and at work - from theft or damage. It's also about preventing unauthorised access to the vast amounts of personal information we store on these devices, and online.
>
> **[NCSC 2021]**

In manufacturing, Operating Technologies (OT) also make up a large percentage of assets found within a system or organisation. From the machining centres to the Internet of Things (IoT) and gateway devices, data and information are now at the core of the manufacturing industry. The HVMC looks to protect said data, information, and people within manufacturing and out into other industries via a range of technologies and methodologies. This creates a key role for Cyber Security.

The prevalence of OT/IT systems within the manufacturing industry means users must become well versed in Security Engineering. The goal of this manual is to act as an introduction or gateway to achieving this.

As such, a good Security Engineer should excel in critical and analytical thinking so that they can both; methodically identify weaknesses in any system and develop the best risk strategy for handling the weaknesses.

Starting from an IT perspective, the core of cyber security lies within a triangle linking confidentiality, integrity and availability (CIA). That is, all three aspects need to be maintained for the secure operation of an IT system. The terms are explained below.

- **Confidentiality:** refers to keeping sensitive data safe and protected from being stolen.
- **Integrity:** relates to the accuracy and completeness of data.
- **Availability:** is linked with proper functioning of a system such that data or information is available when needed

Cyber security aims to maintain the CIA within an IT system so that it behaves as it should do. Similarly, in a manufacturing environment and OT systems, the same CIA principle applies, but priority is given to availability as any downtime or unavailability within a system costs the manufacturer/organisation money. Therefore, cyber security in manufacturing aims to keep the systems available first, then operating correctly (integrity) and securely (confidentiality).

> A security system is only as strong as its weakest link.
>
> **[Anon]**

2 Introduction

The goal of this document is to demonstrate the importance of cyber security within a manufacturing context by providing a basic framework consisting of the steps required for completing a risk analysis and assessment of an OT system.

In this manner, core assets within a production environment should be protected and operating safely at a basic level. As such, by the end of this document, the reader should be able to:

Understand the systems and create an asset inventory and ownership list.

List known threats associated with the previously identified assets.

Identify and quantify how core cyber elements (confidentiality, integrity, availability) could be affected if a threat occurs or a vulnerability is exploited within the system.

Identify the current security controls that are in place and any additional controls that could be implemented to help mitigate risk within the system.

It is suggested that the above information should be made available to a single person or pre-determined group who will be in charge of risk calculation within the organisation. This allows for the risks to be managed centrally in a standardised format.

▶ **This manual will take you through all five steps for completing a cyber-security risk assessment of your system/s (see Figure 1).**

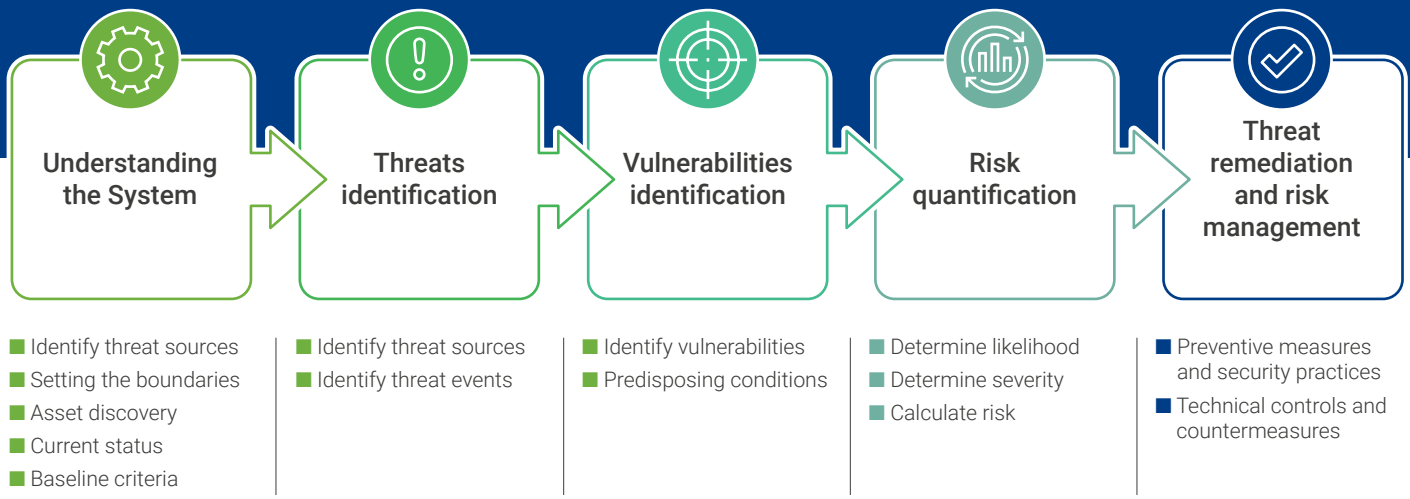


Figure 1 Overview of cyber security risk assessment framework

Before undertaking the risk assessment, it is important for an organisation or department to scope out and set the purpose of the assessment. It is critical to make some initial considerations around the organisation's existing policies and procedures particularly those concerning cybersecurity, budget planning and risk appetite. The risk assessment will then be aligned with the organisation's strategy and priorities. It can then be used to inform decisions regarding the next steps and actions needed to protect a system, and manage, control and mitigate the risks identified.

3 Understanding the system

This section provides guidance orientated towards the understanding of the system under consideration, what elements it may cover, and what information is necessary to collect in order to effectively identify the system under consideration and eventually perform a meaningful assessment.

3.1 Identifying the system under consideration

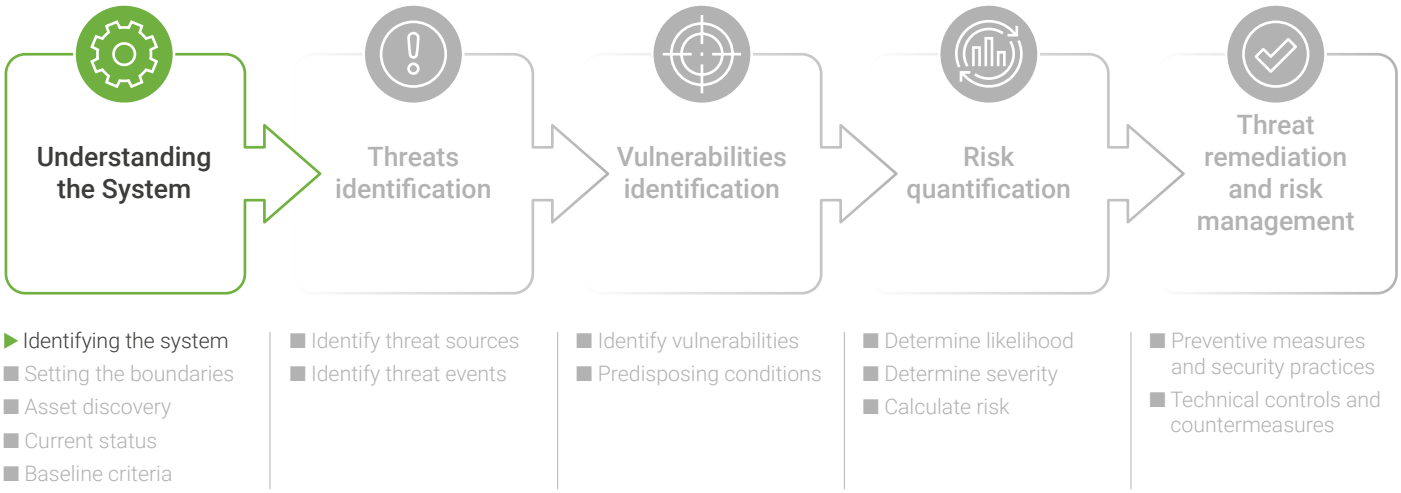


Figure 2 Understanding the system – Identifying the system activity

The first step when conducting a risk assessment is to identify the System Under Consideration (SUC) and set a clear definition of its security perimeter along with all access points to the system (Figure 2). Each access point on a SUC may constitute a potential entry point for a cyber-attack, while the contained sub-units of the SUC may present various vulnerabilities that can be exposed and used in the occurrence of a threat event.

How to identify the system under consideration

In an organisation usually, multiple control systems exist and operate, especially in larger industrial facilities. Each of these systems should be defined as a SUC.

In the definition of a SUC, all Industrial Automation Control Systems (IACS) assets required for a complete automation solution need to be included.

Key information useful for identifying all the relevant IACS components of a SUC can be drawn from the organisation's system inventory, architecture diagrams, network diagrams and dataflows.

A SUC may include various subsystems. Some examples of components to include on a SUC are:

- Basic process control systems (BPCSs)
- Distributed control systems (DCSs)
- Safety instrumented systems (SISs)
- Supervisory control and data acquisition (SCADA)
- IACS product supplier's packages

3.1.1 Defining the boundaries

This section provides guidance in defining the boundaries of the risk assessment around the identified System Under Consideration.

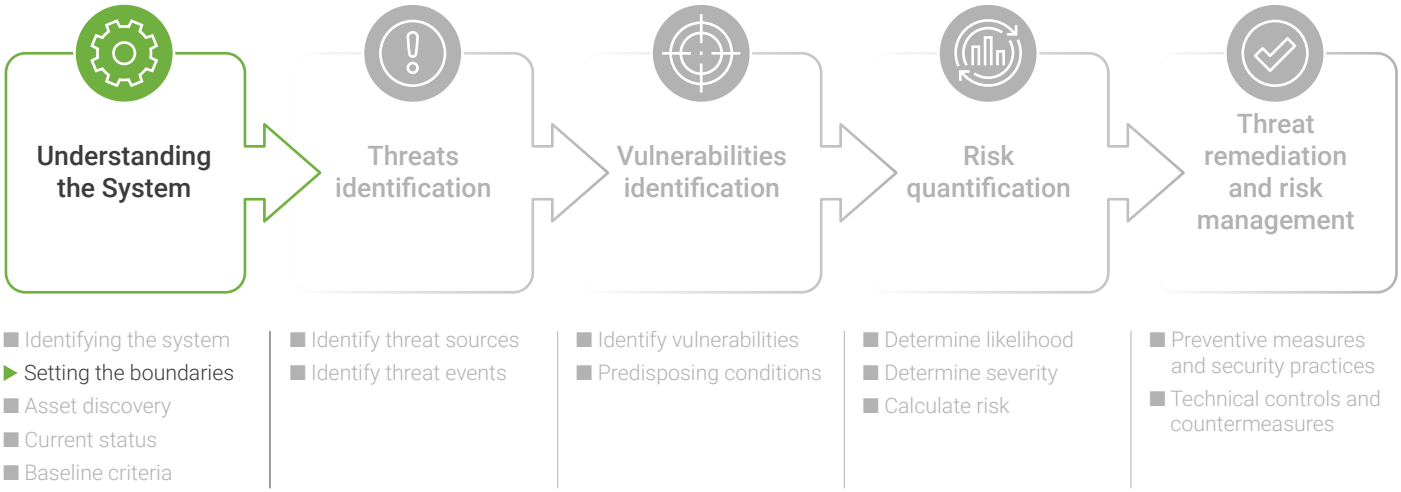


Figure 3 Understanding the system – Setting the boundaries

Risk assessments can be carried out at different levels (tiers) across a business, according to the standard NIST 800-30 (section 2.4, p17); the three layers are shown in Figure 4 below.

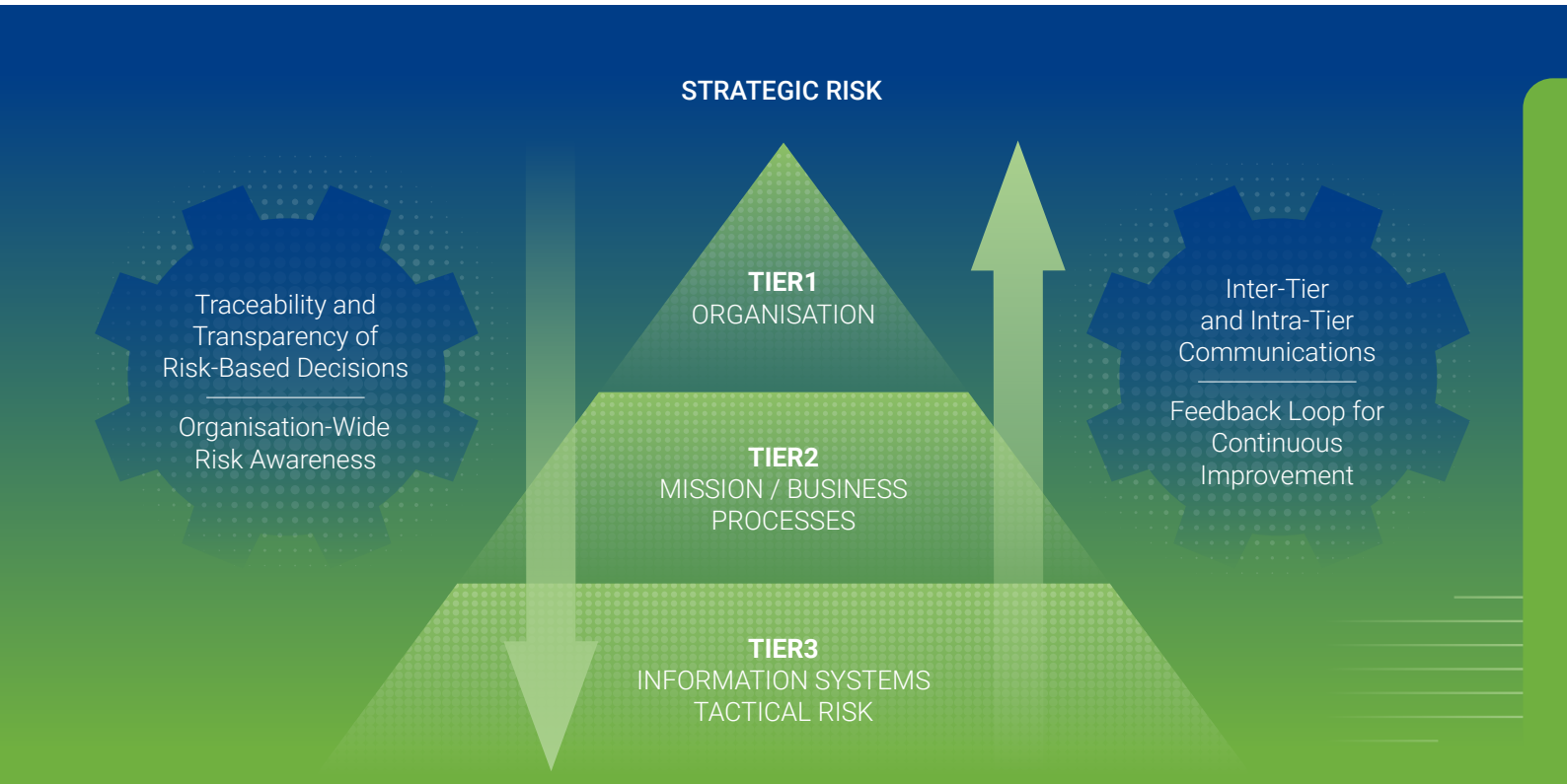


Figure 4 Risk management hierarchy ((NIST 800-30 (section 2.4, p17))

The definition of the boundaries of a risk assessment will facilitate the effective completion of it, limiting the length of the assessment only within the pre-set boundaries. It will also help in the identification of key personnel and information necessary for carrying out the assessment.

How to define the system's boundaries

The purpose of a risk assessment is to inform the task of setting the boundaries for the assessment. Key considerations to follow across each tier are suggested below:

Tier 1 – the risk assessment at this level may affect organisational decisions with regards to cyber security policies, programs and procedures as well as the risk response (risk tolerance, avoidance, mitigation, etc.) and investment decisions on IT systems and technologies.

Tier 2 – the risk assessment will support the protection of the processes, operation and resilience requirements aligned with the organisation's architectures. It may also inform decisions on the selection of common controls, suppliers, services and contractors.

Tier 3 – the risk assessment is conducted with the aim to inform decisions about design (selection and tailoring of security controls and systems), implementation (products' and systems' configuration to meet requirements) and operation (monitoring, upgrading and maintenance decisions) at the information system level.

▶ More information regarding this section can be found in Appendix 1A.

3.2 Asset Discovery

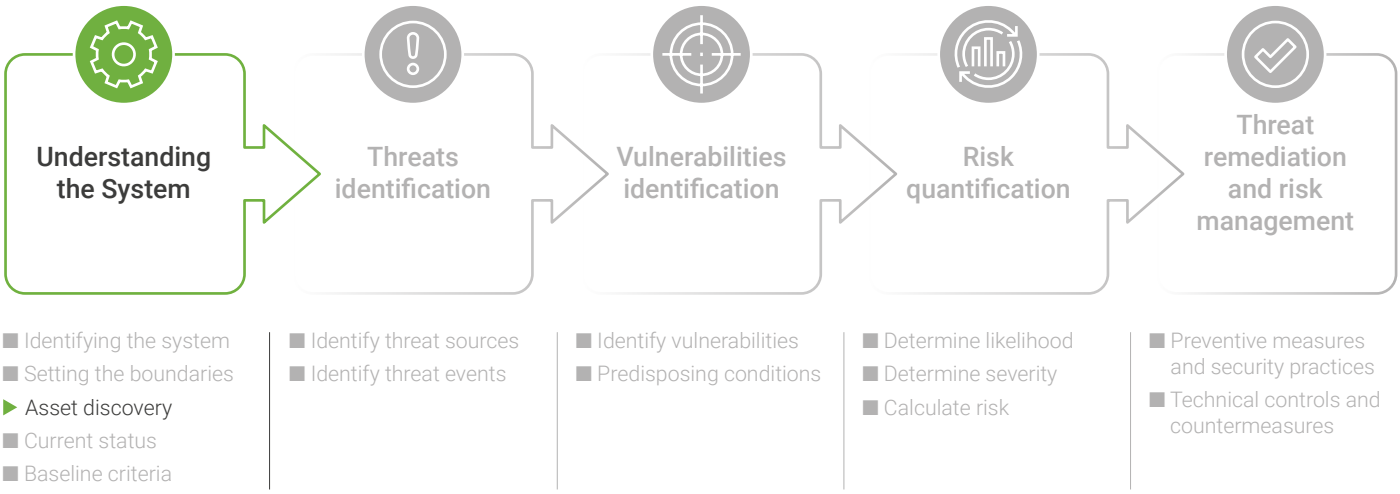


Figure 5 Understanding the system – Asset discovery

This section of the risk framework focuses on identifying all assets contained within the system under consideration including both information and physical assets (Figure 5).

This provides the system owner with an overview of all the assets within their system which is key to initially identifying and understanding risks within a system. Common asset types found within a typical system include:

- **Hardware** – IT servers, network equipment, workstations, mobile devices etc.
- **Software** – Purchased or bespoke software
- **Data** – Information or data in any format physical and/or digital
- **Services** – the actual service provided to end-users (e.g. database systems, e-mail etc.)
- **Locations & Buildings** – Sites, buildings, offices etc.
- **People** – Employees, temporary staff, contractors, volunteers etc.

How to discover assets

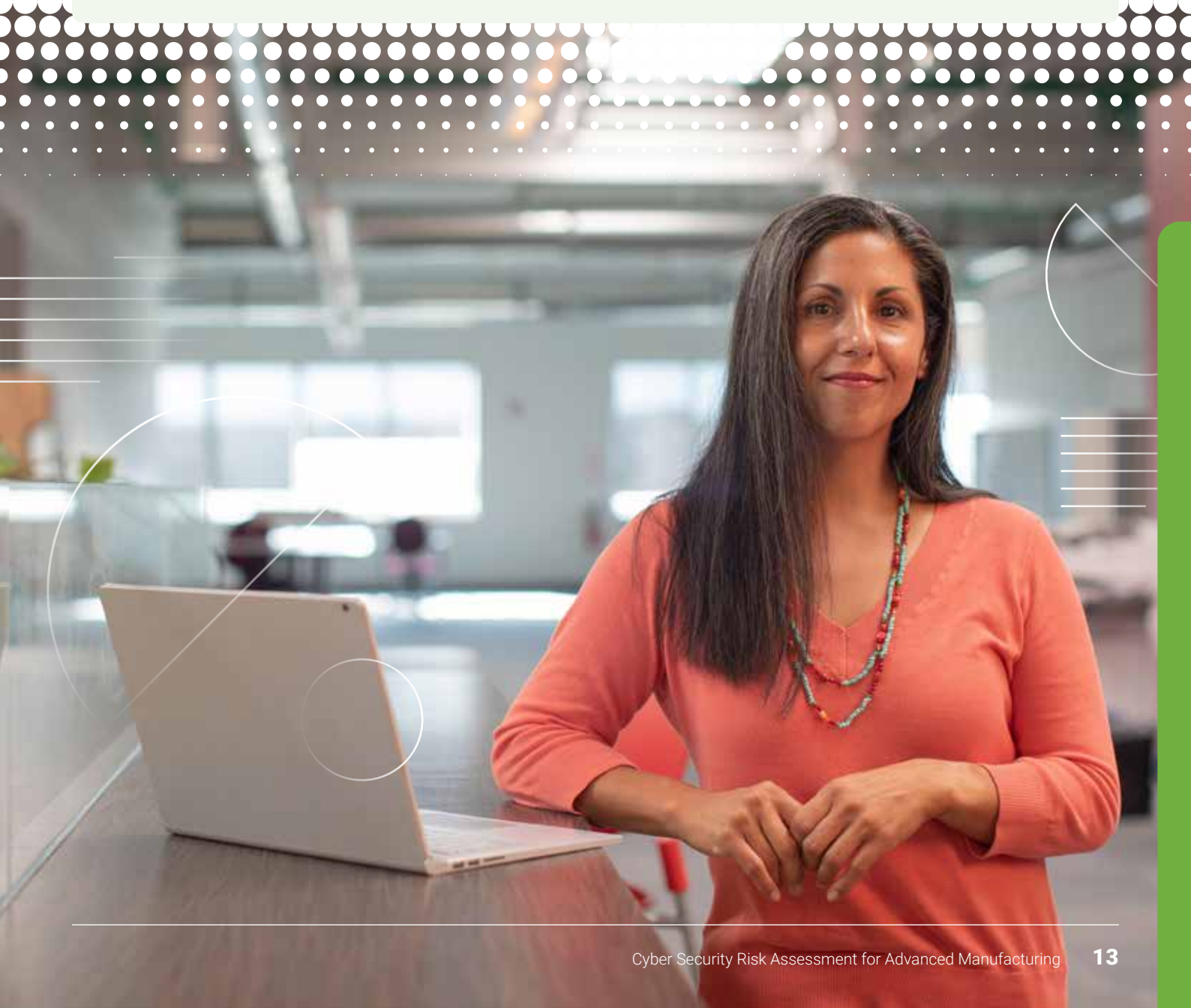
The most common method for recording and managing assets and the owners responsible for said assets is via an asset register and through relevant diagrams such as network and deployment diagrams. Table 1 below shows an example of an asset list and highlights the information that needs to be recorded.

