EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Interoperable EU Risk Management Toolbox

FEBRUARY 2023

About ENISA

The European Union Agency for Cybersecurity (ENISA) is the EU's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with EU Member States and EU bodies and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the EU's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

Authors

Kostas Papadatos, Cyber Noesis

Konstantinos Rantos, Cyber Noesis

Argyris Makrygeorgou, Cyber Noesis

Konstantinos Koulouris, Cyber Noesis

Stefania Klontza, Cyber Noesis

Costas Lambrinoudakis, University of Piraeus

Stefanos Gritzalis, University of Piraeus

Christos Xenakis, University of Piraeus

Sokratis Katsikas, University of Piraeus

Maria Karyda, University of Piraeus

Aggeliki Tsochou, University of Piraeus

Alexandros Zacharis, ENISA

Legal notice

Copyright notice

Print ISBN 978-92-9204-609-5 doi:10.2824/713364 TP-04-22-275-EN-C
PDF ISBN 978-92-9204-608-8 doi:10.2824/68948 TP-04-22-275-EN-N

Contents

1. INTRODUCTION 6

1.1. Purpose and scope 6

1.2. Report structure 6

1.3. Definitions of abbreviations 7

2. INTEROPERABLE EU RM TOOLBOX 8

2.1. Method of work 8

2.2. EU RM toolbox description 8

2.3. Toolbox components 10

2.3.1. Knowledge base 10
2.3.2. Functional components 15

3. METHOD OF USE 16

3.1. Basic concepts and terms 16

3.2. Risk evaluation against a specific threat 17

3.3. Use case development process 19

4. TOOLBOX EVOLVEMENT 20

5. CONCLUSIONS 22

A Annex I – Toolbox terminology 23

B Annex II – Toolbox asset classification 32

C Annex III – Toolbox threat taxonomy 33

D Annex IV – Toolbox impact scale 41

E Annex V – Toolbox risk scale 43

F ANNEX VI – Risk calculation interoperability samples 45

G Annex VII – Toolbox libraries 46

H Annex VIII – Use case example 47

Scenario description 47

Indicative assets in scope 47

Attack path 48

Attack scenarios 49

Deliverables 51

6. BIBLIOGRAPHY/REFERENCES 52

Executive summary

The benefits of the European digital economy and society can only be fully attained under the premise of cybersecurity. All layers of society can be affected and the EU needs to be ready to respond to massive (large-scale and cross-border) cyberattacks and cyber crises. Cross-border interdependencies have highlighted the need for effective cooperation between EU Member States and EU institutions for a faster response and proper coordination of efforts at all levels (strategic, operational, technical and communications). Under this perspective, it is important not only to define interoperable terms in EU risk management (RM) and regulatory frameworks, but also to develop common/comparative risk scales, which will allow for the interpretation of the risk analysis outputs that result from different RM methods, so that the risk levels are comparable.

This document presents the EU RM toolbox, a solution proposed by ENISA to address interoperability concerns related to the use of information security RM methods. The toolbox aims to facilitate the smooth integration of various RM methods in an organisation's environment or across organisations and bridge the gaps associated with the methods' disparate respective approaches. With the help of the toolbox, shareholders will be able to have a common understanding of risks and report interoperable risk assessment results to the community and competent authorities.

1. Introduction

1.1. Purpose and scope

This report is part of ENISA's project 'Building interoperable EU risk management frameworks vol. 02', which extends and builds on prior work carried out in 2021 and produced the following reports:

1. *Interoperable EU Risk Management Framework* (https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework);
2. *Compendium of Risk Management Frameworks with Potential Interoperability* (https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks).

The interoperable EU RM toolbox (also referred to in this document as the 'toolbox') aims to provide a reference framework that supports the interpretation, comparison and aggregation of the results produced by different risk assessment methods. The EU RM toolbox will allow different stakeholders to work on common threats and risk scenarios and compare their risk levels, even if they are assessed through different or proprietary tools and methods. Such comparative results on the security posture of the organisations will allow different organisations, along with policymakers and regulators, to develop an integrated view on the cybersecurity posture of organisations against specific and/or emerging threats in specific sectors, and across different sectors and countries.

To this end, the EU RM toolbox will provide directions and facilitate the comparison and interpretation of the cybersecurity readiness of different information systems infrastructures against a specific threat scenario or a set of threat scenarios (e.g. physical threats).

The objective of this document is to define a scheme and the required set of components (common terminology, assets classification, threat taxonomy and impact/risk scales) that will allow for the interpretation of the risk analysis outputs that result from different RM frameworks.

1.2. Report structure

This report includes four sections: **Section 1 (Introduction)** defines the toolbox's purpose and scope; **Section 2 (Interoperable EU RM toolbox)** presents the concept, the scheme and the components of the toolbox; **Section 3 (Method of use)** outlines the way in which the EU RM toolbox will be used by stakeholders; and **Section 4 (Toolbox evolvement)** proposes ways in which the toolbox can be further enriched with additional information to achieve its long-term objectives. **Section 5 (Conclusions)** summarises our conclusions.