Table 1 Asset list template and relevant details required per item

Asset Number	Asset Category	Manufacturer	Model/ Version	Serial No	Location	Existing connections	Asset Owner	Accessible Users	Operating System	Review Date
001										
002										
003										

▶ More information on this section can be found in Appendix 1B – Asset Discovery.

It is worth noting that the documentation produced within this section can contain information that is critical to the security of the asset or system. It is therefore important the produced documentation is kept in a secure location and is not distributed. For added security, the documentation should be password protected and encrypted, follow this guide for more information on how to do this within Windows and with Microsoft Office.



3.3 Cyber Security Status & Baseline Security Criteria

The final step in understanding the system under consideration is identifying the current security status of assets and the system as a whole as well as identifying the baseline security criteria of the business. This will be the first step in identifying risks within the system as it will provide the system owner with an understanding of where their system is at from a cyber-security perspective and whether it meets the business' cyber security criteria.

1.1.1. Defining a system's current cyber security status

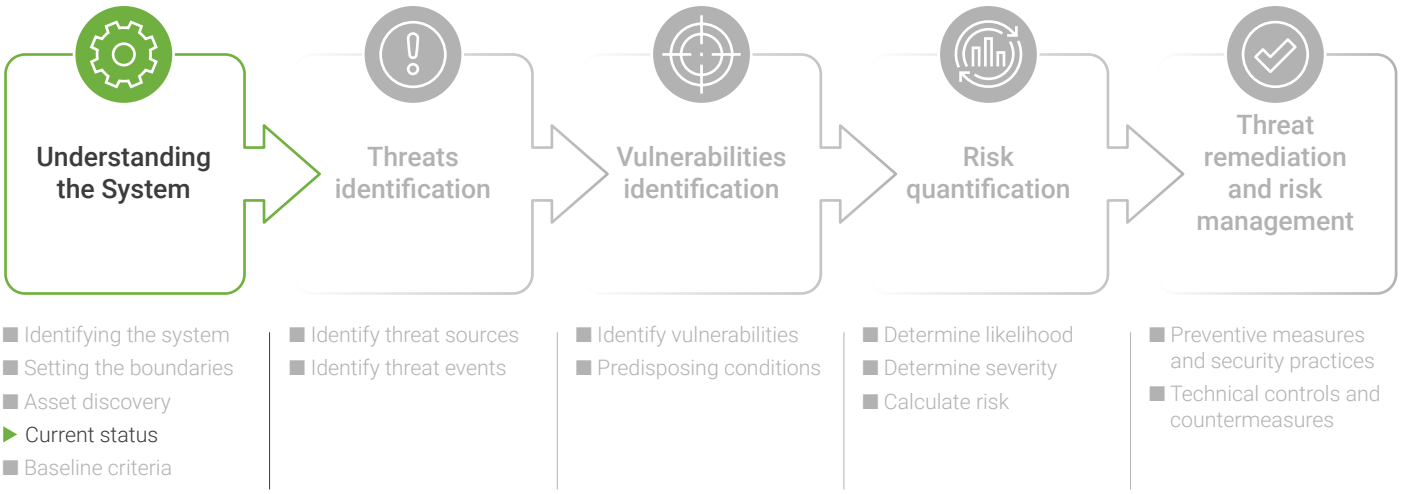


Figure 6 Understanding the system – Determine the current security status

At the next step for assessing the status of cyber security of the SUC (Figure 6), the auditor or system owner should identify the current cyber security procedures that are in place within the SUC. Once identified, the asset owner should then list assets from least to most vulnerable to create a cyber-security posture rating.

Activities in identifying a system's current cyber security status:

- Map the attack surface - this is the set of interfacing points between a user and a piece of software or hardware that could be used as an entry point by an attacker.
- Business criticality of the asset.
- For each point of the attack surface, it is required to consider:
- The severity of a known vulnerability relevant to the asset.
- Threat level. Is the attack method currently being exploited in the wild by attackers.
- Exposure/usage to the vulnerability. Based on where the asset is deployed and used, vulnerabilities are exploitable or not.
- Risk-negating effect of any security control in place.

▶ More information on this section can be found in Appendix 1C- Cyber Security Status & Baseline Security Criteria.

3.3.1 Defining a system's baseline security criteria

This part of the framework will guide the definition of the SUC's baseline security criteria (Figure 7).

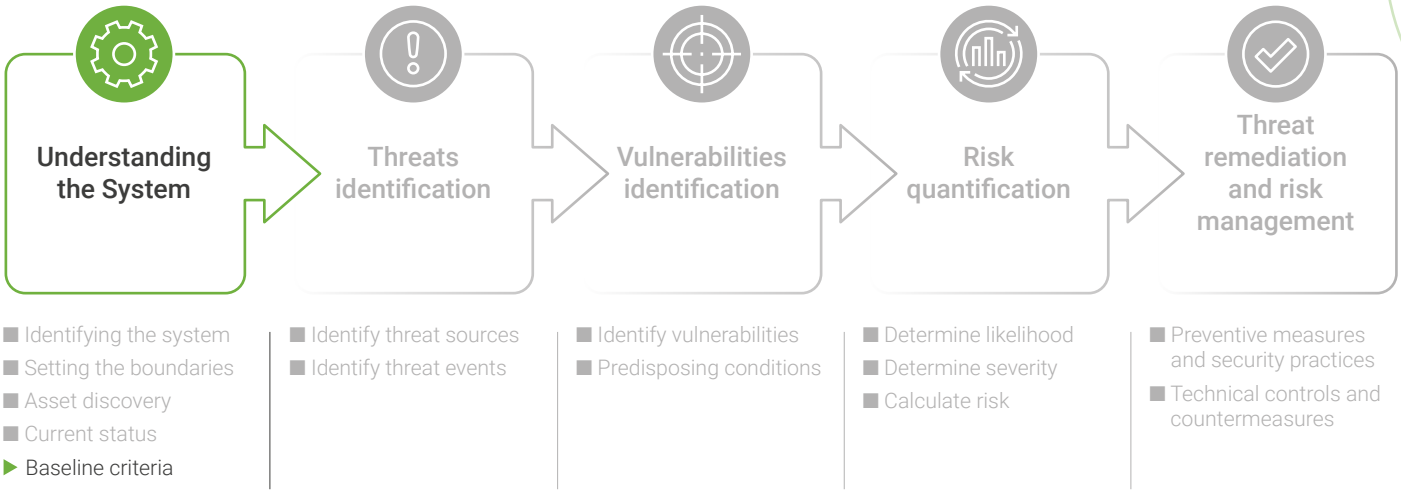


Figure 7 Understanding the system – Define the baseline security criteria

According to the National Institute of Standards and Technology (NIST), a security control baseline refers to "the set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system"(NIST 800-30). Figure 8 shows how cyber risk tolerances impact technology usage.

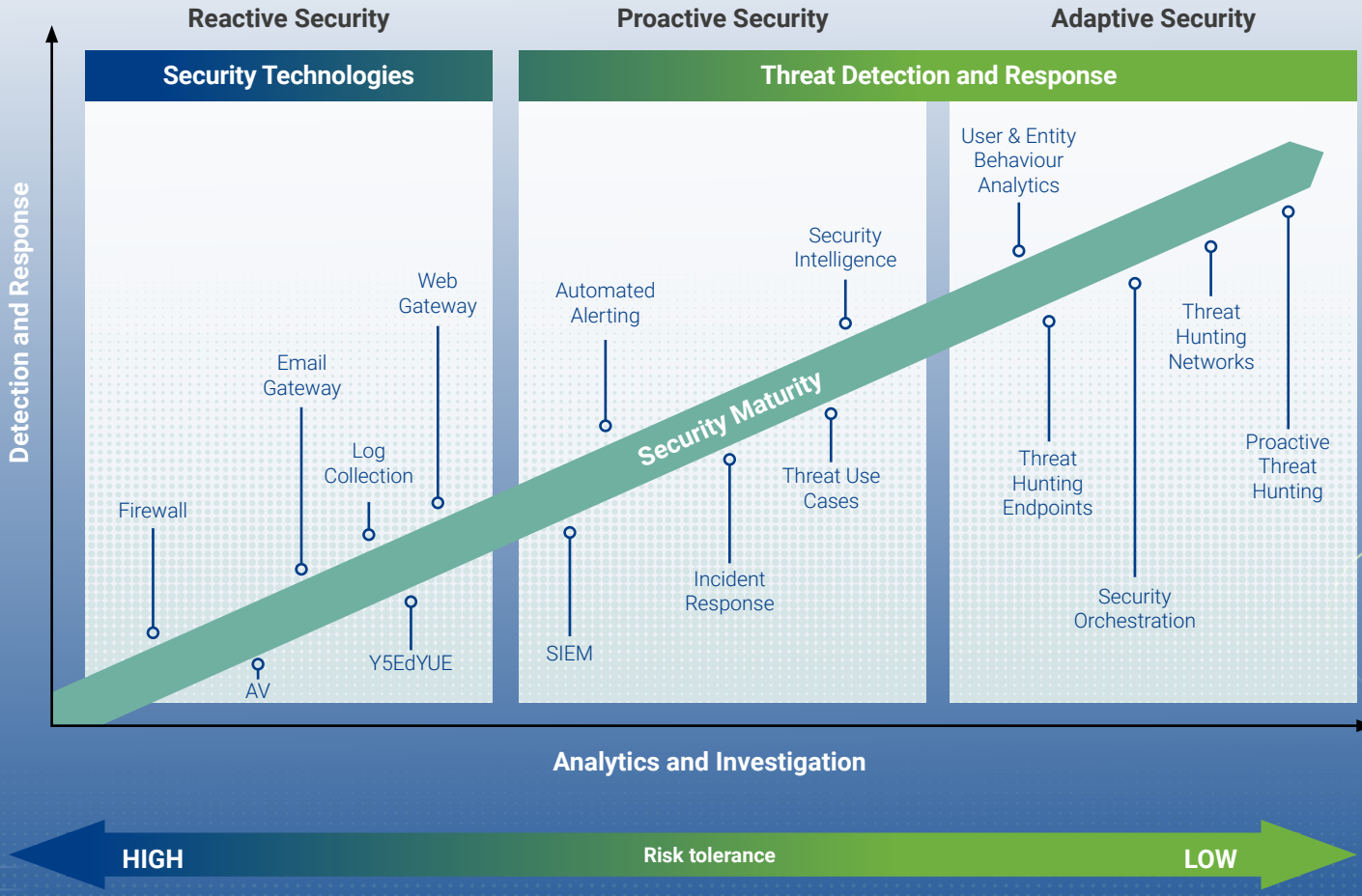


Figure 8 A perspective on how high and low cyber-risk tolerances impact technology usage [source]

How to define a system's baseline security criteria

To define baseline security criteria, the system owner/organisation must first define the risk tolerance for the system/organisation. The risk tolerance according to NIST is "the level of risk an entity is willing to assume in order to achieve a potential desired result"(NIST 800-30). To do this the system owner/organisation must first identify the critical assets within the system/organisation, defining what they are and where they sit. Critical assets can be described as assets that perform a critical function within the system or interact with sensitive data in one way or another. When defining the risk tolerance level, the system owner/organisation should take into account numerous drivers, such as:

- Compliance drivers
- Privacy risks
- Security threats
- Data and asset value
- Industry and competitive pressure
- Management preferences.

To assist with defining the risk tolerance for the system/organisation, Table 2 highlights some of the factors a system/organisation may have/implement and the subsequent tolerance for the risk the system owner/organisation should have.

Table 2 Factors to consider when defining the risk tolerance

Risk tolerance level	Factors
High	No compliance requirements
	No sensitive data
	Customers do not expect your organisation to implement and maintain strong security controls.
	Innovation and revenue generation comes before security, so more risk is accepted.
	Organisation does not have remote locations.
Medium	Some compliance requirements (e.g. HIPAA, PIPEDA).
	Some sensitive data, required to retain records.
	Customers will eventually need strong security controls for their activities.
	Due to the sensitive data, information security is more visible to senior management.
	Organisation has some remote locations.
Low	Multiple compliance requirements and house sensitive data, e.g. medical records.
	Customers require and expect your organisation to have and maintain strong security controls.
	Information security is highly visible to senior management and public investors.
	Organisation has multiple remote locations.
	Assess the security pressure posture

4 Threat identification

A threat is any circumstance or event with the potential to adversely impact organisational operations and assets, individuals, or other organisations, through an information system via unauthorised access, destruction, disclosure, or modification of information, and/or denial of service.

A threat is derived by its source and event in the way that a threat source can initiate or not a threat event. The initiation of an event depends on various parameters such as required technical capabilities and skills, the intention and the target. There might be a case where a threat source might be identified but the event cannot be initiated and as such, the attack cannot be carried out. These occasions must be carefully considered and therefore the threat identification stage is broken down into two phases as explained below. Further information is available in Appendix 2A.

4.1 Identification of threat sources

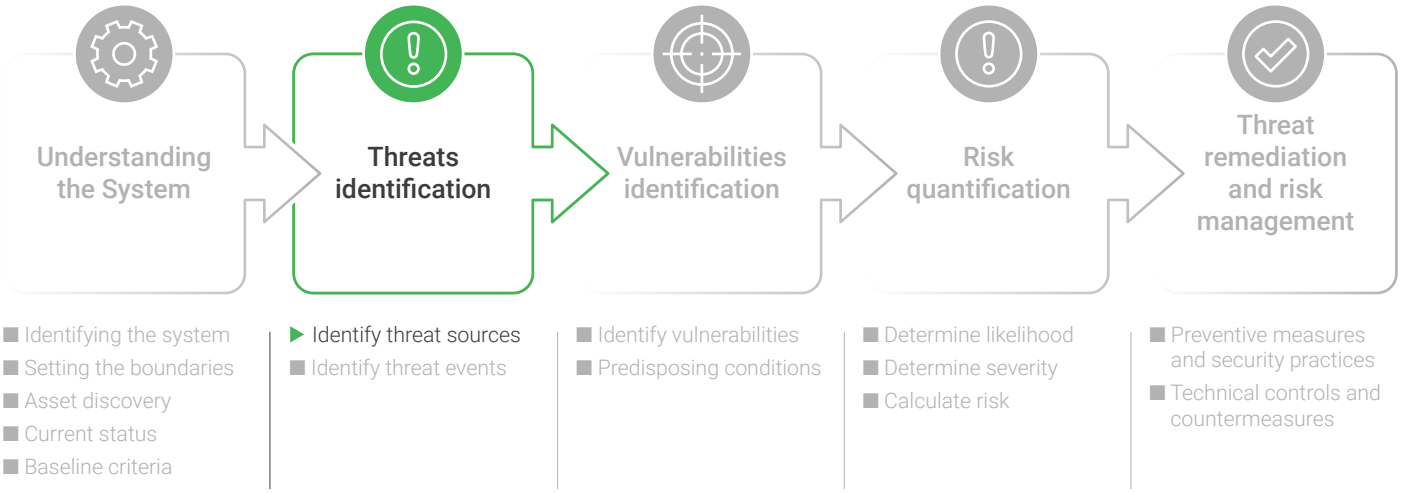


Figure 9 Threats identification – Identify threat sources

The following activities are required to complete the task of threat sources identification (Figure 9):

- Identify threat source inputs from organisation
- Identify threat sources
- Determine if threat sources are relevant to the organisation and in scope
- Identify key characteristics of threat sources:

For relevant adversarial threat sources:

- Assess adversary capability
- Assess adversary intent
- Assess adversary targeting

For relevant non-adversarial threat sources:

- Assess the range of effects from threat sources

▶ Appendix 2B provides tables that may facilitate the collection of key information and completion of the tasks above.

4.2 Identification of threat events

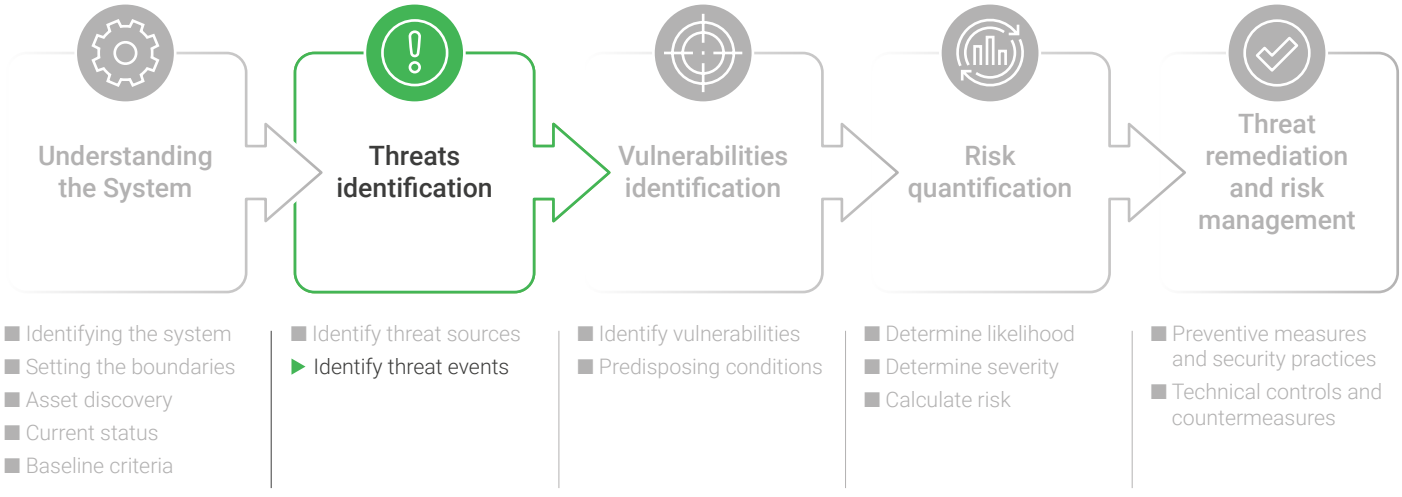


Figure 10 Threats identification - Identify threat events

The key activities to complete the task are in summary:

- Identify threat events input
- Identify threat events for adversarial and non-adversarial occasions
- Identify and link to relevant threat sources
- Assess the relevance to an organisation and link to a risk tolerance pre-set

▶ Appendix 2C provides more information that will facilitate the collection of key information for the completion of the tasks above.

5 Vulnerabilities identification

This task supports the identification of vulnerabilities across the SUC (Figure 11). Supplementary to this, predisposing conditions need to be considered and recorded.

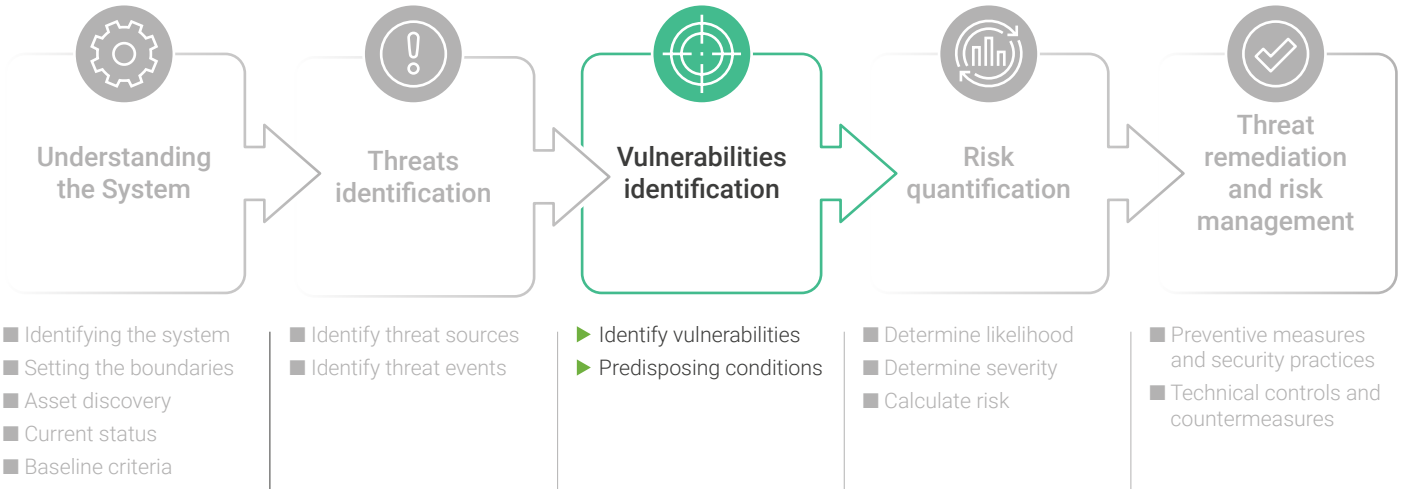


Figure 11 Vulnerabilities identification - Identify vulnerabilities & predisposing conditions

A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. Therefore, it is essential to identify these weak points and act proactively with the aim to prevent a threat event or mitigate the impacts' severity if the event happens.

A predisposing condition is a condition that exists within an organisation, a mission or business process, enterprise architecture, information system, or environment of operation, which affects the likelihood that threat events, once initiated, resulting in adverse impacts to the organisational operations and assets, individuals, and other organisations.

How to identify vulnerabilities

Key activities necessary for completing this task are:

- Identify useful inputs and information
- Identify vulnerabilities and predisposing conditions
- Assess the severity of vulnerabilities if exposed
- Assess pervasiveness of predisposing conditions
- Associate with a threat or group of threats if possible.

▶ Useful tables relevant to these activities are provided in Appendix 3A - Vulnerabilities and predisposing conditions identification. Additional information can also be found in Appendix 3B - Further vulnerabilities assessment methods.

6 Risk quantification

The risk quantification is done in three main steps. First, the likelihood of threats to occur and vulnerabilities to be exposed is estimated qualitatively or quantitatively. Then, the severity of the impacts on the organisation or systems is calculated. Finally, the overall risk is assessed incorporating the previous two steps.

Risk is defined as the level of impact on organisational operations, assets and individuals resulting from the impact of a threat and its probability of occurrence. It is important to understand where the system/organisation is vulnerable, and the risks associated with those vulnerabilities so an attack can be prevented. The level of the risks identified will then inform the subsequent control measures and mitigation plans necessary to reduce risk and reduce their impact once a risk is realised.

6.1 Determine likelihood

As explained the first step is to assess the likelihood of a particular risk happening. This section contains information on how to determine the likelihood (Figure 12).

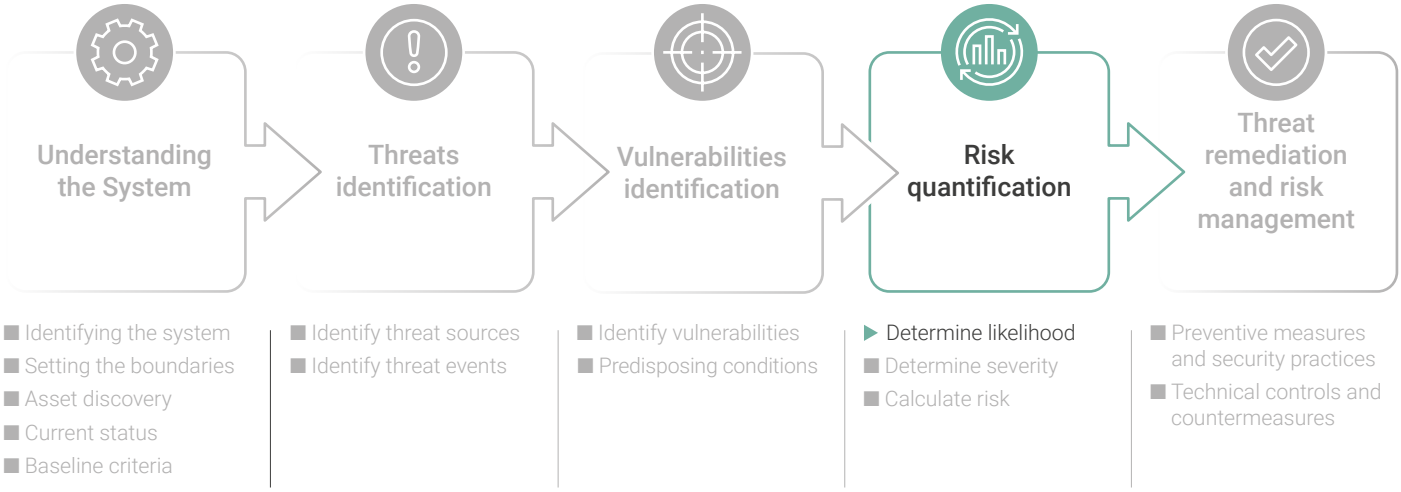


Figure 12 Risk quantification – Determine likelihood of threat/vulnerability

The likelihood of occurrence is a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities). The likelihood risk factor combines an estimate of the likelihood that the threat event will be initiated with an estimate of the likelihood of impact (i.e., the likelihood that the threat.event results in adverse impacts)..

How to determine risk likelihood

The range of likelihood can be broken down into categories to support a more accurate identification of the appropriate level of probability for an incident to occur. Depending on the granularity of the risk assessment qualitative or quantitative scales can be used. Table 3 below presents an example of a likelihood scale.

Table 3 Example of a risk likelihood scale

Likelihood scale	Guideword	Likelihood description	Frequency-based guidance
1	Certain	Almost certain	>10^-1per year (High demand)
2	Likely	Likely to occur	10^-1 to 10^-3per year (Low demand)
3	Possible	Quite possible or not unusual to occur	10^-3 to 10^-4 per year
4	Unlikely	Conceivably possible, but very unlikely to occur	10^-4 to 10^-5per year
5	Remote	So unlikely that it can be assumed it will not occur	>10^-5 per year

6.2 Determine severity

This task is about assessing the severity of impacts from threat events identified if they occur (Figure 13).

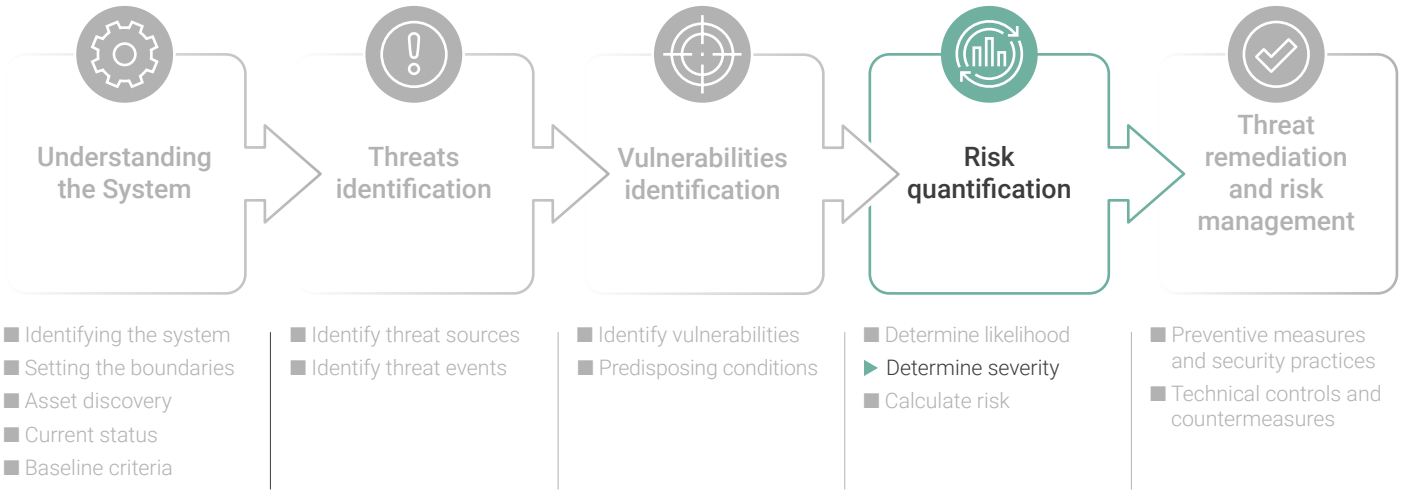


Figure 13 Risk quantification – Determine severity of threat/vulnerability

This is a quantification of the impact's severity which will affect the final risk relevant to a threat event and/or vulnerability. The magnitude plays a key role in the response of the organisation either to prevent the event or mitigate the consequences if the event happens.

How to determine risk severity

The severity scale can be broken down into discrete categories. Multiple ways and criteria can be included in the classification. In Table 4 below an example can be seen in which a guideword, a likelihood description and a frequency scale are used.

Table 4 Example of a risk severity scale

	Operational			Financial			HSE		
Category	Outage at one site	Outage at multiple sites	National infrastructure and services	Cost (Million USD)	Legal	Public confidence	People onsite	People offsite	Environment
A (High)	>7 days	>1 day	Impacts multiple sectors or disrupts community services in a major way	>500	Felony criminal offence	Loss of brand image	Fatality	Fatality or major community incident	Citation by regional agency or long-term significant damage over a large area
B (Medium)	<2 days	>1 hour	Potential to impact sector at a level beyond the company	>5	Misdemeanour criminal offence	Loss of customer confidence	Loss of work day or major injury	Complaints or local community impact	Citation by a local agency
C (Low)	<1 day	<1 hour	Little to no impact to sectors beyond the individual company. Little to no impact on the community	<5	None	None	First aid or recordable injury	No complaints	Small, contained release below reportable limits

6.3 Risk calculation

This is the final step in risk quantification where the risk to the organisation from threat events of concern is determined, considering: (i) the impact that would result from the events; and (ii) the likelihood of the events occurring (Figure 14).

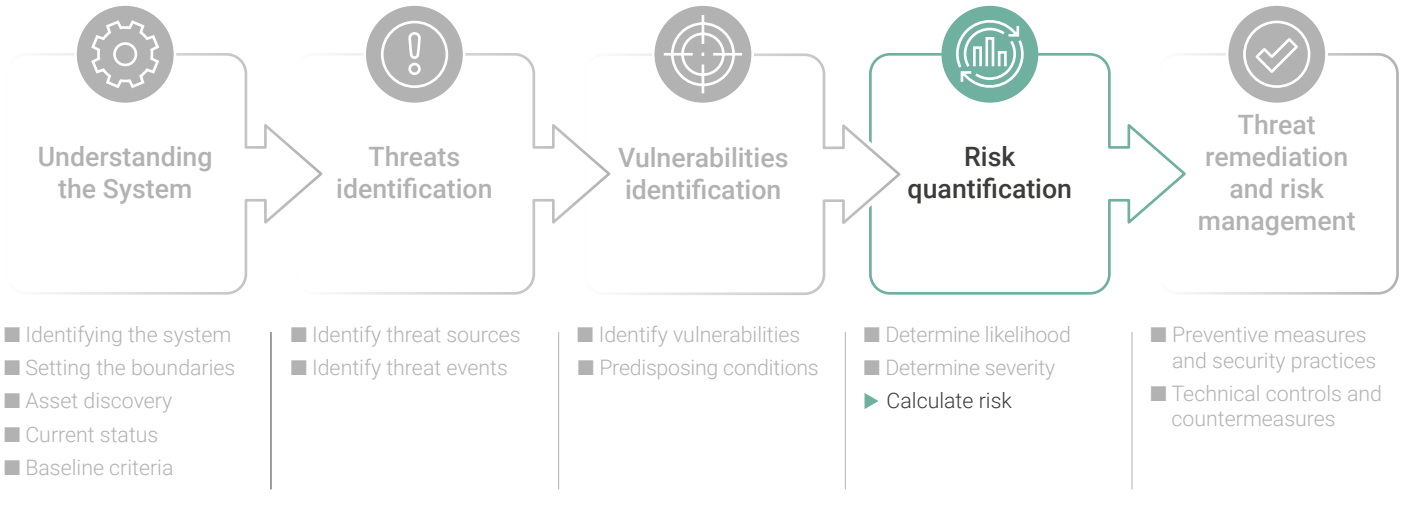


Figure 14 Risk quantification – Risk calculation

This will provide a measure of the combined likelihood and severity of a threat event happening or vulnerability being exposed. The output from this stage will inform the decision making around control measures and mitigation plans necessary to avoid an incident or reduce the impact on the organisation.

How to perform risk calculations

Risk matrices are required when determining the level of a risk considering the likelihood of an incident occurring and the severity of the impact if the incident occurs. A risk matrix includes likelihood on one axis and severity on the other. The intersection between the lowest likelihood and severity provides the lowest rank. Similarly, the highest rank is identified. Risk matrices might vary in size, although they always have two dimensions. The following table will help in combining already existing information around the likelihood and impact of a risk.

▶ Several examples are provided in Appendix 4A to illustrate the function and design considerations

Table 5 Example of a risk likelihood – severity matrix

		Severity		
		A	B	C
Likelihood	5	High	High	Med-high
	4	High	Med-high	Medium
	3	Med-high	Medium	Med-low
	2	Medium	Med-low	Low
	1	Med-low	Low	Low

With the completion of the risk assessment, an organisation needs to structure a risk management strategy that will address how each of the identified and quantified risks is going to be faced. There might be cases where a risk can be accepted, transferred or eliminated. A key consideration to add to that is for example the cost for taking preventive measures and the cost for resolving the issue caused by an incident. If the cost for resolving the issues is less than the deployment of a preventative measure, then this risk can be considered for acceptance. Another parameter to add to the risk management strategy would be the organisation's reputation. In this manner, all the risks identified in the conducted assessment should be included in the organisation's strategy and subsequently inform the next steps of remediation plans and risk management approach.

7 Threat remediation and risk management

This section discusses and demonstrates how cyber-security risks within an organisation can be addressed and managed using a range of Threat Remediation and Risk Management techniques that are currently available.

Threat Remediation & Risk Management are key parts of the risk assessment framework as they look to mitigate risks within a system and reduce the number of vulnerabilities a system may have. These types of solutions do not completely remove risk or vulnerability within a system but will seek to reduce how accessible or impactful a risk or vulnerability may be to the SUC.

7.1 General preventive measures & security practices

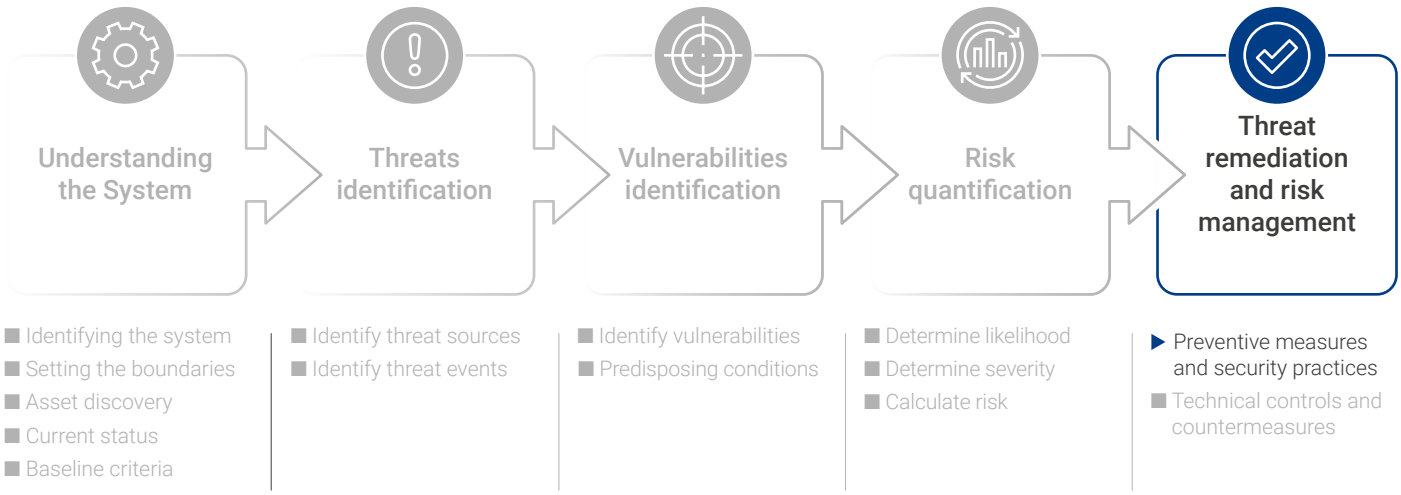


Figure 15 Threat remediation Preventive measures and security practices

There are many different preventative measures and practices that can be applied to a system to manage risks and remediate threats as the key actions upon the completion of the risk assessment (Figure 15). These measures are more generic and do not necessarily consider the specifics of a system but will still assist in mitigating any risks a system may have. When implementing preventative measures and security practices, the topics below should be considered.

7.1.1 Risk review

Before a business can implement preventative measures and security practices, the business must first consider its risk appetite. A business's risk appetite is the "amount and type of risk that an organisation is willing to pursue or retain" as no business can ever be completely free from risk (IS Guide, 2009). For a business to define the risk appetite, it must first consider the threat landscape (see Appendix 2A) and then consider the risks the business would find acceptable vs the risks the business needs to be immune to.

To assist with this, the business should consider certain factors, such as:

- Whether the risks would affect mission-critical internal business systems.
- Whether the risks would affect systems that could impact health and well-being.
- Whether the risks would affect databases containing sensitive information.
- Whether the risks would affect mission-critical external business systems.
- Whether the risks would affect core infrastructure and partner portals.

If a business cares about one or more of these factors, then it is seen as having a "low appetite" for these types of risks, and therefore, should review and mitigate those types of risks within the business.

▶ More information regarding this section is available in Appendix 5A - Risk Review.

7.1.2 Training

General guidelines to be followed to make sure everyone involved within a business or system is trained and aware of cyber security procedures (NCSF CAF Guidance, 2019).

Cyber security awareness training plays a key role in managing and preventing risks within a business/system. By making sure all staff, regardless of technical ability, are aware of the business's cyber-security policies, a company/user can reduce the likelihood that an employee falls victim to a cyber-security attack such as Malware or Phishing attacks. Not all cyber-security attacks are caused by a malicious actor, however, as some attacks are accidental and can originate from users within a business or involved within the development of a system who are untrained when carrying out certain tasks, resulting in a system vulnerability or even a breach of security.

General set of guidelines (Cybersecurity and Infrastructure Agency, 2020):

- Identify Cyber Security awareness needs.
- Identify the skills required for specific roles.
- Identify any skill gaps in personnel responsible for Cyber Security.
- Identify training needs to address the identified skill gaps.
- Conduct cyber-security awareness activities for all personnel assigned to support the critical service.
- Conduct Cyber Security training for the critical services i.e. ensure all staff are appropriately skilled in their roles.
- Conduct cyber-security training activities for all cyber-security personnel assigned to support the critical service.
- Evaluate the effectiveness of all the cyber-security awareness and training programs that support the critical service.
- Revise, as needed, all of the cyber-security awareness and training activities that are in support of the critical service.
- Conduct training in the roles and responsibilities for privileged users that support the critical service.
- Conduct training in the roles and responsibilities for executive users that support the critical service.
- Conduct training in the roles and responsibilities for physical and information security personnel that support the critical service.

▶ More information regarding this section can be found in Appendix 5B – Training.

7.1.3 Passwords & access control

Security practices can be used to improve password security or improve the security of a system that uses passwords.

Passwords are simple, low-cost security measures that are usually the first line of defence against any malicious actors. Many assets within a system or business use passwords, usually implementing default passwords set by the manufacturer during production. Although easy to use, passwords can be obtained in many ways including phishing attacks, data breaches, brute-force attacks, key-loggers, and more. Passwords can also be obtained in easier ways such as if employees make notes of certain passwords or if passwords provided by the manufacturer for certain hardware/software are left as default and are not changed. Should a malicious actor obtain a password for a system, then they may be able to gain access to said system and affect it in some way.

To prevent this there are a range of methods that can be used to increase the security passwords provide, by either using them in conjunction with other technologies or by improving how users use and set a password.

- Multi -factor authentication (MFA)
- Throttling & account lockout
- Monitoring
- Password deny lists
- Changing default passwords
- Password management software
- Use strong passwords or passphrases

▶ More information regarding this section can be found in Appendix 5C- Passwords & Access control.

7.1.4 Patch management

Patch Management (Langner, 2019) is the process whereby vulnerabilities in software or devices are updated and fixed to prevent any malicious actors from exploiting the discovered vulnerability. These vulnerabilities are slightly different from the ones previously discussed as they are usually found within a product vendor's offering such as software the vendor provides and so usually can't be directly fixed by the user. Once a vulnerability has been identified within a product, the product owner/ vendor will review the vulnerability and produce a patch which will usually be available as an update to the product. More information regarding this section can be found in Appendix 5D- Patch Management.

7.1.5 System partitioning & segmentation

System partitioning and segmentation (IEC technical committee, 2020) is the process of separating a system into zones and conduits as a preventative measure for reducing the risks within a system. More information regarding this section can be found in Appendix 5E- System partitioning & segmentation.

7.2 Technical controls and countermeasures

Technical controls and countermeasures are used in conjunction with general preventive measures and security practices (Figure 16). More information available in Appendix 5F – Technical controls and countermeasures.

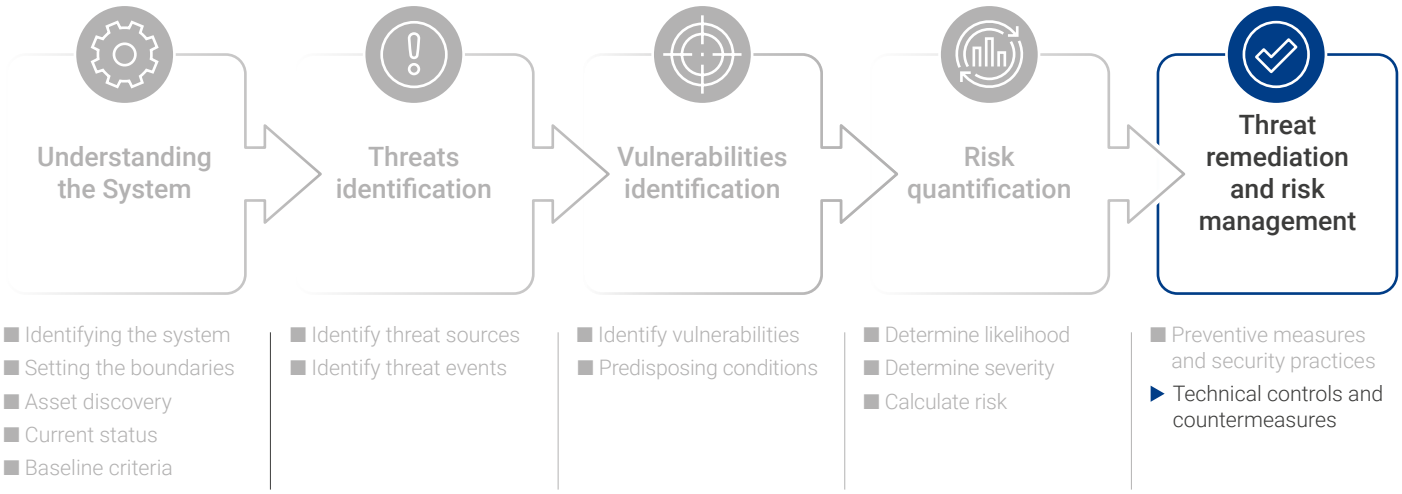


Figure 16 Threat remediation Technical controls and countermeasures

7.2.1 Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS)

It is recommended that IDS & IPS systems are used in tandem to monitor and protect a network. This allows malicious content to be blocked whilst also providing deeper analytical tools and a copy of the malicious content which can be analysed further. It is also worth noting that many solutions for IDS or IPS include a combination of both and so you only need to purchase one system instead of two. More information regarding this section can be found in Appendix 5F- Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS).

7.2.2 Security Information & Event Management (SIEM)

Security Information and Event Management (SIEM) (Gartner, 2022) solutions are systems that "analyse event data in real-time for the early detection of targeted attacks and event breaches". SIEM systems are also used for analytical and forensic purposes as they can collect, store, investigate, and report on log data. This log data is produced by security devices/solutions, network infrastructure, systems, and applications and is captured and aggregated by the SIEM system. More information regarding this section can be found in Appendix 5F- Security Information & Event Management (SIEM).