This report also includes the following annexes:

- Annex I – Terminology
- Annex II – Assets
- Annex III – Threats
- Annex IV – Impact levels
- Annex V – Risk levels
- Annex VI – Risk calculation interoperability samples
- Annex VII – Toolbox libraries
- Annex VIII – Use case example.

1.3. Definitions of abbreviations

The abbreviations used in this document and their definitions are listed below.

Abbreviation	Definition
API	application programming interface
CIS	communication and information system
DSO	distribution system operator
ICT	information and communications technology
IoT	internet of things
IT	information technology
ITSRM²	IT security risk management methodology
NIS	network and information systems
OT	operational technology
RM	risk management

2. Interoperable EU RM toolbox

2.1. Method of work

The EU RM toolbox has been designed and developed by building on the directions provided in the 2022 ENISA report *Interoperable EU Risk Management Framework*, so as to facilitate the uptake of a coordinated and interoperable RM framework that would provide a consistent methodology and risk assessment practices among Member States.

To design the EU RM toolbox, the results of assessing the potential interoperability of several prominent RM frameworks and methodologies, as included in the previous report, were considered. The toolbox is comprised of the main elements that were identified and assessed as important for the interoperability of RM methods, including the identification and categorisation of assets, the identification of threats, the description of attack scenarios, the assessment and comparison of risk levels, along with a common vocabulary that facilitates the understanding of the outcomes of different RM methods.

Finally, also drawing from the outcome of the 2022 ENISA report *Interoperable EU Risk Management Framework*, the method used to apply the toolbox follows the basic RM processes included in ISO/IEC 27005:2018 and the information technology security risk management methodology (ITSRM^2) method, as these were shown by the report to have provided extended opportunities for supporting interoperability.

2.2. EU RM toolbox description

The EU RM toolbox aims to provide stakeholders with a reference framework to align their RM efforts so that they have a common understanding about risks and associated risk levels, regardless of the RM approach they adopt and the tool(s) they use. Having said that, the EU RM toolbox respects the peculiarities of the corresponding RM methods and does not modify the way that organisations have been working towards the management of their information security risks. With the EU RM toolbox, stakeholders will be able to use interoperable components to compare results with other organisations for specific risk scenarios, even when using different RM methods and tools.

With the use of the EU RM toolbox, regulatory and supervisory bodies can have a horizontal view of the risk levels and the security posture of the organisations in a specific sector or in their domain of authority or jurisdiction, with regard to specific threats and risk scenarios (possible adverse events that can affect the organisation's strategy and objectives), and can therefore appropriately guide them. The alignment of the stakeholders' respective RM efforts and the normalisation of the corresponding results, using a reference framework and common metrics for risk levels, will help these entities better compare the outcomes and produce tangible results that will easily guide them in their follow-up activities.