7.2.3 Firewalls

"A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules" (Cisco, 2021). Firewalls can be used to create a buffer zone between the business/system's network and another network e.g. the internet by setting a range of rules to allow, or more importantly block, data coming over the network using certain protocols or targeting specific ports. This will reduce the exposure of the business/system's network to certain network-based attacks by filtering and inspecting all network traffic in & out of the network (NCSC, 2019).

"A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

7.2.4 Malware & antivirus protection

Malware is malicious software that can affect assets such as computers and controllers within a system (NCSC, 2019). To defend against malware and other malicious code, it is recommended that Antivirus protection is installed which is used to detect, quarantine, and/or delete malicious code so that it does not affect the device/system. More information on this section can be found in Appendix 5F- Malware & Antivirus Protection.

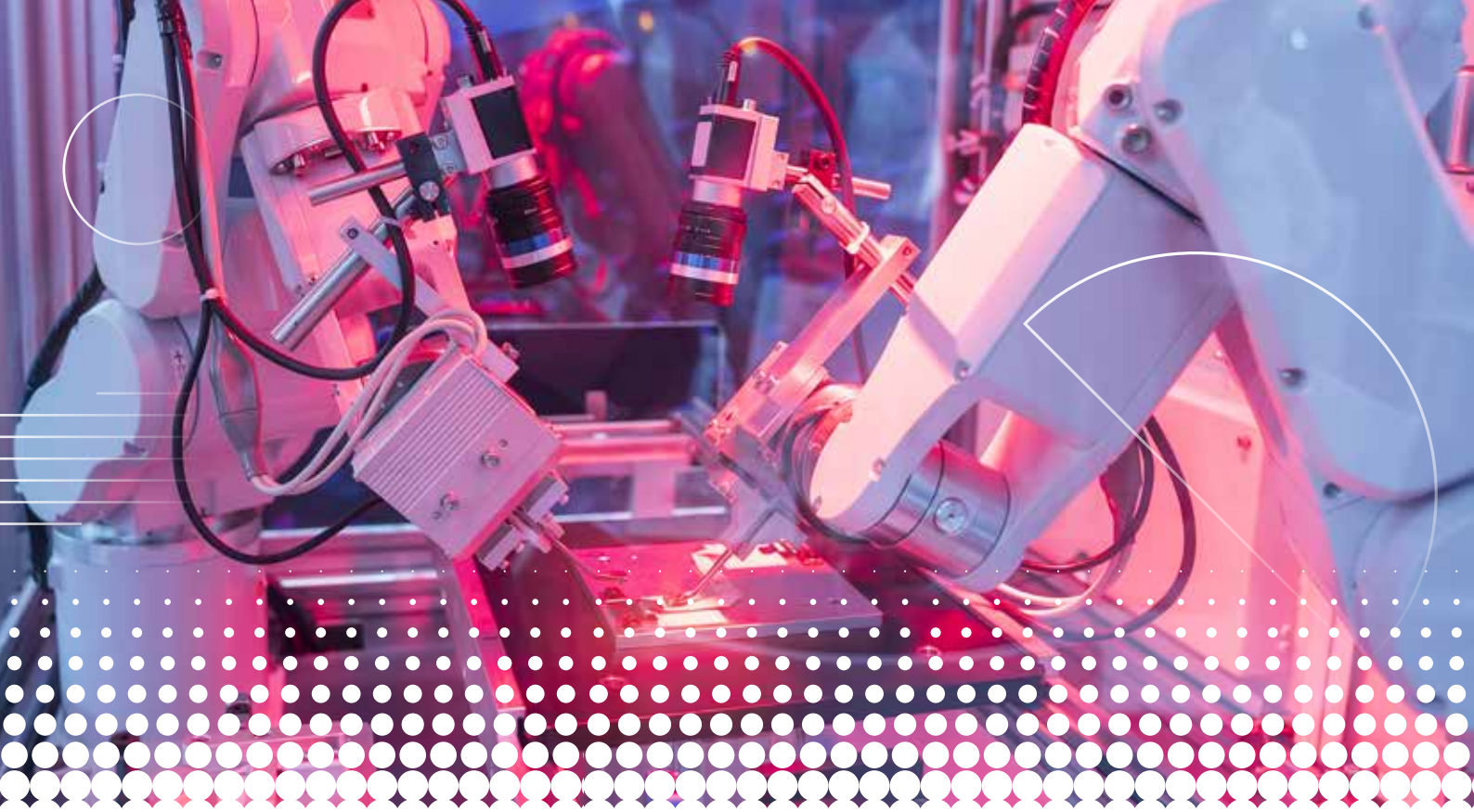
7.3 Mitigation strategies & defence-in-depth

When creating a mitigation strategy, the risks and vulnerabilities previously identified within the system should be the core on which the strategy is based (Lebanidze, 2013). To create a mitigation strategy, the user must first identify the risks within their system and the likelihood of said risks being exploited.

Please find below a table (Table 6) of the available and recommended solutions and strategies for Defence-in-Depth security (Homeland security, 2016). It is recommended that users/organisations use multiple solutions mentioned in the table (as well as within the sections General Preventative Measures & Security Practices and the Technical Controls & Countermeasures sections for methods of mitigating risks) to build up a robust defence against risks within a system. More information on this section can be found in Appendix 5G- Mitigation Strategies & Defence-in-Depth.

Table 6 Recommended solution and strategies for Defence-in-Depth security [source]

Defence-in-Depth	Strategy Elements
Risk management	■ Identify threats ■ Characterise risk and its likelihood ■ Maintain an asset inventory and network architecture
Cyber Security Architecture	■ Standards/Recommendations ■ Policies ■ Procedures
Physical Security	■ Mobile electronics locked down ■ Control centre & asset access controls ■ Remote site video security, physical barriers and access controls
Network Architecture & Security	■ Network Segmentation (Zones & Conduits) ■ Firewalls ■ Remote Access & Authentication
Host Security	■ Patch Management ■ Virtual Machines ■ Malware & Antivirus Protection ■ Password & Access Controls
Security Monitoring	■ Intrusion Detection Systems (IDS) & Intrusion Prevention Systems (IPS) ■ Security Audit Logging ■ Security Incident & Event Monitoring (SIEM)
The Human Element	■ Policies ■ Procedures ■ Training and Awareness



7.4 Residual risk & acceptable risk

Residual risk refers to the "portion of risk remaining after security measures have been applied" (National Institute of Standards and Technology, 2022). This is identified in the way any risks within a system are identified by evaluating the likelihood and impact of the risk after the security measures have been implemented within the system. The reason why residual risk needs to be identified is to measure the effectiveness of the mitigating actions that were applied to the original risk and to assist with monitoring risks within a system or business.

The acceptable risk level is usually defined when a system owner or business performs a risk review and defines the risk appetite for the system/business.

▶ More information on this section can be found in Appendix 5H - Residual Risk & Acceptable Risk.

7.4.1 Incident response and recovery plan

Users & businesses should have a response and recovery plan in place if a breach was ever to occur within their system. More information can be found in Appendix 5I- Incident Response and Recovery Plan.

A good response and recovery plan looks to prevent the loss of data, decrease the system downtime and allow the user to analyse the breach after it occurred. Before any recovery & response plan can be created, the business/user first needs to define a few things such as what the user/business defines as an incident or breach. As a general rule, an incident or breach is an adverse event that has a negative consequence within a system such as malware which destroys data.

Incident Response is the methodology an organisation uses to respond to and manage a cyber-attack. An incident response aims to reduce the damage caused by a cyber-attack and allow the organisation to recover as quickly as possible. An investigation is also a key component in order to learn from the attack and better prepare for the future.

A recovery plan seeks to redirect resources into restoring data and information systems following a cyber-attack. The recovery plan differs from incident response which focuses on information gathering and coordinated decision making to understand and address a specific event. Recovery plans, when they are properly designed and executed, enable the efficient recovery of critical systems and help an organisation avoid further damage to mission-critical operations.

8 Overview and reporting

This section presents an overview of the proposed methodology and summarise the key tasks and sub-activities as depicted in Figure 17. The flowchart displays mainly the flow of actions needed for carrying out a risk assessment for cyber-security on an advanced manufacturing system.

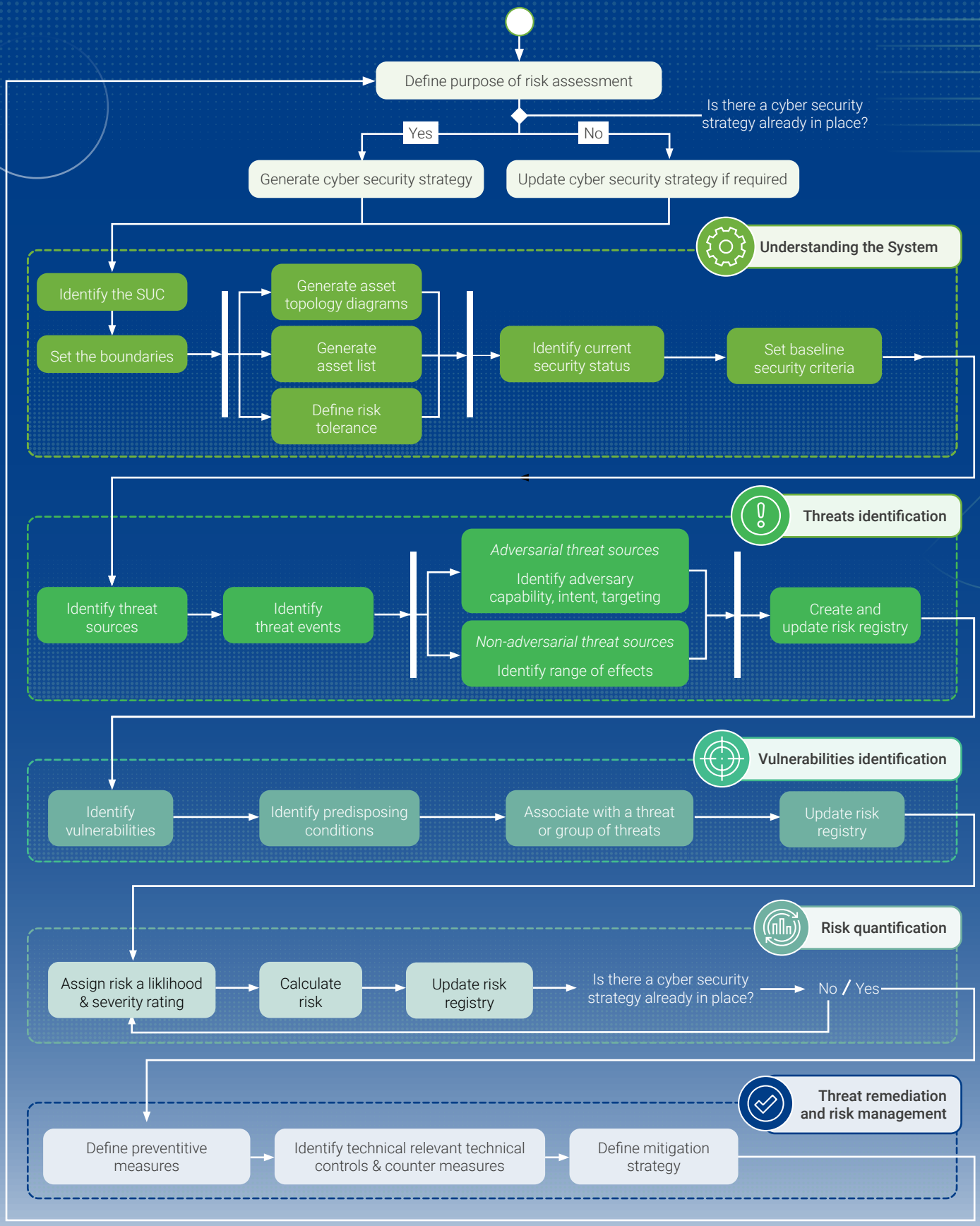


Figure 17 Flowchart of the proposed risk assessment framework

The main steps for carrying out a cyber-security risk assessment are:

- Understanding the system
- Threats identification
- Vulnerabilities identification
- Risk quantification
- Threat remediation and risk management

The data collected and generated throughout the risk assessment could be captured in the following tables.

8.1 Asset list

The template provided below in Table 7 is proposed for capturing information relevant to existing assets on the systems involved in the evaluation. In each column is shown the required data to collect that will feed into the final risk assessment.

Table 7 Asset list template and relevant details required per item

Asset Number	Asset Category	Manufacturer	Model/ Version	Serial No	Location	Existing connections	Asset Owner	Accessible Users	Operating System	Review Date
001										
002										
003										

8.2 Asset topology diagrams

The diagram presented in Figure 18 shows the Purdue model - a structural model for industrial control system (ICS) security, concerning physical processes, sensors, supervisory controls, operations and logistics. The diagram shows the different levels of critical infrastructure used in production and how to secure them.

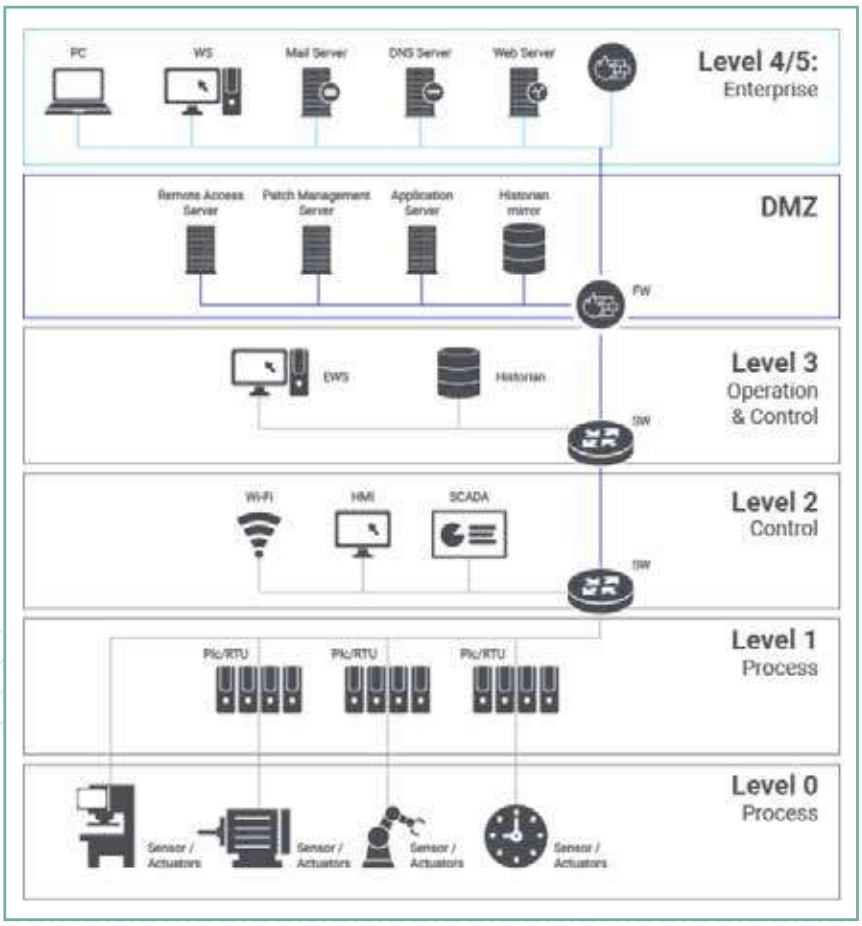


Figure 18 The Purdue model - a structural model for industrial control system (ICS) security, concerning physical processes, sensors, supervisory controls, operations and logistics. (Source: Zscaler)

8.3 Risk registry

The risk register template is suggested for collating and storing all the information collected during the steps of the risk assessment. Therefore, an overview of the current cyber security state can be provided so as relevant decisions can be informed easily. Table 8 presents the risk register template.

Table 8 Example of a risk register

Risk ID	Asset	Thread Source/Event	Vulnerability	Impact	Existing Controls	Initial Risk Rating			Responsible person/ Risk Owner	Mitigating Actions	Residual Risk Rating			Notes	Tolerated Risk
						Probability	Severity	Risk Rating			Probability	Severity	Risk Rating		
1															
2															
3															

9 Conclusion

This handbook has been structured to provide technical support and guidance for carrying out a cyber-security risk assessment on a smart manufacturing system. The purpose of this manual is to introduce the subject of cyber risks and security to engineers and help them develop a suitable risk assessment tool. To achieve this, they can combine different sources of information and integrate parts of various methodologies to create their own more bespoke risk assessment tool.

What is suggested through the various steps does not constitute a single solution, but rather a framework that includes the key steps of a basic cyber security risk assessment. The depth and breadth of the risk assessment will depend upon; the organisation, the purpose of the assessment and the context within which the assessment is undertaken.

On completion of reading this manual, an engineer should be able to:

- Understand the systems and create an asset inventory and ownership list;
- List the known threats associated with those assets;
- Estimate roughly what kind and how much of the core cyber elements (confidentiality, integrity, availability) could be affected if a threat occurs or a vulnerability is exploited;
- Understand which security controls are in place, and which ones could be implemented to mitigate risk.

Additional information for deeper analysis is provided through a series of appendices at the end of this manual for those wishing to develop a stronger understanding of cyber security in manufacturing.

Key points and learnt outcomes

As already highlighted, there is a strong link between IT and OT and the essential cyber security tools and methods from IT can be transferred and applied in the case of an advanced manufacturing system. With the development of novel digital technologies for incorporation in production facilities, the convergence of IT and OT becomes more extensive. This creates additional needs for secure data collection, handling and storage as well as operation of both the software and hardware.

The introduction of Industry 4.0 systems and solutions drive businesses towards a data-driven production environment, where data adds value to both the enterprise operation and the final product itself. Data, therefore, becomes equally critical to the end customer through the service or product that they receive. In this vein, cyber security may be included in the main strategy pillars of an organisation, in order to secure the added value resulting from this use of data.

Producing a cyber-security risk assessment is a lengthy process. When constructing this manual an effort was made to make the methodology as compact as possible. However, thorough preparation is still necessary in order to identify the correct sources of information within an organisation. Engagement and data collection from many sources across many different business functions may be necessary.

A cyber security risk assessment is a living element that should be used, advised and updated continuously. Many changes may occur throughout the operation of a manufacturing system such as; a new threat or vulnerability being recognised, new control measures being required upon the deployment or removal of a piece of equipment, or even a change to the purpose for which the system is used. Subsequently, the risk registry must be continuously updated as relevant decisions are made.

Cyber security is not only related to the production layer of a manufacturing business but is also linked to upstream hierarchical layers such as the administration, enterprise operations and boards. A suitable strategy and relevant policies must therefore be in place as these will impact decisions made regarding investments, partners and supplier relationships. More importantly, as already mentioned, such a strategy will serve as the backbone for protecting the value added by data management and cyber security across the entire organisation.

Appendices

Appendix 1A- Identifying the system under consideration & defining boundaries

The SUC may include several sub-systems such as basic control process systems (BPCS), distributed control systems (DCS), safety instrumented systems (SIS), supervisory control and data acquisition systems (SCADA) and IACS product supplier's packages. Additional technologies to include might be Industrial Internet of Things (IIoT) devices and cloud based solutions normally identified within the IT space. To assist in defining the boundary for the risk assessment, it is advised that users should focus on areas of the system that are of high value, offer a critical service, contain sensitive data and/or are most at risk of attack.

Risk assessment at Tier 1 supports organisational strategies, policies, guidance and processes for managing risk. The focus of an assessment at this level is on the organisation's operation, assets and individuals. What can be addressed at Tier 1 includes specific threats directed at an organisation, systemic weaknesses or deficiencies identified across multiple information systems of the organisation that may be exploited to adversaries, adverse impacts from the loss or compromise of organisational information and the use of new IT technologies and computing systems such as mobile/cloud and the potential effects on the company's ability to keep serving the missions and carry out operations.

At Tier 1 a risk assessment may affect decisions at an organisational level with regards to information security programs, policies, procedures and guidance, type of risk responses (risk acceptance, avoidance, mitigation, etc), investment decisions for information technologies and systems, conformance to business security architectures and strategies for monitoring authorisation on systems and controls.

At Tier 2, risk assessments support the definition of protection of mission/business processes and resilience requirements, and the alignment of these requirements to the organisation's architectures. This is accomplished through an information security framework embedded within the wider organisation's architecture. A Tier 2 risk assessment may also affect enterprise security architecture design decisions, the selection of common controls, the selection of suppliers, services, and contractors to support organisational missions or business functions, the development of risk-aware mission/business processes and the interpretation of information security policies with respect to enterprise information systems and environments in which those systems operate.

At Tier 3 a risk assessment may inform the decisions around design (including selection and tailoring of security controls and systems), implementation (systems and product configurations to meet security control requirements) and operation (level of monitoring activity, frequency of information system authorisations and maintenance decisions). At this layer, a risk assessment may include descriptions for vulnerabilities in the systems, an assessment of the risks associated with each vulnerability and corrective actions to mitigate the risks identified. This will subsequently inform the assessment of the organisation's overall risk while operating the systems as evaluated. The assessment outputs can feed back to Tiers 1 and 2.

A cyber security risk assessment may also inform other risk management activities related to non-security aspects. For instance at Tier 1, insights from the assessment might feed into operational risk determination with regards to business continuity and function, financial risk management, as well as other kinds of risk such as regulatory, reputational, supply chain and partnerships. At Tier 2 similar insights can be provided relevant to specific business functions and operations. At Tier 3, risk assessment outcome can inform other types of assessment such as costs, schedule and performance pertinent to information systems. Those outcomes from a risk assessment across a tier can also be shared with and contribute to other tiers' non security risk management.

Appendix 1B – Asset discovery

Before assets can be identified, it is important for the system owner to have in place the procedures and responsibilities for identifying, recording, and managing assets within the SUC. The most common method for recording and managing assets and the owners responsible for said assets is via an asset register and through relevant diagrams such as network and deployment diagrams. An asset register is a document that identifies all of the assets within the SUC along with relevant information about said assets. The information about each asset should include:

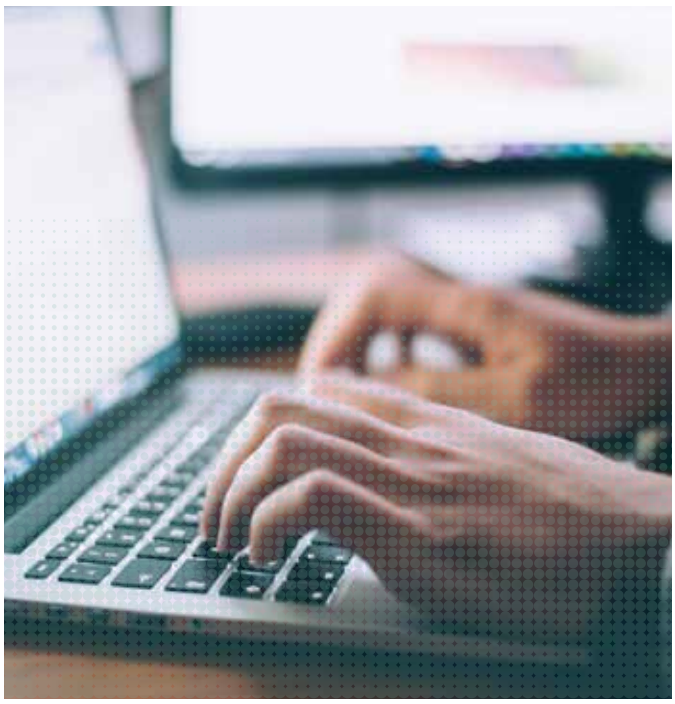
- Unique identifier, location and zone reference
- Asset / conduit type, manufacturer, serial number etc.
- Relevant risk profile and/or criticality information (e.g. risk-level, restore criticality, known vulnerabilities such as untreated CVEs etc.)
- Responsible person (where responsibilities are divided, e.g. between different departments)
- Network connectivity arrangements (e.g. addresses, ports, connection type, network protocols, encryption algorithms etc.) for each network connection.
- Network connection type, e.g. for multi-homed assets, or other (e.g. fieldbus) connections.
- Conduits – expected data flows to allow data flow rules to be defined.
- Any temporary connections such as portable assets (e.g. laptops) and assets where portable media connections are required / used.
- Firmware, operating system, and application software (including security software such as AV) types and versions (could be part of another system rather than the asset register but should be recorded)

In addition to the asset properties above, it is also recommended that the system owner identifies who has access to the individual assets or parts of the system as well as identifies assets or parts of the system they have no control over. An asset which the user has no control over can include products or services that are used within the system and may collect information about the system or user and are provided by a third party or vendor. Here the user has control over whether they use the asset within the system and to a lesser extent how the asset is used within the system but has no control over how the asset functions.

Within the procedures for managing assets, it is also important to have in place decision making processes, plans or roadmaps for what happens to assets throughout their lifecycle, in particular obsolescence. It is also important to recognise that industrial assets tend to have much longer operational lifespans than commercial IT systems.

If a system has many digital assets or applications, it may also be of value to create a secondary digital asset list in addition to the primary asset list. This digital asset should include information about the digital assets, including:

- Software name and publisher
- Installation date, version number and motivations
- Local and remote roles
- Generic accounts
- Dedicated accounts
- Access control list with read, write and execution rights
- When existing, outgoing connections shall be considered (IP/Ports destination). If unknown, information shall be identified as “missing”
- Licence number.



Diagrams are important in understanding the system and should be generated to show the architecture and topology of the system and how the assets within the asset register are connected. The logical topology of networks (e.g. IP and non-IP addressing scheme, subset names, logical links, principal devices in operation) should be recorded in the form of inventories and diagrams. Such documentation could include:

- List of IP address range with, for each one:
  - The list of switches concerned
  - The functional description of the IP range;
  - Interconnections with other ranges.
- List of non-IP networks with, for each network:
  - The list of MAC addresses or addresses specific to the industrial protocols on the network
  - The list of switches concerned
  - Functional description of the network
  - Devices connected to the other network(connectors).
- List of non-Ethernet access points with, for each one:
  - The list of access ports
  - Addressing, if there is a special protocol
  - The list of connected devices.
- List of logical servers and desktops with, for each one, if applicable:
  - IP addressing (network, mask, gateway)
  - Operating system version
  - Underlying physical server
  - Applications and their versions
  - Services and versions
- List of connectors and communication field devices (remote I/O, smart sensors, smart actuators, etc.) with, for each one:
  - IP addressing (network, mask, gateway) for associated MAC addressing and network or the specific addressing, if appropriate
  - applications
- Interconnection points with “external” entities and all interconnections with the internet.

Appendix 1C- Cyber security status & baseline security criteria - Defining a systems current cyber security status

The following steps can be carried out to assist with defining the cyber security procedures that are in place in the system under consideration:

- X-Y plot (things that can go wrong over devices & apps on your network- infrastructure, apps, endpoints, IoTs, Cloud, Supply Chain). In a typical breach, the adversary uses some point on this attack surface to compromise an (Internal facing) asset.
- Understand the cyber risk. Cyber risk has an inverse relationship with your security posture. As your security posture becomes stronger, your cyber risk decreases.
- Risk is defined as the probability of a loss event (likelihood) multiplied by the magnitude of loss resulting from that loss event (impact). Cyber risk is the probability of exposure or potential loss resulting from a cyberattack or data breach.
- An accurate cyber risk calculation needs to consider 5 factors: impact (business criticality), likelihood (vulnerabilities, exposure, threats, mitigating controls).

For each point of the attack surface we must consider:

1. The severity of a known vulnerability relevant to the asset;
2. Threat level. Is the attack method currently being exploited in the wild by attackers.
3. Exposure/usage to the vulnerability. Based on where the asset is deployed and used, vulnerabilities are exploitable or not;
4. Risk-negating effect of any security control in place;
5. Business criticality of the asset.

This calculation needs to be performed for all points of the attack surface. This result is an accurate picture of where your cyber-risk is and helps you prioritise risk mitigation actions while avoiding busy work fixing low risk issues.

Appendix 2A – Threats identification and assessment

As explained in the introductory part of the manual, the threats and resulting risks within a manufacturing environment are linked to the triad of availability, integrity and confidentiality. That is when a threat is implemented and an incident happens, this will lead to the loss of at least one of the above elements.

Attacks targeting availability intend to make a system unavailable to perform a task by overloading it. The target can be either the equipment (machinery) or the relevant network access. Most common types of attacks are DDoS - distributed denial of service which aims to flood the bandwidth or other resources of the system. Other attacks affect the network such as grey hole, black hole, relay attacks

Integrity relates to the accuracy and completeness of data. Relevant threat is similar to sabotage. The aim is to later the industrial communication protocol or network traffic. Most of the used protocols in industry are legacy which means they were designed without security considerations. Common attacks are of Man-in-the-middle type which aims to alter and relay the communication between two entities.

Confidentiality threats consist of accessing or stealing sensitive data pertinent to industrial processes, configurations, customers and administration. These are usually called cyber espionage and can be achieved through passive analysis of the network traffic, active code injection into operational applications to obtain security credentials or corrupt control measurements.

An additional characteristic that could be equally considered is authentication. Relevant threats target design flaws or software vulnerabilities to escalate privileges and gain access to protected resources. Such attacks include phishing, spam letter chains to collect strategic information. Misconfiguration leading to unsuitable access at physical or logical level can entail similar security issues.

The majority of threats faced in a smart factory can be classified into the following categories.

Cyber espionage. This includes stealing sensitive information and IP such as product and corporate data. As Industry 4.0 enables collaboration of multiple partners (such as suppliers in a network), this subsequently might make the task easier for attackers as they have many pathways and high potential for very fast spreading.

Denial-of-Service (DoS) aims to make a system unavailable. This can be achieved by launching waves of requests to a server to consume all the resources, passing malformed data to crash a process, virus infiltration and destroying or disabling the sensors on a system. Since most of the devices in a factory are interconnected and therefore interdependent, their unavailability might be critical for the production. The development of cloud computing has also launched new ways of DoS attacks, thus pushing companies to increase their attention to it.

Supply chain and extended systems. With the use of smart technologies, the supply chain can be interconnected involving multiple organisations (suppliers, partners, clients). However the supply chain has inherent system vulnerabilities which can be exploited by cyber-attackers. Thus, if a supplier is attacked by phishing or credentials theft, this will result in a massive exposure of data from the connected partners.

Employees' awareness. A big challenge within the current manufacturing industry is that companies are not fully aware of the cyber security risks associated with Industry 4.0 and smart technologies. As a consequence they mainly deal with cyber security when a serious incident occurs. Awareness of the employees around cyber security is really important, from the skilled machine operators to software and planning engineers. This can be achieved by awareness raising campaigns engaging the entire manufacturing environment as well as by research organisations working on cyber security topics and delivering guidelines and practices to industrial professionals.

Advanced Persistent Threats (APT). The main idea behind this is for the attacker to identify and take advantage of the network's vulnerabilities, infiltrate it and stay unnoticed for as long as possible. Then propagate to the whole network with the aim to infiltrate devices and collect information or modify the system's function. The identification of vulnerabilities can be achieved owing to a possible metadata leakage coming from servers, Programmable Logic Controllers (PLC) or sensing devices. These issues can expand over the cloud or IoT network and must be thoroughly taken into consideration.

Supply chain and extended systems. With the use of smart technologies, the supply chain can be interconnected involving multiple organisations (suppliers, partners, clients). However the supply chain has inherent system vulnerabilities which can be exploited by cyber-attackers. Thus, if a supplier is attacked by phishing or credentials theft, this will result in a massive exposure of data from the connected partners.

Employees' awareness. A big challenge within the current manufacturing industry is that companies are not fully aware of the cyber security risks associated with Industry 4.0 and smart technologies. As a consequence they mainly deal with cyber security when a serious incident occurs. Awareness of the employees around cyber security is really important, from the skilled machine operators to software and planning engineers. This can be achieved by awareness raising campaigns engaging the entire manufacturing environment as well as by research organisations working on cyber security topics and delivering guidelines and practices to industrial professionals.

Advanced Persistent Threats (APT). The main idea behind this is for the attacker to identify and take advantage of the network's vulnerabilities, infiltrate it and stay unnoticed for as long as possible. Then propagate to the whole network with the aim to infiltrate devices and collect information or modify the system's function. The identification of vulnerabilities can be achieved owing to a possible metadata leakage coming from servers, Programmable Logic Controllers (PLC) or sensing devices. These issues can expand over the cloud or IoT network and must be thoroughly taken into consideration.

Parameters to consider in identifying cyber threats:

- Attack source (inside/outside)
- Objectives/goals of the attack
- Cyber layer including execution layer (sensors, actuator), data transport (network), application layer (user data storage)

According to IEC 62443-3-2:2020 it is also suggested that a threats identification list should include:

- Description of the threat source
- Description of the capability or skill level of the threat source
- Description of possible threat vectors
- Identification of the potentially affected assets.

Some examples of a threat description are provided below:

- A non-malicious employee physically accesses the process control zone and plugs a USB memory stick into one of the computers
- An authorised support person accesses the process control zone using an infected laptop
- A non-malicious employee opens a phishing email compromising access credentials

Appendix 2B - Threats sources identification

Threat events are caused by threat sources. A threat source is characterised as: (i) the intent and method targeted at the exploitation of a vulnerability; or (ii) a situation and method that may accidentally exploit a vulnerability. In general, types of threat sources include:

- hostile cyber or physical attacks;
- human errors of omission or commission;
- structural failures of organisation-controlled resources (e.g., hardware, software, environmental controls);
- natural and man-made disasters, accidents, and failures beyond the control of the organisation.

Various taxonomies of threat sources have been developed. Some taxonomies of threat sources use the type of adverse impacts as an organising principle. Multiple threat sources can initiate or cause the same threat event—for example, a provisioning server can be taken off-line by a denial-of-service attack, a deliberate act by a malicious system administrator, an administrative error, a hardware fault, or a power failure.

Table 9 Possible inputs to threat source identification task (adapted from (National Institute of Standards and Technology, 2012))

Description	Provided To		
	Tier 1	Tier 2	Tier 3
From Tier 1: (Organisation level) ■ Sources of threat information deemed to be credible (e.g., open source and/or classified threat reports, previous risk/threat assessments). ■ Threat source information and guidance specific to Tier 1 (e.g., threats related to organisational governance, core missions/business functions, management/ operational policies, procedures, and structures, external mission/business relationships). ■ Taxonomy of threat sources, annotated by the organisation, if necessary. ■ Characterization of adversarial and non-adversarial threat sources. ■ Assessment scales for assessing adversary capability, intent, and targeting, annotated by the organisation, if necessary. ■ Assessment scale for assessing the range of effects, annotated by the organisation, if necessary. ■ Threat sources identified in previous risk assessments, if appropriate.	No	Yes	Yes if not provided by Tier 2
From Tier 2: (Mission/business process level) ■ Threat source information and guidance specific to Tier 2 (e.g., threats related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies). ■ Mission/business process-specific characterization of adversarial and non-adversarial threat sources.	Yes via RAR	Yes via peer sharing	Yes
From Tier 3: (Information system level) ■ Threat source information and guidance specific to Tier 3 (e.g., threats related to information systems, information technologies, information system components, applications, networks, environments of operation). ■ Information system-specific characterization of adversarial and non-adversarial threat sources.	Yes via RAR	Yes via RAR	Yes via peer sharing

Table 10 Taxonomy of threat sources (National Institute of Standards and Technology, 2012)

Type of Threat Source	Description	Characteristics
ADVERSARIAL ■ Individual - Outsider - Insider - Trusted Insider - Privileged Insider ■ Group - Ad hoc - Established ■ Organisation - Competitor - Supplier - Partner - Customer ■ Nation-State	Individuals, groups, organisations, or states that seek to exploit the organisation's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).	Capability, Intent, Targeting
ACCIDENTAL ■ User ■ Privileged User/Administrator	Erroneous actions taken by individuals in the course of executing their everyday responsibilities.	Range of effects
STRUCTURAL ■ Information Technology (IT) Equipment - Storage - Processing - Communications - Display - Sensor - Controller ■ Environmental Controls - Temperature/Humidity Controls - Power Supply ■ Software - Operating System - Networking - General-Purpose Application - Mission-Specific Application	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.	Range of effects
ENVIRONMENTAL ■ Natural or man-made disaster - Fire - Flood/Tsunami - Windstorm/Tornado - Hurricane - Earthquake - Bombing - Overrun ■ Unusual Natural Event (e.g., sunspots) ■ Infrastructure Failure/Outage - Telecommunications - Electrical Power	Natural disasters and failures of critical infrastructures on which the organisation depends, but which are outside the control of the organisation. Note: Natural and man-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities housing mission-critical systems, making those systems unavailable for three weeks).	Range of effects

Table 11 Threat sources identification and assessment - characteristics of adversary capabilities (National Institute of Standards and Technology, 2012)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.
High	80-95	8	The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.
Moderate	21-79	5	The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.
Low	5-20	2	The adversary has limited resources, expertise, and opportunities to support a successful attack.
Very Low	0-4	0	The adversary has very limited resources, expertise, and opportunities to support a successful attack.

Table 12 Threat sources identification and assessment - characteristics of adversary intent (National Institute of Standards and Technology, 2012)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary seeks to undermine, severely impede, or destroy a core mission or business function, program, or enterprise by exploiting a presence in the organisation's information systems or infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede its ability to complete stated goals.
High	80-95	8	The adversary seeks to undermine/impede critical aspects of a core mission or business function, program, or enterprise, or place itself in a position to do so in the future, by maintaining a presence in the organisation's information systems or infrastructure. The adversary is very concerned about minimizing attack detection/disclosure of tradecraft, particularly while preparing for future attacks.
Moderate	21-79	5	The adversary seeks to obtain or modify specific critical or sensitive information or usurp/disrupt the organisation's cyber resources by establishing a foothold in the organisation's information systems or infrastructure. The adversary is concerned about minimizing attack detection/disclosure of tradecraft, particularly when carrying out attacks over long time periods. The adversary is willing to impede aspects of the organisation's missions/business functions to achieve these ends.
Low	5-20	2	The adversary actively seeks to obtain critical or sensitive information or to usurp/disrupt the organisation's cyber resources and does so without concern about attack detection/disclosure of tradecraft.
Very Low	0-4	0	The adversary seeks to usurp, disrupt, or deface the organisation's cyber resources, and does so without concern about attack detection/disclosure of tradecraft.

Table 13 Threat sources identification and assessment - characteristics of adversary targeting (National Institute of Standards and Technology, 2012)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary analyses information obtained via reconnaissance and attacks to target persistently a specific organisation, enterprise, program, mission or business function, focusing on specific high- value or mission-critical information, resources, supply flows, or functions; specific employees or positions; supporting infrastructure providers/suppliers; or partnering organisations.
High	80-95	8	The adversary analyses information obtained via reconnaissance to target persistently a specific organisation, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions, specific employees supporting those functions, or key positions.
Moderate	21-79	5	The adversary analyses publicly available information to target persistently specific high-value organisations (and key positions, such as Chief Information Officer), programs, or information.
Low	5-20	2	The adversary uses publicly available information to target a class of high-value organisations or information, and seeks targets of opportunity within that class.
Very Low	0-4	0	The adversary may or may not target any specific organisations or classes of organisations.

Table 14 Threat sources identification - range of effects for non-adversarial sources

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The effects of the error, accident, or act of nature are **sweeping**, involving almost all of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organisation/governance structure].
High	80-95	8	The effects of the error, accident, or act of nature are **extensive**, involving most of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organisation/governance structure], including many critical resources.
Moderate	21-79	5	The effects of the error, accident, or act of nature are **wide-ranging**, involving a significant portion of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organisation/governance structure], including some critical resources.
Low	5-20	2	The effects of the error, accident, or act of nature are **limited**, involving some of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organisation/governance structure], but involving no critical resources.
Very Low	0-4	0	The effects of the error, accident, or act of nature are **minimal**, involving few if any of the cyber resources of the [Tier 3: information systems; Tier 2: mission/business processes or EA segments, common infrastructure, or support services; Tier 1: organisation/governance structure], and involving no critical resources.

Appendix 2C - Threats events identification

It is important to identify potential threat events, relevance of the events, and the threat sources that could initiate the events along with tactics, techniques and procedures (TTPs) to carry out the attacks (for adversarial events). Since a threat source can initiate many events and an event might be initiated by more than one source there can be a many-to-many relationship among threat sources and events which eventually will increase the complexity of a risk assessment. For each threat event identified the relevance to the organisation must be defined. The tables provided below can help in each of the sub-activities required to complete the task. To identify how each event can harm organisational operations, assets, individuals or the whole organisation general descriptions are provided for adversarial events and non-adversarial events. A quantification of the relevance of the event serving as well as a linkage to the organisation's risk tolerance are required. The more risk averse, the greater the value is considered. When accepting a greater risk or having a higher risk tolerance, it is more likely to require substantive evidence before considering more in depth threat events. If a threat event is considered as irrelevant, no further consideration is given. For relevant threat events, all threat sources that could initiate the event need to be identified. Alternatively, the set of all possible threat sources that could lead to a threat event can be identified.

Determine the likelihood that threat events of concern result in adverse impacts, considering: (i) the characteristics of the threat sources that could initiate the events;

i. the vulnerabilities/predisposing conditions identified;

ii. the organisational susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.

For adversarial threats, an assessment of likelihood of occurrence is typically based on: (i) adversary intent; (ii) adversary capability; and (iii) adversary targeting. For those other than adversarial threat events, the likelihood of occurrence is estimated using historical evidence, empirical data, or other factors.

Note that the likelihood that a threat event will be initiated or will occur is assessed with respect to a specific time frame (e.g., the next six months, the next year, or the period until a specified milestone is reached). If a threat event is almost certain to be initiated or occur in the (specified or implicit) time frame, the risk assessment may take into consideration the estimated frequency of the event. The likelihood of threat occurrence can also be based on the state of the organisation (including for example, its core mission/business processes, enterprise architecture, information security architecture, information systems, and environments in which those systems operate)—taking into consideration predisposing conditions and the presence and effectiveness of deployed security controls to protect against unauthorised/undesirable behaviour, detect and limit damage, and/or maintain or restore mission/business capabilities. The likelihood of impact addresses the probability (or possibility) that the threat event will result in an adverse impact, regardless of the magnitude of harm that can be expected.

To determine the overall likelihood of threat events organisations typically need to consider the likelihood that threat events will be initiated (for adversarial threat events) or will occur (for non-adversarial threat events). They must also consider the likelihood that the threat events once initiated or occurring, will result in adverse impacts or harm to organisational operations and assets, individuals or other organisations. Finally, the overall likelihood as a combination of likelihood of event initiation/occurrence and likelihood of the event resulting in adverse impact must be considered.

Table 15 Possible inputs for the threat identification task (adapted from (National Institute of Standards and Technology, 2012))

Description	Provided To		
	Tier 1	Tier 2	Tier 3
From Tier 1: (Organisation level) ■ Sources of threat information deemed to be credible (e.g., open source and/or classified threat reports, previous risk/threat assessments. ■ Threat event information and guidance specific to Tier 1 (e.g., threats related to organisational governance, core missions/business functions, external mission/business relationships, management/operational policies, procedures, and structures). ■ Exemplary adversarial threat events, annotated by the organisation, if necessary. ■ Exemplary non-adversarial threat events, annotated by the organisation, if necessary. ■ Assessment scale for assessing the relevance of threat events, annotated by the organisation, if necessary. ■ Threat events identified in previous risk assessments, if appropriate.	No	Yes	Yes If not provided by Tier 2
From Tier 2: (Mission/business process level) ■ Threat event information and guidance specific to Tier 2 (e.g., threats related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies). ■ Mission/business process-specific characterization of adversarial and non-adversarial threat events.	Yes Via RAR	Yes Via Peer Sharing	Yes
From Tier 3: (Information system level) ■ Threat event information and guidance specific to Tier 3 (e.g., threats related to information systems, information technologies, information system components, applications, networks, environments of operation). ■ Information system-specific characterization of adversarial and non-adversarial threat events. ■ Incident reports.	Yes Via RAR	Yes Via RAR	Yes Via Peer Sharing

Table 16 Examples of adversarial threat events (continued below) (National Institute of Standards and Technology, 2012)

Threat Events (Characterized by TTPs)	Description
Perform reconnaissance and gather information.	
Perform perimeter network reconnaissance/ scanning.	Adversary uses commercial or free software to scan organisational perimeters to obtain a better understanding of the information technology infrastructure and improve the ability to launch successful attacks.
Perform network sniffing of exposed networks.	Adversary with access to exposed wired or wireless data channels used to transmit information, uses network sniffing to identify components, resources, and protections.
Gather information using open source discovery of organisational information.	Adversary mines publicly accessible information to gather information about organisational information systems, business processes, users or personnel, or external relationships that the adversary can subsequently employ in support of an attack.
Perform reconnaissance and surveillance of targeted organisations.	Adversary uses various means (e.g., scanning, physical observation) over time to examine and assess organisations and ascertain points of vulnerability.
Perform malware-directed internal reconnaissance.	Adversary uses malware installed inside the organisational perimeter to identify targets of opportunity. Because the scanning, probing, or observation does not cross the perimeter, it is not detected by externally placed intrusion detection systems.
Craft or create attack tools.	
Craft phishing attacks.	Adversary counterfeits communications from a legitimate/trustworthy source to acquire sensitive information such as usernames, passwords, or SSNs. Typical attacks occur via email, instant messaging, or comparable means; commonly directing users to websites that appear to be legitimate sites, while actually stealing the entered information.
Craft spear phishing attacks.	Adversary employs phishing attacks targeted at high value targets (e.g., senior leaders/ executives).
Craft attacks specifically based on deployed information technology environment.	Adversary develops attacks (e.g., crafts targeted malware) that take advantage of adversary knowledge of the organisational information technology environment.
Create counterfeit/spoof website.	Adversary creates duplicates of legitimate websites; when users visit a counterfeit site, the site can gather information or download malware.
Craft counterfeit certificates.	Adversary counterfeits or compromises a certificate authority, so that malware or connections will appear legitimate.
Create and operate false front organisations to inject malicious components into the supply chain.	Adversary creates false front organisations with the appearance of legitimate suppliers in the critical life-cycle path that then inject corrupted/malicious information system components into the organisational supply chain.
Deliver/insert/install malicious capabilities.	
Deliver known malware to internal organisational information systems (e.g., virus via email).	Adversary uses common delivery mechanisms (e.g., email) to install/insert known malware (e. g., malware whose existence is known) into organisational information systems.
Deliver modified malware to internal organisational information systems.	Adversary uses more sophisticated delivery mechanisms than email (e.g., web traffic, instant messaging, FTP) to deliver malware and possibly modifications of known malware to gain access to internal organisational information systems.
Deliver targeted malware for control of internal systems and exfiltration of data.	Adversary installs malware that is specifically designed to take control of internal organisational information systems, identify sensitive information, exfiltrate the information back to adversary, and conceal these actions.
Deliver malware by providing removable media.	Adversary places removable media (e.g., flash drives) containing malware in locations external to organisational physical perimeters but where employees are likely to find the media (e.g., facilities parking lots, exhibits at conferences attended by employees) and use it on organisational information systems.

Threat Events (Characterized by TTPs)	Description
Insert untargeted malware into downloadable software and/or into commercial information technology products.	Adversary corrupts or inserts malware into common freeware, shareware or commercial information technology products. Adversary is not targeting specific organisations, simply looking for entry points into internal organisational information systems. Note that this is particularly a concern for mobile applications.
Insert targeted malware into organisational information systems and information system components.	Adversary inserts malware into organisational information systems and information system components (e.g., commercial information technology products), specifically targeted to the hardware, software, and firmware used by organisations (based on knowledge gained via reconnaissance).
Insert specialized malware into organisational information systems based on system configurations.	Adversary inserts specialized, non-detectable, malware into organisational information systems based on system configurations, specifically targeting critical information system components based on reconnaissance and placement within organisational information systems.
Insert counterfeit or tampered hardware into the supply chain.	Adversary intercepts hardware from legitimate suppliers. Adversary modifies the hardware or replaces it with faulty or otherwise modified hardware.
Insert tampered critical components into organisational systems.	Adversary replaces, though supply chain, subverted insider, or some combination thereof, critical information system components with modified or corrupted components.
Install general-purpose sniffers on organisation-controlled information systems or networks.	Adversary installs sniffing software onto internal organisational information systems or networks.
Install persistent and targeted sniffers on organisational information systems and networks.	Adversary places within internal organisational information systems or networks software designed to (over a continuous period of time) collect (sniff) network traffic.
Insert malicious scanning devices (e.g., wireless sniffers) inside facilities.	Adversary uses postal service or other commercial delivery services to deliver to organisational mailrooms a device that is able to scan wireless communications accessible from within the mailrooms and then wirelessly transmit information back to adversary.
Insert subverted individuals into organisations.	Adversary places individuals within organisations who are willing and able to carry out actions to cause harm to organisational missions/business functions.
Insert subverted individuals into privileged positions in organisations.	Adversary places individuals in privileged positions within organisations who are willing and able to carry out actions to cause harm to organisational missions/business functions. Adversary may target privileged functions to gain access to sensitive information (e.g., user accounts, system files, etc.) and may leverage access to one privileged capability to get to another capability.
Exploit and compromise.	
Exploit physical access of authorised staff to gain access to organisational facilities.	Adversary follows ("tailgates") authorised individuals into secure/controlled locations with the goal of gaining access to facilities, circumventing physical security checks.
Exploit poorly configured or unauthorised information systems exposed to the Internet.	Adversary gains access through the Internet to information systems that are not authorised for Internet connectivity or that do not meet organisational configuration requirements.
Exploit split tunneling.	Adversary takes advantage of external organisational or personal information systems (e.g., laptop computers at remote locations) that are simultaneously connected securely to organisational information systems or networks and to nonsecure remote connections.
Exploit multi-tenancy in a cloud environment.	Adversary, with processes running in an organisationally used cloud environment, takes advantage of multi-tenancy to observe behavior of organisational processes, acquire organisational information, or interfere with the timely or correct functioning of organisational processes.
Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones).	Adversary takes advantage of fact that transportable information systems are outside physical protection of organisations and logical protection of corporate firewalls, and compromises the systems based on known vulnerabilities to gather information from those systems.
Exploit recently discovered vulnerabilities.	Adversary exploits recently discovered vulnerabilities in organisational information systems in an attempt to compromise the systems before mitigation measures are available or in place.

Threat Events (Characterized by TTPs)	Description
Exploit vulnerabilities on internal organisational information systems.	Adversary searches for known vulnerabilities in organisational internal information systems and exploits those vulnerabilities.
Exploit vulnerabilities using zero-day attacks.	Adversary employs attacks that exploit as yet unplublicised vulnerabilities. Zero-day attacks are based on adversary insight into the information systems and applications used by organisations as well as adversary reconnaissance of organisations.
Exploit vulnerabilities in information systems timed with organisational mission/business operations tempo.	Adversary launches attacks on organisations in a time and manner consistent with organisational needs to conduct mission/business operations.
Exploit insecure or incomplete data deletion in multi-tenant environment.	Adversary obtains unauthorised information due to insecure or incomplete data deletion in a multi-tenant environment (e.g., in a cloud computing environment).
Violate isolation in multi-tenant environment.	Adversary circumvents or defeats isolation mechanisms in a multi-tenant environment (e.g., in a cloud computing environment) to observe, corrupt, or deny service to hosted services and information/data.
Compromise critical information systems via physical access.	Adversary obtains physical access to organisational information systems and makes modifications.
Compromise information systems or devices used externally and reintroduced into the enterprise.	Adversary installs malware on information systems or devices while the systems/devices are external to organisations for purposes of subsequently infecting organisations when reconnected.
Compromise software of organisational critical information systems.	Adversary inserts malware or otherwise corrupts critical internal organisational information systems.
Compromise organisational information systems to facilitate exfiltration of data/information.	Adversary implants malware into internal organisational information systems, where the malware over time can identify and then exfiltrate valuable information.
Compromise mission-critical information.	Adversary compromises the integrity of mission-critical information, thus preventing or impeding ability of organisations to which information is supplied, from carrying out operations.
Compromise design, manufacture, and/or distribution of information system components (including hardware, software, and firmware).	Adversary compromises the design, manufacture, and/or distribution of critical information system components at selected suppliers.
Conduct an attack (i.e., direct/coordinate attack tools or activities).	
Conduct communications interception attacks.	Adversary takes advantage of communications that are either unencrypted or use weak encryption (e.g., encryption containing publically known flaws), targets those communications, and gains access to transmitted information and channels.
Conduct wireless jamming attacks.	Adversary takes measures to interfere with wireless communications so as to impede or prevent communications from reaching intended recipients.
Conduct attacks using unauthorised ports, protocols and services.	Adversary conducts attacks using ports, protocols, and services for ingress and egress that are not authorised for use by organisations.
Conduct attacks leveraging traffic/data movement allowed across perimeter.	Adversary makes use of permitted information flows (e.g., email communication, removable storage) to compromise internal information systems, which allows adversary to obtain and exfiltrate sensitive information through perimeters.
Conduct simple Denial of Service (DoS) attack.	Adversary attempts to make an internet-accessible resource unavailable to intended users, or prevent the resource from functioning efficiently or at all, temporarily or indefinitely.
Conduct Distributed Denial of Service (DDoS) attacks.	Adversary uses multiple compromised information systems to attack a single target, thereby causing denial of service for users of the targeted information systems.
Conduct targeted Denial of Service (DoS) attacks.	Adversary targets DoS attacks to critical information systems, components, or supporting infrastructures, based on adversary knowledge of dependencies.
Conduct physical attacks on organisational facilities.	Adversary conducts a physical attack on organisational facilities (e.g., sets a fire).
Conduct physical attacks on infrastructures supporting organisational facilities.	Adversary conducts a physical attack on one or more infrastructures supporting organisational facilities (e.g., breaks a water main, cuts a power line).
Conduct cyber-physical attacks on organisational facilities.	Adversary conducts a cyber-physical attack on organisational facilities (e.g., remotely changes HVAC settings).

Threat Events (Characterized by TTPs)	Description
Conduct data scavenging attacks in a cloud environment.	Adversary obtains data used and then deleted by organisational processes running in a cloud environment.
Conduct brute force login attempts/password guessing attacks.	Adversary attempts to gain access to organisational information systems by random or systematic guessing of passwords, possibly supported by password cracking utilities.
Conduct nontargeted zero-day attacks.	Adversary employs attacks that exploit as yet unplublicised vulnerabilities. Attacks are not based on any adversary insights into specific vulnerabilities of organisations.
Conduct externally-based session hijacking.	Adversary takes control of (hijacks) already established, legitimate information system sessions between organisations and external entities (e.g., users connecting from off-site locations).
Conduct internally-based session hijacking.	Adversary places an entity within organisations in order to gain access to organisational information systems or networks for the express purpose of taking control (hijacking) an already established, legitimate session either between organisations and external entities (e.g., users connecting from remote locations) or between two locations within internal networks.
Conduct externally-based network traffic modification (man in the middle) attacks.	Adversary, operating outside organisational systems, intercepts/eavesdrops on sessions between organisational and external systems. Adversary then relays messages between organisational and external systems, making them believe that they are talking directly to each other over a private connection, when in fact the entire communication is controlled by the adversary. Such attacks are of particular concern for organisational use of community, hybrid, and public clouds.
Conduct internally-based network traffic modification (man in the middle) attacks.	Adversary operating within the organisational infrastructure intercepts and corrupts data sessions.
Conduct outsider-based social engineering to obtain information.	Externally placed adversary takes actions (e.g., using email, phone) with the intent of persuading or otherwise tricking individuals within organisations into revealing critical/ sensitive information (e.g., personally identifiable information).
Conduct insider-based social engineering to obtain information.	Internally placed adversary takes actions (e.g., using email, phone) so that individuals within organisations reveal critical/sensitive information (e.g., mission information).
Conduct attacks targeting and compromising personal devices of critical employees.	Adversary targets key organisational employees by placing malware on their personally owned information systems and devices (e.g., laptop/notebook computers, personal digital assistants, smart phones). The intent is to take advantage of any instances where employees use personal information systems or devices to handle critical/sensitive information.
Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware.	Adversary targets and compromises the operation of software (e.g., through malware injections), firmware, and hardware that performs critical functions for organisations. This is largely accomplished as supply chain attacks on both commercial off-the-shelf and custom information systems and components.
Achieve results (i.e., cause adverse impacts, obtain information)	
Obtain sensitive information through network sniffing of external networks.	Adversary with access to exposed wired or wireless data channels that organisations (or organisational personnel) use to transmit information (e.g., kiosks, public wireless networks) intercepts communications.
Obtain sensitive information via exfiltration.	Adversary directs malware on organisational systems to locate and surreptitiously transmit sensitive information.
Cause degradation or denial of attacker-selected services or capabilities.	Adversary directs malware on organisational systems to impair the correct and timely support of organisational mission/business functions.
Cause deterioration/destruction of critical information system components and functions.	Adversary destroys or causes deterioration of critical information system components to impede or eliminate organisational ability to carry out missions or business functions. Detection of this action is not a concern.
Cause integrity loss by creating, deleting, and/or modifying data on publicly accessible information systems (e.g., web defacement).	Adversary vandalizes, or otherwise makes unauthorised changes to, organisational websites or data on websites.
Cause integrity loss by polluting or corrupting critical data.	Adversary implants corrupted and incorrect data in critical data, resulting in suboptimal actions or loss of confidence in organisational data/services.

Threat Events (Characterized by TTPs)	Description
Cause integrity loss by injecting false but believable data into organisational information systems.	Adversary injects false but believable data into organisational information systems, resulting in suboptimal actions or loss of confidence in organisational data/services.
Cause disclosure of critical and/or sensitive information by authorised users.	Adversary induces (e.g., via social engineering) authorised users to inadvertently expose, disclose, or mishandle critical/sensitive information.
Cause unauthorised disclosure and/or unavailability by spilling sensitive information.	Adversary contaminates organisational information systems (including devices and networks) by causing them to handle information of a classification/sensitivity for which they have not been authorised. The information is exposed to individuals who are not authorised access to such information, and the information system, device, or network is unavailable while the spill is investigated and mitigated.
Obtain information by externally located interception of wireless network traffic.	Adversary intercepts organisational communications over wireless networks. Examples include targeting public wireless access or hotel networking connections, and drive-by subversion of home or organisational wireless routers.
Obtain unauthorised access.	Adversary with authorised access to organisational information systems, gains access to resources that exceeds authorization.
Obtain sensitive data/information from publicly accessible information systems.	Adversary scans or mines information on publicly accessible servers and web pages of organisations with the intent of finding sensitive information.
Obtain information by opportunistically stealing or scavenging information systems/components.	Adversary steals information systems or components (e. g., laptop computers or data storage media) that are left unattended outside of the physical perimeters of organisations or scavenges discarded components.
Maintain a presence or set of capabilities.	
Obfuscate adversary actions.	Adversary takes actions to inhibit the effectiveness of the intrusion detection systems or auditing capabilities within organisations.
Adapt cyber attacks based on detailed surveillance.	Adversary adapts behavior in response to surveillance and organisational security measures.
Coordinate a campaign.	
Coordinate a campaign of multi-staged attacks (e.g., hopping).	Adversary moves the source of malicious commands or actions from one compromised information system to another, making analysis difficult.
Coordinate a campaign that combines internal and external attacks across multiple information systems and information technologies.	Adversary combines attacks that require both physical presence within organisational facilities and cyber methods to achieve success. Physical attack steps may be as simple as convincing maintenance personnel to leave doors or cabinets open.
Coordinate campaigns across multiple organisations to acquire specific information or achieve desired outcome.	Adversary does not limit planning to the targeting of one organisation. Adversary observes multiple organisations to acquire necessary information on targets of interest.
Coordinate a campaign that spreads attacks across organisational systems from existing presence.	Adversary uses existing presence within organisational systems to extend the adversary's span of control to other organisational systems including organisational infrastructure. Adversary thus is in position to further undermine organisational ability to carry out missions/ business functions.
Coordinate a campaign of continuous, adaptive, and changing cyber attacks based on detailed surveillance.	Adversary attacks continually change in response to surveillance and organisational security measures.
Coordinate cyber attacks using external (outsider), internal (insider), and supply chain (supplier) attack vectors.	Adversary employs continuous, coordinated attacks, potentially using all three attack vectors for the purpose of impeding organisational operations.

Table 17 Examples of non-adversarial threat events (National Institute of Standards and Technology, 2012)

Threat Event	Description
Spill sensitive information	Authorised user erroneously contaminates a device, information system, or network by placing on it or sending to it information of a classification/sensitivity which it has not been authorised to handle. The information is exposed to access by unauthorised individuals, and as a result, the device, system, or network is unavailable while the spill is investigated and mitigated.
Mishandling of critical and/or sensitive information by authorised users	Authorised privileged user inadvertently exposes critical/sensitive information.
Incorrect privilege settings	Authorised privileged user or administrator erroneously assigns a user exceptional privileges or sets privilege requirements on a resource too low.
Communications contention	Degraded communications performance due to contention.
Unreadable display	Display unreadable due to aging equipment.
Earthquake at primary facility	Earthquake of organisation-defined magnitude at primary facility makes facility inoperable.
Fire at primary facility	Fire (not due to adversarial activity) at primary facility makes facility inoperable.
Fire at backup facility	Fire (not due to adversarial activity) at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
Flood at primary facility	Flood (not due to adversarial activity) at primary facility makes facility inoperable.
Flood at backup facility	Flood (not due to adversarial activity) at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
Hurricane at primary facility	Hurricane of organisation-defined strength at primary facility makes facility inoperable.
Hurricane at backup facility	Hurricane of organisation-defined strength at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
Resource depletion	Degraded processing performance due to resource depletion.
Introduction of vulnerabilities into software products	Due to inherent weaknesses in programming languages and software development environments, errors and vulnerabilities are introduced into commonly used software products.
Disk error	Corrupted storage due to a disk error.
Pervasive disk error	Multiple disk errors due to aging of a set of devices all acquired at the same time, from the same supplier.
Windstorm/tornado at primary facility	Windstorm/tornado of organisation-defined strength at primary facility makes facility inoperable.
Windstorm/tornado at backup facility	Windstorm/tornado of organisation-defined strength at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.

Table 18 Identification of relevance of threat events to the organisation (National Institute of Standards and Technology, 2012)

Value	Description
Confirmed	The threat event or TTP has been seen by the organisation.
Expected	The threat event or TTP has been seen by the organisation's peers or partners.
Anticipated	The threat event or TTP has been reported by a trusted source.
Predicted	The threat event or TTP has been predicted by a trusted source.
Possible	The threat event or TTP has been described by a somewhat credible source.
N/A	The threat event or TTP is not currently applicable. For example, a threat event or TTP could assume specific technologies, architectures, or processes that are not present in the organisation, mission/business process, EA segment, or information system; or predisposing conditions that are not present (e.g., location in a flood plain). Alternately, if the organisation is using detailed or specific threat information, a threat event or TTP could be deemed inapplicable because information indicates that no adversary is expected to initiate the threat event or use the TTP.

Appendix 3A – Vulnerabilities and predisposing conditions identification

Most information system vulnerabilities can be associated with security controls that either have not been applied (either intentionally or unintentionally), or have been applied, but retain some weakness. However, it is also important to allow for the possibility of emergent vulnerabilities that can arise naturally over time as organisational missions/business functions evolve, environments of operation change, new technologies proliferate, and new threats emerge. In the context of such change, existing security controls may become inadequate and may need to be reassessed for effectiveness. The tendency for security controls to potentially degrade in effectiveness over time reinforces the need to maintain risk assessments during the entire system development life cycle and also the importance of continuous monitoring programs to obtain ongoing situational awareness of the organisational security posture

In addition to vulnerabilities, organisations also need to consider predisposing conditions. A predisposing condition is a condition that exists within an organisation, a mission or business process, enterprise architecture, information system, or environment of operation, which affects the likelihood that threat events, once initiated, result in adverse impacts to the organisational operations and assets, individuals, and other organisations.

Predisposing conditions include, for example, the location of a facility in a hurricane – or flood-prone region (increasing the likelihood of exposure to hurricanes or floods) or a stand-alone information system with no external network connectivity (decreasing the likelihood of exposure to a network-based cyber-attack). Vulnerabilities resulting from predisposing conditions that cannot be easily corrected could include, for example, gaps in contingency plans, use of outdated technologies, or weaknesses/deficiencies in information system backup and failover mechanisms. In all cases, these types of vulnerabilities create a predisposition toward threat events having adverse impacts on organisations. Vulnerabilities (including those attributed to predisposing conditions) are part of the overall security posture of organisational information systems and environments of operation that can affect the likelihood of occurrence of a threat event.

Table 19 Possible inputs to the vulnerabilities and predisposing conditions identification (adapted from (National Institute of Standards and Technology, 2012))

Description	Provided To		
	Tier 1	Tier 2	Tier 3
From Tier 1 (Organisation level) ■ Sources of vulnerability information deemed to be credible (e.g., open source and/or classified vulnerabilities, previous risk/vulnerability assessments, Mission and/or Business Impact Analyses). ■ Vulnerability information and guidance specific to Tier 1 (e.g., vulnerabilities related to organisational governance, core missions/business functions, management/operational policies, procedures, and structures, external mission/ business relationships). ■ Taxonomy of predisposing conditions, annotated by the organisation, if necessary. ■ Characterization of vulnerabilities and predisposing conditions. ■ Assessment scale for assessing the severity of vulnerabilities, annotated by the organisation, if necessary. ■ Assessment scale for assessing the pervasiveness of predisposing conditions, annotated by the organisation, if necessary. ■ Business Continuity Plan, Continuity of Operations Plan for the organisation, if such plans are defined for the entire organisation.	No	Yes	Yes If not provided by Tier 2
From Tier 2: (Mission/business process level) ■ Vulnerability information and guidance specific to Tier 2 (e.g., vulnerabilities related to organisational mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies). ■ Business Continuity Plans, Continuity of Operations Plans for mission/business processes, if such plans are defined for individual processes or business units.	Yes Via RAR	Yes Via Peer Sharing	Yes
From Tier 3: (Information system level) ■ Vulnerability information and guidance specific to Tier 3 (e.g., vulnerabilities related to information systems, information technologies, information system components, applications, networks, environments of operation). ■ Security assessment reports (i.e., deficiencies in assessed controls identified as vulnerabilities). ■ Results of monitoring activities (e.g., automated and nonautomated data feeds). ■ Vulnerability assessments, Red Team reports, or other reports from analyses of information systems, subsystems, information technology products, devices, networks, or applications. ■ Contingency Plans, Disaster Recovery Plans, Incident Reports. ■ Vendor/manufacturer vulnerability reports.	Yes Via RAR	Yes Via RAR	Yes Via Peer Sharing

Table 20 Assessment scale for vulnerability's severity (National Institute of Standards and Technology, 2012)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The vulnerability is exposed and exploitable, and its exploitation could result in severe impacts. Relevant security control or other remediation is not implemented and not planned; or no security measure can be identified to remediate the vulnerability.
High	80-95	8	The vulnerability is of high concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is planned but not implemented; compensating controls are in place and at least minimally effective.
Moderate	21-79	5	The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is partially implemented and somewhat effective.
Low	5-20	2	The vulnerability is of minor concern, but effectiveness of remediation could be improved. Relevant security control or other remediation is fully implemented and somewhat effective.
Very Low	0-4	0	The vulnerability is not of concern. Relevant security control or other remediation is fully implemented, assessed, and effective.

Table 21 Taxonomy of predisposing conditions relevant to vulnerability (National Institute of Standards and Technology, 2012)

Type of Predisposing Condition	Description
INFORMATION-RELATED ■ Classified National Security Information ■ Compartments ■ Controlled Unclassified Information ■ Personally Identifiable Information ■ Special Access Programs ■ Agreement-Determined - NOFORN - Proprietary	Needs to handle information (as it is created, transmitted, stored, processed, and/or displayed) in a specific manner, due to its sensitivity (or lack of sensitivity), legal or regulatory requirements, and/or contractual or other organisational agreements.
TECHNICAL ■ Architectural - Compliance with technical standards - Use of specific products or product lines - Solutions for and/or approaches to user-based collaboration and information sharing - Allocation of specific security functionality to common controls ■ Functional - Networked multiuser - Single-user - Stand-alone / nonnetworked - Restricted functionality (e.g., communications, sensors, embedded controllers)	Needs to use technologies in specific ways.
OPERATIONAL / ENVIRONMENTAL ■ Mobility - Fixed-site (specify location) - Semi-mobile - Land-based, Airborne, Sea-based, Space-based - Mobile (e.g., handheld device) ■ Population with physical and/or logical access to components of the information system, mission/business process, EA segment - Size of population - Clearance/vetting of population	Ability to rely upon physical, procedural, and personnel controls provided by the operational environment.

Table 22 Pervasiveness of predisposing conditions (National Institute of Standards and Technology, 2012)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Applies to all organisational missions/business functions (Tier 1), mission/ business pro-cesses (Tier 2), or information systems (Tier 3).
High	80-95	8	Applies to most organisational missions/business functions (Tier 1), mission/ business processes (Tier 2), or information systems (Tier 3).
Moderate	21-79	5	Applies to many organisational missions/business functions (Tier 1), mission/ business processes (Tier 2), or information systems (Tier 3).
Low	5-20	2	Applies to some organisational missions/business functions (Tier 1), mission/ business processes (Tier 2), or information systems (Tier 3).
Very Low	0-4	0	Applies to few organisational missions/business functions (Tier 1), mission/ business processes (Tier 2), or information systems (Tier 3).

Appendix 3B - Further vulnerabilities assessment methods

Originating from the domain of Information Technology (IT), a vulnerability is defined as a weakness that might be exploited by cyber attackers to compromise a system. Similarly, a smart manufacturing system might have security vulnerabilities; that is unexpected weaknesses, due to the complexity of the interconnection between the different pieces of equipment within a system. The categories of a vulnerability can be:

- Remote access vulnerability
- Software vulnerability
- Local Area Network (LAN) or Wireless LAN (WLAN)

There are two main techniques for identifying the vulnerabilities of a system: Gap assessment and Penetration testing. Additionally, active and passive assessments can be used. The sections below describe the methodologies.

Gap assessment

The aim of a gap assessment is to identify and quantify the differences between the current and target states. To achieve this it is essential to carry out employee interviews, site tours and business policy/procedure reviews. Company processes, personnel and technology should be involved. Supplementary to a gap assessment, passive or active assessments can be used.

Current state definition

This step is around determining the current state of the system(s) to assess. The following standards can support this activity as follows:

- ISO27001 – Create an asset inventory [source].
- IEC62443-3-2:2020 – Segmentation methodology for structuring a model of the ICS into simple zones and conduits between them.
- NIST-SP800-30 - this proposes a system characterisation under the Risk Management guide for information technology systems [source].

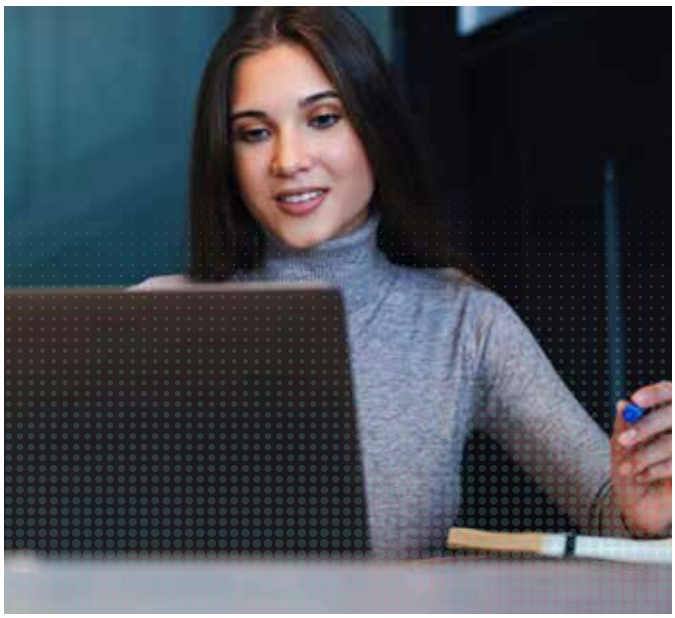
Target state definition

At this step the expectations for cyber security controls, processes and procedures are set. In this activity IT, OT, Physical security and HR are working together to agree on a common set of security controls. Interviews and review of organisational procedures can feed into that as well.

Gap Analysis

With the current and target states defined, a gap analysis can be undertaken to identify and quantify the differences so that the necessary actions to achieve the desired status can be decided and planned. The following standards can provide further instructions in detail.

- IEC 62443-3-3:2019 - introduces the security levels to use in the gap analysis, to address the gaps and suggests a standardised nomenclature.
- NIST-SP800-30 - this standard proposes practices for vulnerability identification that can also be used for gaps classification (source).



Penetration testing

Penetration testing [source] is a method for assuring that an IT system is secure, by attempting to breach some or all of the system's security using tools and techniques that an adversary might employ. Therefore security vulnerabilities are discovered. Penetration testing is not a primary method for identifying vulnerabilities, but can be used to validate and test effectiveness of countermeasures followed by a risk assessment.

Penetration testing is a suitable approach for identifying vulnerabilities and risks on an operational system consisting of components and services from multiple vendors. Also it is a useful method for systems and applications developed in-house. However it is not appropriate to use it for product specific testing. A penetration test can only validate systems' security on known issues on the day of the test. It is very common that vulnerabilities might exist for long periods of time without knowing them if only penetration testing is used to check and validate a system's security.

Types of penetration test

Several tests can be conducted depending on the purpose of the audit. Some cases are illustrated below.

1. Test basis can be carried out by testers provided or not with information about the system under consideration.

a. White-box testing - full information about the target system is given to the tester. This test checks the effectiveness of internal vulnerability assessment and controls applied by identifying known software issues, vulnerabilities and misconfigurations on the systems.

b. Black-box testing - no information around the target is given to the tester with the aim to identify ways to access the under testing system or asset. The benefit of this approach is that it models more accurately the risks faced by an attacker that are unknown. The lack of information can also help in discovering vulnerabilities unknown during the time of the test.

2. Test type can be run as either a white-box or black-box operation.

a. Vulnerability identification in bespoke or niche software. This is usually carried out in web applications and provides feedback on coding practices that avoid introducing the categories of vulnerability identified.

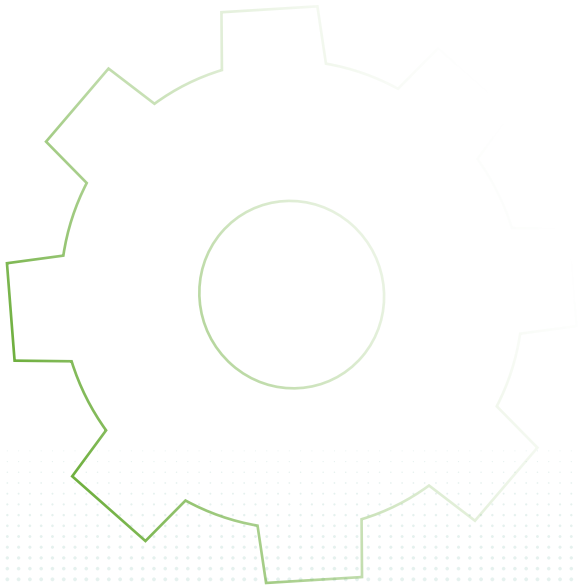
b. Scenario driven testing for identifying vulnerabilities - a particular scenario is explored to test if it leads to a vulnerability. Possible scenarios may include: lost laptop, unauthorised device connected to internal network, compromised host and many others.

c. Scenario driven testing for detection and response capability. The aim is to measure capabilities on detecting and responding to various vulnerabilities. The test's efficacy is limited to the specific scenario on each test for the relevant capabilities.

Active and passive assessment

To perform an active assessment, this involves the use of tools (e.g. Nmap, Shodan, Nessus) to scan the network to discover devices on the network, device software/ firmware versions and potential vulnerabilities. The main goal of it is to place traffic on the IACS network which could introduce risk and detect the outcomes.

In the case of passive assessment, the focus is on discovering network devices using passive means such as site surveys, network/architecture drawings, system logs, equipment configuration files, network traffic analysis. The team can also review equipment data against vulnerability databases.



Appendix 4A – Risk quantification

As presented in the introduction, the outcome of a risk analysis is to preserve the confidentiality, integrity and availability of the assets within a manufacturing environment. Therefore, for a deeper investigation and risk assessment, it suggested that for each risk identified and linked to a threat or vulnerability a connection should be made with regards to the kind of impacts from the perspective of the CIA triad and the type of loss that can be caused (i.e. loss of confidentiality, integrity or availability). Below are provided some examples with regards to designing a risk assessment matrix. There can be a variety in the dimensions of the matrix depending on the level and depth of the analysis. Additional information can be found in [source, IEC 62443-3-2:2020, Annex B].

Table 23 Example of a 3x3 risk matrix

Likelihood				
	Highly likely	Medium	High	High
	Possible	Low	Medium	High
	Unlikely	Low	Low	Medium
		Negligible	Moderate Impact	Severe

Table 24 Example of a 5x5 risk matrix

		Consequence				
		Minor problem (Easily handled by normal day-to-day processes)	Some distribution possible (Damage between $500k and $1MM)	Significant time and resources required (Damage between $1MM and $10MM)	Operations severly damaged (Damage between $10MM and $25MM)	Business survival at risk (Damage >$25MM)
Likelihood	Almost certain (>90%)	High	High	Extreme	Extreme	Extreme
	Likely (50% - 90%)	Moderate	High	High	Extreme	Extreme
	Moderate (10% - 50%)	Low	Moderate	High	Extreme	Extreme
	Unikely (3% - 10%)	Low	Low	Moderate	Extreme	Extreme
	Rare (>3%)	Low	Low	Moderate	High	High

Table 25 Example of a 5x5 risk matrix

		Severity			
		Minor problem (Easily handled by normal day-to-day processes)	Some distribution possible (Damage between $500k and $1MM)	Significant time and resources required (Damage between $1MM and $10MM)	Operations severly damaged (Damage between $10MM and $25MM)
Likelihood	Imbrobable (Risk is unlikely to occur)	Low - 1 -	Medium - 4 -	Medium - 6 -	High - 10 -
	Likely (50% - 90%)	Low - 1 -	Medium - 5 -	High - 8 -	Extreme - 11 -
	Moderate (10% - 50%)	Medium - 3 -	High - 7 -	High - 9 -	Extreme - 12 -

Appendix 5A – Risk Review

Once the business has reviewed the threat landscape, as well as it's appetite for risk, the business must then consider how often the business should re-review potential risks and its appetite for them. It is recommended that a business reviews the risks & appetite as regularly as possible to reduce how susceptible a system/business is to risk, however, this is heavily dependent on the business/system, and will depend on factors such as:

- The budget/resources set aside for cyber security
- The size of the business and the number of employees
- The number of assets and devices
- The amount and type of data

Appendix 5B – Training

Cyber security awareness training should be provided to any new starters as well as must be continuously provided and updated to all current members of staff involved in the business or the development of a system. The rate in which this training is provided is subject to the resources available and at the discretion of the business or system owner providing said training. As a general rule users who are involved in cyber security within a business or during the development of a system should be trained more frequently than others, however, everyone should be given some cyber security training [source]. The purpose of this is to not only inform but to create a positive security based culture where users not only follow the rules outlined in the training but also consider the cyber security implications whenever they carry out a task.

To further adhere to the goal of cyber security awareness and training, the following steps [source] can also be taken to manage cyber security risk and support employees:

- Produce & adhere to user security policies - Includes security procedures for all systems with considerations to different roles within a business.
- Establish a staff induction process - New users should be made aware of their personal responsibilities when it comes to cyber security.
- Monitor effectiveness of security training - Involves establishing mechanisms to test the effectiveness of the cyber security training.
- Incident reporting & learning - Staff should be empowered to voice security concerns or incidents without fear and should someone cause an incident they should be confident to report the incident and learn from the incident without the fear of any repercussions (within reason).

Appendix 5C – Passwords & access Control

Below is a list of security practices [source] that can be used to improve password security or improve the security of a system that uses passwords:

1. Multi-factor authentication (MFA) - This involves the use of a password in addition to a second factor which only the user can access. This could be a code sent via SMS/email, a third-party application code or event that needs to be used or even biometrics.
2. Throttling & account lockout - This restricts the number of guesses a user can attempt before the account locks, forcing the user to contact their local system admin and prove their identity.
3. Monitoring - This monitors the number of attempts a user has made logging into a system as well as attempts made to access MFA. This is mainly used in conjunction with throttling.
4. Password deny lists - This is a database of the most commonly used passwords (such as “password”, “123456789”, “qwerty”, etc…) which is looked over whenever a user changes passwords or signs up for an account. If the user attempts to use a password on the list, they will be prompted to re-think their choices.
5. Changing default passwords - IT & OT software/ hardware can sometimes come pre-configured with default passwords or accounts of which are contained within the manual for said software/hardware. These default credentials should be changed as soon as possible to prevent a breach.
6. Password management software - This is software that can keep track of a user’s passwords for a range of different accounts, helping the user to remember their password. This is normally protected by a master password as well as MFA, however, users should be careful with this option as if a malicious actor gained access to their password manager, they would have all of their passwords.
7. Use strong passwords or passphrases - Normally used in conjunction with password managers, users can create passwords which consist of many different characters (normally 12 or more letters numbers and symbols) which can be hard to crack and guess. These generated passwords are also difficult to remember and so passphrases can be used instead which is a string of random dictionary words (usually 4 or more).

In addition to passwords, access control (both physical and digital) should also be considered when implementing general cyber security best practices. This focuses on securing information or services contained within business systems as well as securing the physical premises containing information in all forms. For access control to be possible, a user must be registered via an account/s or a record within the business or system, of which, will contain the access rights associated with said user.

Access controls should be approved and regularly reviewed by asset owners with the idea that everyone should be restricted in the information/assets they can access and restrictions for a user should only be lifted when they can show a valid reason or business requirement e.g. needing to work with said information or asset. When said reason or business requirement is presented, then users should only have access to said information, network, or asset that they have been authorised to use. Examples of access controls can include buildings or areas a user is authorised to enter, assets a user is authorised to access, data a user is authorised to view and/or edit, etc... Access controls should be reviewed within a business or system whenever someone joins or leaves and should be reviewed periodically based on the business/system needs.

Appendix 5D – Patch management

Once a vulnerability has been identified within a product, the product owner/vendor will review the vulnerability and produce a patch which will usually be available as an update to the product.

Reviews for these vulnerabilities should be carried out often, subject to the businesses cyber security requirements, and should be the responsibility of personnel familiar with the system and the use cases. This allows for areas of exposure and risk to be more easily identified. When an issue is identified, this should be assessed in the same manner, all other risks using the above guidance to determine the priority and risk level. Mitigating controls should then be put in place immediately to minimise the risk, and the user should determine via the vendor whether a patch is available.

Patches should be tested before being deployed to live/production environments and should only be obtained from reputable sources, ideally directly from the OEM / OEM recommended distributors. When applying patches, the user/system owner should have a repeatable, methodical approach in place before beginning the patching process. This approach should implement some of the points below:

- The user should back up the system, and should identify key components such as what data needs backing up, whether any configuration/settings require backing up, and whether any bespoke programs or code should be backed up. This is useful should something go wrong during the patching process.
- The user should have in place a set of testing procedures to ensure that the patch fixes the issues it was designed to and does not introduce any new issues.
- The user should identify critical systems that will be affected and should create a priority order to determine which systems/assets should be patched first.
- The user should identify critical components that need to be patched and should not patch anything that has a patch available. It is important to consider whether a component is still required within a system and whether another approach should be used or whether the component could be removed entirely before patching it.

Original Equipment Manufacturers (OEMs) usually publish a vulnerability report on their website detailing the issue, the products affected and mitigating actions to prevent exploitation while a patch is produced. If this is not the case, this may be a newly discovered vulnerability and should be reported to the OEM. It is also advised that users stay up to date with the latest issues facing industrial control systems devices and should check sources such as the alerts section of the CISA website or NIST for vulnerability disclosures and/or NCSC weekly threat report.

It is worth noting that Patching is not a solution to security, only a specific vulnerability, applying all the patches will not make a solution totally secure.

Appendix 5E – System partitioning & segmentation

For a user to achieve system partitioning and segmentation, they must first group assets within a system together into zones or conduits based on factors such as risk (after a risk assessment has been completed), criticality, function, physical/logical location, required access and/or responsible party [source].

Zone: Consists of the grouping of cyber assets that share the same cyber security requirements

Conduit: Consists of the grouping of cyber assets dedicated exclusively to communications, and which share the same cyber security requirements"

The reasoning for the partitioning/segmentation of assets is to group assets that share common security requirements into zones/conduits so that common security measures can be applied to mitigate risk. An example of this is that a manufacturing environment and its subsequent system could be divided up into zones relating to their operation e.g. material storage, treatment, processing, etc. This could be further segmented into functional layers i.e. those defined within the 5 layers of automation (ERP, MES, SCADA, PLC, Production).

Once segmented, mitigating actions such as firewalls can be applied to the connection of each zone or conduit. Creating zones and conduits also has the added benefit of should a zone or conduit become infected with malware or other malicious code, then that malicious content is confined to the zone/conduit it is currently in instead of being spread to the whole system.

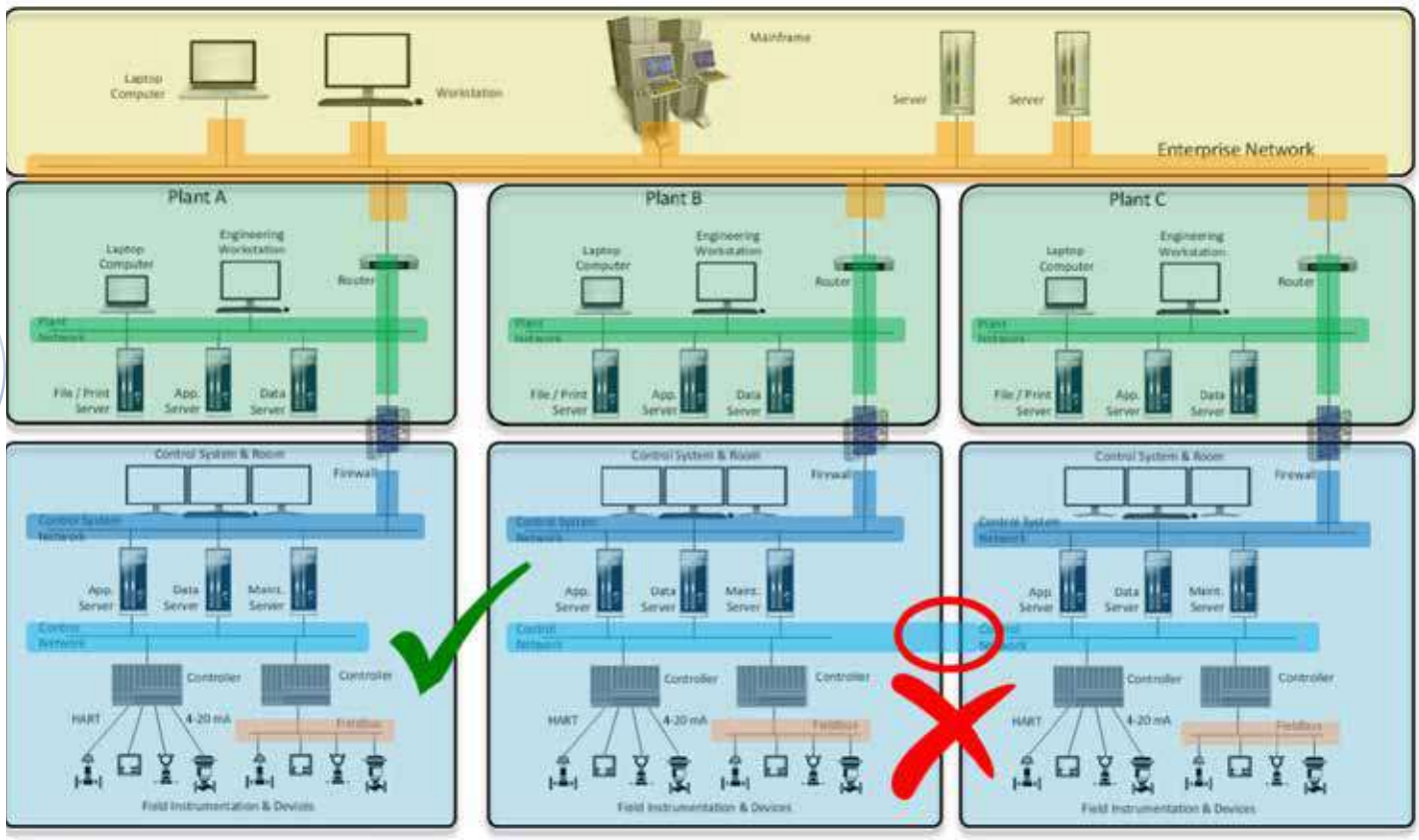


Figure 19 Example of correct and wrong partitioning and segmentation of assets (Source: ISA Global Cybersecurity Alliance)

This preventative measure is best applied during the design & implementation of a system instead of a preventative measure for an already established system. The reasoning for this is because it will be more costly and time consuming to partition/segment and already existing system, resulting in down-time within a business. Should this not be of concern, then it is recommended that a system is partitioned/segmented to reduce the risks within a system, established or otherwise.

Appendix 5F – Technical controls and countermeasures

General preventative measures and security practices are the first step in reducing the risk within a business/system, however, are not the only answer. These methods are usually used in conjunction with other methods such as implementing technical controls and countermeasures. These technical controls will defend a system/network against a range of attacks and are used to reduce the risk to a business/system by preventing and monitoring malicious content within a system/network. When implementing technical controls & countermeasures, the solutions below should be considered.

Appendix 5F – Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS)

Intrusion Detection Systems (IDS): Intrusion Detection Systems are passive systems that monitor the network traffic within a system by making a copy of the packets coming over the network and analysing the signature of each packet [source]. This allows the IDS to identify malicious content being sent over the network without affecting the network packets themselves. When malicious packets are detected, the user is warned so that they can take action in identifying where said packets came from and what they contained. The disadvantage of this is that although it can identify malicious network packets, it can't do anything to prevent them.

Some examples of IDS include SolarWinds Security Event Manager, Kismet, Zeek, Open DLP, Sagan, and Suricata.

Intrusion Prevention System (IPS): Intrusion Prevention Systems are active systems that, similar to IDS, monitor the network traffic within a system. This allows IPS to monitor malicious content over the network, however unlike IDS, IPS can block any malicious content by analysing the packets headers and payloads. As IPS only analyses the packet's headers and content, it can't do as much as IDS in preventing future malicious content from being sent as there is less information to analyse.

Some examples of IDS include SolarWinds Security Event Manager, Datadog Real-time Threat Monitoring, Zeek, Splunk, Sagan, and Fail2Ban [source].

Appendix 5F – Security information & Event Management (SIEM)

Contextual information such as data related to users, assets, threats, and vulnerabilities can also be combined with the log data to provide a full overview of the information captured by the SIEM system. This data can then be used for analytical and forensic purposes to identify risk and vulnerabilities within the system and create plans to mitigate said risk/vulnerabilities.

This functionality allows SIEM solutions to be used in many scenarios [source], such as:

- Real-Time Monitoring - Monitor, find, and stop threats in real-time.
- Incident Response - Addressing & managing potential breaches as well as the aftermath of security breaches to limit damage and recovery time.
- User Monitoring - Monitoring of user activity and privileges to pinpoint breaches and monitor user security compliance.
- Threat Intelligence - Recognise abnormal activity, assess the risk, and prioritise the response.
- Advanced Analytics - Producing insights from collected data.
- Advanced Threat Detection - Monitor, analyse, and detect threats.

Some examples of SIEM solutions [source] include Arcsight ESM, IBM QRadar and Splunk.

Appendix 5F – Malware & antivirus protection

Malware is malicious software that can affect assets such as computers and controllers within a system [source]. Malware usually consists of malicious code that can affect many parts of a system including the data stored within which malware can steal, edit, encrypt, or delete. Malware can be passed from device to device on a network, but is usually first downloaded to a device within a system via a malicious file/document that is sent via email, removable media device, or even malicious website. Once a system is infected with Malware, more vulnerabilities and breaches can be created via the malware as it spreads from device to device within a system, affecting the network and the devices as it spreads.

To defend against malware and other malicious code, it is recommended that Antivirus protection is installed which is used to detect, quarantine, and/or delete malicious code so that it does not affect the device/system. Most modern-day operating systems (OSs) come with built in antivirus protection, however, this is very basic and may not catch all malicious content on a device. Other third-party antivirus software can be installed and deployed to a device to improve the malicious content detection capabilities, however, this adds additional costs.

Appendix 5G – Mitigation strategies & defence-in-depth

When creating a mitigation strategy, the risks and vulnerabilities previously identified within the system should be the core in which the strategy is based around [source]. To create a mitigation strategy, the user must first identify the risks within their system and the likelihood of said risks being exploited. Once the user is aware of the risks, they can assess which risks are acceptable and which need mitigating. The user must then identify which mitigating actions will best reduce the likelihood and severity of each risk. Please see the General Preventative Measures & Security Practices and the Technical Controls & Countermeasures sections for methods of mitigating risks.

One widely used strategy is the Defence-in-Depth strategy which looks to integrate "people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organisation" and or system [source]. This means that no one single solution is used, but multiple different solutions for many different assets and risks across all layers of the organisation or system. The idea of this approach is to raise the cost of an intrusion for a malicious actor to break into a system, whilst improving the probability of detecting said intrusion and providing the capabilities to deal with it.

Appendix 5H – Residual risk & acceptable Risk

Residual risk refers to the remaining risk after control and mitigation measures have been implemented. The main purpose of identifying the residual risks is to measure the effectiveness of the mitigating actions that were applied to the original risk and to assist with monitoring risks within a system or business.

Acceptable risk refers to "the level of Residual Risk that has been determined to be a reasonable level of potential loss/disruption for a specific IT system" [source]. The acceptable risk level is usually defined when a system owner or business performs a risk review and defines the risk appetite for the system/business. This accepted level of risk is heavily influenced by the health & safety and legal requirements within a system/business. As previously mentioned, no system can be 100% secure and so the user needs to define a level of risk within a business or system that they would find acceptable to have.

For a residual risk to be considered acceptable, the user needs to compare the residual risk (using the quantitative scores within the risk assessment) to the risk level the business/user defined as acceptable during the risk review stage. If the residual risk level is equal to or lower than that of the acceptable level, then the residual risk can now be considered acceptable. Should the residual risk level be higher than the acceptable level, then more mitigating actions are required to decrease the residual risk level to a more acceptable one. This can be done by either applying more mitigating actions to the one residual risk, or by breaking down the residual risk into smaller risks and applying mitigating actions to each one individually.

Once a risk is considered acceptable, it can't be forgotten about, it must be monitored to make sure the risk level never increases and to make sure any mitigating actions put in place are still valid. To this extent, it is recommended that information captured during previous risk assessments is maintained or extended upon so that the accepted risks from past risk assessments can be identified and re-evaluated when the risk assessment is carried out again.

Appendix 5I – Incident response and recovery plan

A response plan can't be as simple as turning off all affected assets and disconnecting them from the network as this may lose important information for understanding a breach. A good response and recovery plan looks to prevent the loss of data, decrease the system down-time and allow the user to analyse the breach after it has occurred. In addition to the business related reasons, some regulatory departments require a response & recovery plan to be in place, should the system have an effect on the health & safety of others or use an individual's personal data in some way. This section therefore seeks to provide the user with a general overview of how to create a response and recovery plan.

Before any recovery & response plan can be created, the business/user first needs to define a few things such as what the user/business defines as an incident or breach. As a general rule, an incident or breach is an adverse event that has a negative consequence within a system such as malware which destroys data. The reason for this definition is so that the user/business knows what events within a system are considered an incident/ breach and whether they require a response. Once a user/business has defined this, they must then identify the individuals/teams that will be involved in responding to the incident and they should also define the expectations and capabilities the user/business wants the response team to provide. This team should consist of individuals/teams that have in-depth knowledge of the system, including both IT & OT devices. The final thing that needs to be put into place before defining a recovery/response plan is the policies and procedures that everyone involved with the incident is required to follow. These policies and procedures should include the following [source]:

- The purpose & objectives of the policy
- The scope of the policy ("to whom and what it applies and under what circumstances")
- The definition of a security incident or breach and any related terms
- The organisational structure in relation to the incident team
- The responsibilities and level of authority of the incident team as well as any expectations
- The levels of communication e.g. how/when the incident team can and should interact with other third parties such as law enforcement, the media, third party incident response teams, etc.
- The severity rating for incidents and how they are prioritised
- Performance measures
- Reporting & contact details

Once the above policies are in place, a response plan can then be constructed for how an organisation or system owner responds to any incidents within a system. This plan should look to involve specific elements, such as the mission/objective, key contacts with the levels of elevation, and an overview of the incident response process. The incident response process is a grouping of processes that looks to secure a system after an incident has occurred. This process has 4 main stages:

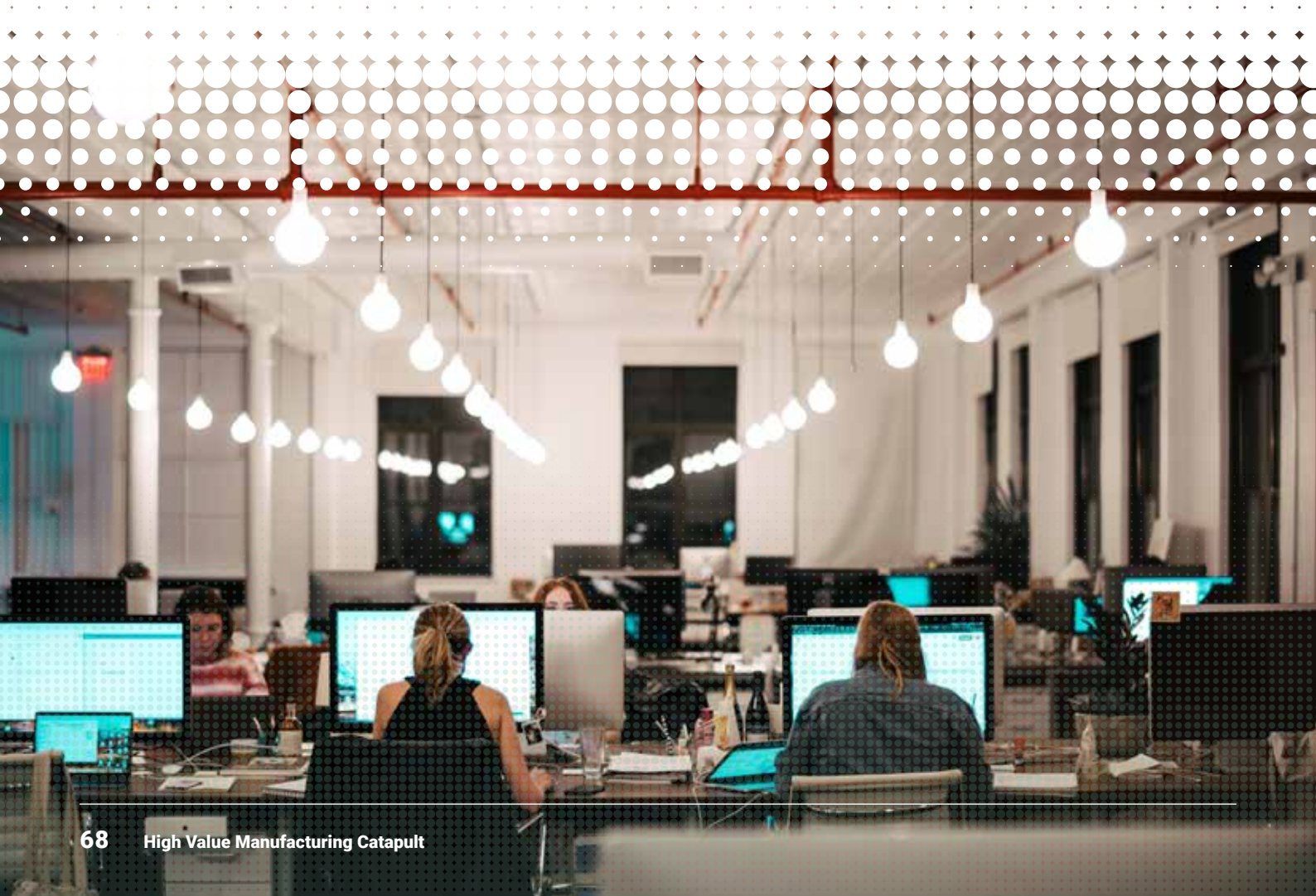
1. Preparation: This refers to any actions that may be carried out prior to a cyber security incident and can include conducting a risk assessment to assess the SUC and identify and vulnerabilities or risks. This stage can also include the gathering of information, both relevant to components within the system and the staff members involved.
2. Detection & Analysis: This refers to the detection of vulnerabilities via a range of methods including detecting vulnerabilities using the risk assessment conducted in the preparation phase, through intrusion detection or prevention systems, or through the analysis of past incidents.
3. Containment, Eradication, & Recovery: This looks at how breaches within a system/organisation can be contained & eradicated. Once these stages have been completed, this stage will then look at how the user can begin to recover aspects of the system that may have become corrupted or vulnerable.

Containment of a breach is an important step in mitigating the amount of damage a breach can cause to an organisation or system. To contain a breach, the organisation and/or system owner must first put in place a list of containment strategies based on the type of incident that occurs i.e. the containment strategy for an email-based malware breach will be different to that of a network-based Distributed Denial of Service. Containment also does not prevent a breach from causing further damage to the system.

Once contained, the malicious content/breach can be eradicated by deleting the malware and disabling any breached user accounts. This also includes mitigating any and all vulnerabilities in the system that were the initial cause of the breach to prevent the exact same breach happening again.

Finally once all of the malicious content is eradicated, then the system can be restored back to its normal functioning state. This can be done by:

- Restoring the system from a clean back-up
- Rebuilding the system from scratch
- Installing patches
- Replacing compromised files
- Changing passwords
- Increasing network security.



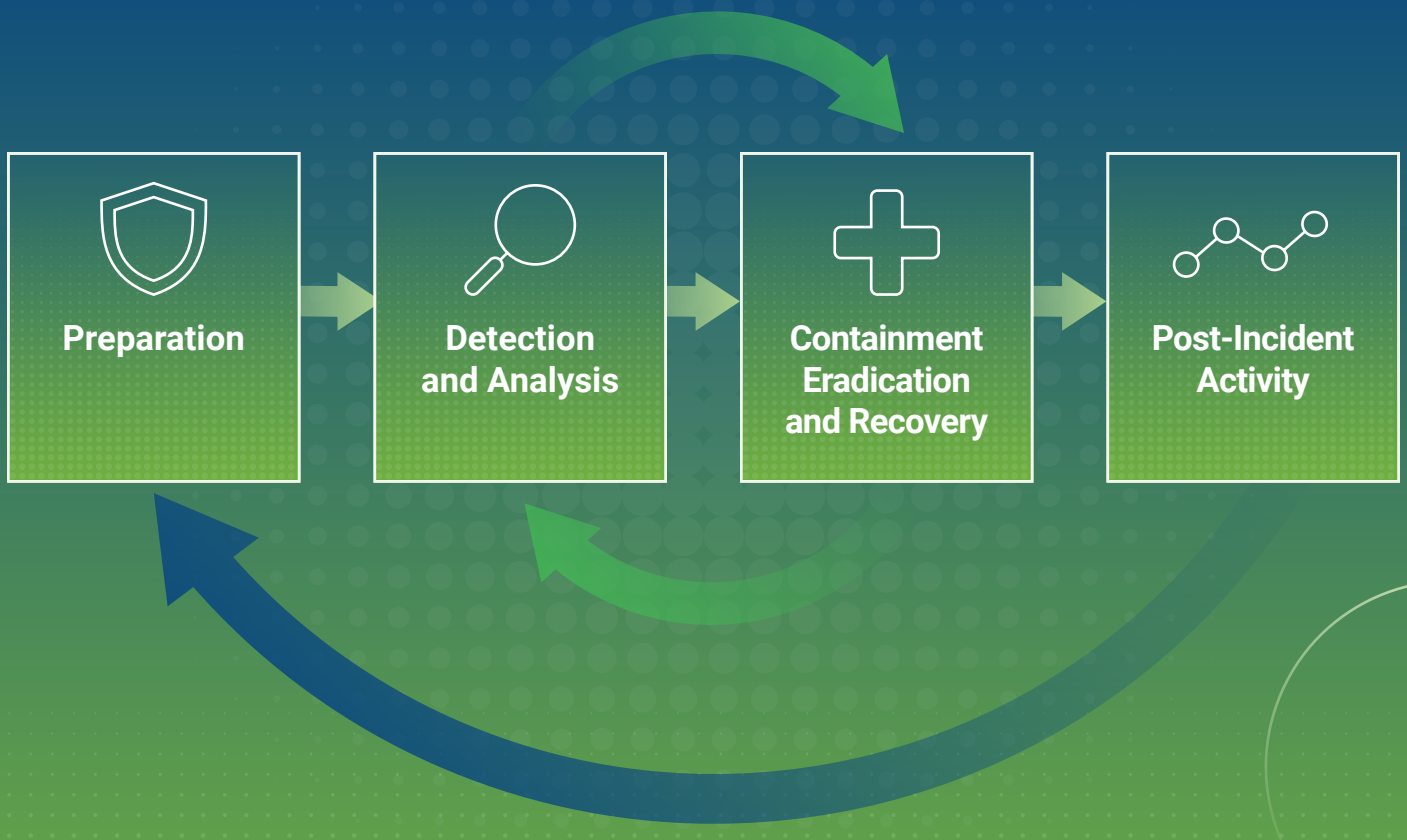
The recovery step can take anywhere from a couple of days to months depending on the size of the breach, number of affected accounts/assets, and back-up capabilities of the system owner/organisations.

4. Post-Incident Activities: The final process looks at the lessons learnt from the breach, and looks at how the system can be improved to decrease the number of risks within the system. This can consist of a meeting soon after the breach has been resolved that consists of all of the major parties involved in dealing with the breach. This process should look at:

- What happened during the breach and when?
- How did employees handle the breach and were the procedures followed?
- Are the current cyber security policies and procedures adequate?
- How the breach could originally have been mitigated and was a vulnerability overlooked?
- What additional tools, resources, and security measures are required in the future?

This process should also look to collect relevant information from the incident and store it for future use. This can be collated to show the number of incidents that have occurred over time, how long each incident lasted from the time of the initial breach to the recovery of the system, and an objective & subjective overview of each incident looking at the data captured and how each incident was handled. Any data captured during the incident response should be used to improve on the current incident response & recovery plan.

Figure 20 Post-incident activities overview



References

[i]Anon., n.d. ISO Guide 73:2009 Risk Management - Vocabulary.
[Online] Available at: https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en [Accessed 13 09 2021].

Cisco Press, 2009. Network Security Using Cisco IOS IPS.
[Online] Available at: https://www.ciscopress.com/articles/article.asp?p=1336425 [Accessed 13 09 2021].

Cisco, n.d. What Is a Firewall?. [Online] Available at: https://www.cisco.com/c/en_uk/products/security/firewalls/what-is-a-firewall.html [Accessed 13 09 2021].

Colón, M., 2019. Why Your Cyber Risk Tolerance May Be Lower Than You Think.
[Online] Available at: https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/why-your-cyber-risk-tolerance-may-be-lower-than-you-think/ [Accessed 13 09 2021].

Cybersecurity and Infrastructure Security Agency , 2020. CYBER RESILIENCE REVIEW (CRR) - Question Set with Guidance, s.l.: U.S. Department of Homeland Security.

dig8ital, n.d. DO YOU KNOW YOUR CYBER RISK APPETITE?.
[Online] Available at: https://dig8ital.com/resources/library/its-time-to-identify-your-cyber-security-risk-appetite [Accessed 13 09 2021].

DNS Stuff, 2020. 7 Best Intrusion Detection Software and Latest IDS Systems.
[Online] Available at: https://www.dnsstuff.com/network-intrusion-detection-software [Accessed 13 09 2021].

EDUCAUSE, n.d. Incident Management and Response.
[Online] Available at: https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/incident-management-and-response [Accessed 13 09 2021].

Gartner, n.d. What is Security Information and Event Management (SIEM)?.
[Online] Available at: https://www.gartner.com/reviews/market/security-information-event-management [Accessed 13 09 2021].

Homeland Security, 2016. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies.
[Online] Available at: https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf [Accessed 13 09 2021].

IEC technical committee 65, 2020. Security for Industrial Automation and Control Systems - Part 3-2: Security Risk Assessment for System Design, s.l.: BSI Standards Publication.

Imperva, n.d. Security information and event management (SIEM).
[Online] Available at: https://www.imperva.com/learn/application-security/siem/ [Accessed 13 09 2021].

IsecT Ltd., 2013. ISO/IEC 27001.
[Online] Available at: https://www.iso27001security.com/html/27001.html [Accessed 13 09 2021].

Kon, M., n.d. How to Define Zones and Conduits.
[Online] Available at: https://gca.isa.org/blog/how-to-define-zones-and-conduits [Accessed 13 09 2021].

LANGNER, 2019. The five things you need to know about OT/ICS vulnerability and patch management.
[Online] Available at: https://www.langner.com/2019/02/the-five-things-you-need-to-know-about-ot-ics-vulnerability-and-patch-management/ [Accessed 13 09 2021].

Lebanidze, E., n.d. Guide to Developing a Cyber Security and Risk Mitigation Plan, Arlington: National Rural Electric Cooperative Association.

National Cyber Security Centre, 2015. Reducing your exposure to cyber attack.
[Online] Available at: https://www.ncsc.gov.uk/information/reducing-your-exposure-to-cyber-attack [Accessed 13 09 2021].

National Cyber Security Centre, 2017. Penetration Testing.
[Online] Available at: https://www.ncsc.gov.uk/guidance/penetration-testing [Accessed 13 09 2021].

National Cyber Security Centre, 2018. Password administration for system owners.
[Online] Available at: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach [Accessed 13 09 2021].

National Cyber Security Centre, 2019. NCSC CAF guidance.
[Online] Available at: https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/b-6-staff-awareness-and-training [Accessed 13 09 2021].

National Cyber Security Centre, 2019. What is an antivirus product? Do I need one?.
[Online] Available at: https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product [Accessed 13 09 2021].

National Cyber Security Centre, 2021. 10 Steps to Cyber Security.
[Online] Available at: https://www.ncsc.gov.uk/collection/10-steps/architecture-and-configuration [Accessed 13 09 2021].

National Cyber Security Centre, n.d. What is cyber security?.
[Online] Available at: https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security [Accessed 13 09 2021].

National Institute of Standards and Technology, 1998. Acceptable Risk, Washington, D.C: U.S. Department of Commerce.

National Institute of Standards and Technology, 2012. Guide for Conducting Risk Assessments , Washington, D.C.: U.S. Department of Commerce.

National Institute of Standards and Technology, n.d.
[Online] Available at: https://csrc.nist.gov/glossary/term/residual_risk [Accessed 13 09 2021].

splunk, n.d. The SIEM Buyer's Guide for 2021.
[Online] Available at: https://www.splunk.com/pdfs/ebooks/the-siem-buyers-guide-for-2020.pdf [Accessed 13 09 2021].