Figure 1: The role of the EU RM toolbox and its positioning in the RM process

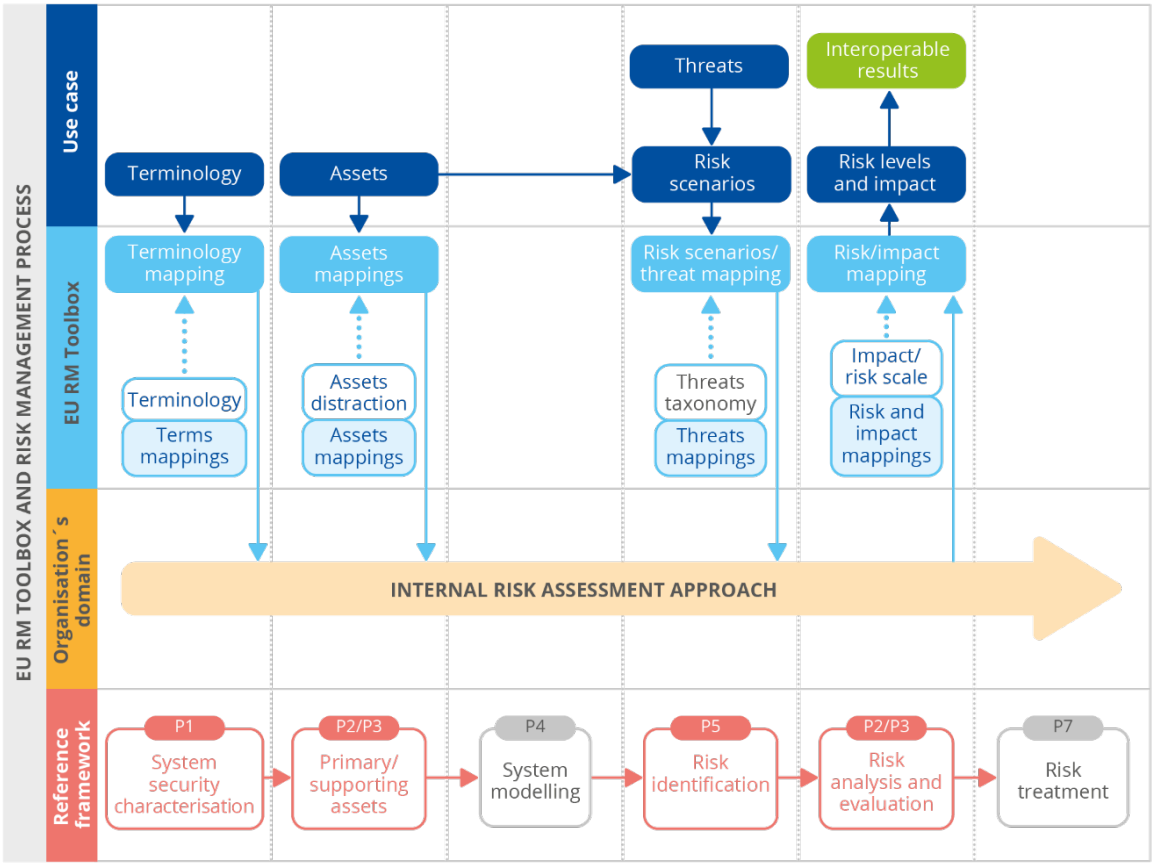


Figure 1 demonstrates the positioning of the EU RM toolbox with respect to the use case scenarios and the corresponding tools that the organisations utilise in their environment. The EU RM toolbox acts as an intermediate and abstract layer between the use case scenarios (i.e. the set of risk scenarios against which the organisation or a competent authority wants to assess risk levels) and the organisation-adopted RM methodology that is used for this assessment. To this end, the toolbox does not aim to alter the way that organisations manage risks internally. Instead, it provides stakeholders with the means to have a common understanding on risk scenarios and unambiguously interpret involved assets and threats prior to using the RM tools of their choice to assess risks, but also the means to interpret their calculated risk levels towards interoperable results.

Having said that, the toolbox interprets risk scenarios developed using the toolbox's terminology, assets classifications and threats taxonomies to the respective risk assessment methodologies, and normalises the risk assessment results to a common risk matrix that provides comparable results.

Using the ITSRM[2] as a reference framework for the RM activities, the EU RM toolbox facilitates the alignment of RM activities in four RM functions (Figure 1).

- **Establish a common understanding on the activities that will be undertaken during the RM process.** The EU RM toolbox provides a set of interoperable terms based on RM and regulatory frameworks as well as international standards that are used to establish the context of RM. This allows for an unambiguous description and understanding of the RM activities, regardless of the RM methodology used. If necessary, mappings between the EU RM toolbox and respective RM methodologies

terminology will complement the toolbox in the future, so that no ambiguous activities will emerge.

- **Define the scope of the environment in which the risk assessment process will be applied.** The EU RM toolbox contributes to this function by providing a classification of assets to categorise those involved in a risk scenario, and the organisation's additional assets found in the scoped environment. This classification facilitates the development of unambiguous risk scenarios and the proper interpretation for the respective assets that will be considered in the risk assessment process. Having identified and classified their assets using the provided categories, the organisations will be able to identify whether and how a risk or attack scenario applies to their environment (i.e. check whether assets found in the organisation's environment are used or are affected by a specific risk scenario).
- **Identify risk scenarios related to a specific threat or group of threats.** The high-level risk scenarios related to a specific threat or group of threats that are being investigated with the use of the EU RM toolbox must be mapped to the organisation's environment to be properly assessed. Once a risk scenario has been chosen for assessment, it can utilise the threat taxonomy provided by the toolbox and the assets related to the risk scenario to map it to the corresponding internal RM method. This allows organisations to easily assess their risk levels and the security posture of their organisation for risk scenarios and proceed to the normalisation of the calculated results.
- **Map calculated risk values to a common risk scale.** Having calculated the risk values using the chosen internal RM method, the organisation has to normalise the results based on a risk level mapping process, specifically designed for each RM method, and a set of pre-defined risk levels adopted by the toolbox. The mapping process utilises the risk scale of the chosen internal method and maps them to the toolbox risk scale, thus giving stakeholders the means to use a common reference scale to evaluate their risks. The toolbox is expected, in its future updated versions, to provide an extended set of mappings for various methods.

Note that the terminology, assets classification, threats taxonomy, risk scale and, more importantly, the corresponding mappings of various RM methods to them, which will have the form of toolbox libraries, are envisioned as components that will be dynamically enriched to cover needs that stem from various applicable domains, but also from RM methods and tools as detailed in Section 4.

Moreover, subsequent versions of the toolbox can also seek the development of a common set of measures that will also be mapped to the various methods, to facilitate the proper and unified treatment of risks.

2.3. Toolbox components

The EU RM toolbox comprises several components that contribute either as functional components towards the alignment of RM activities, or as the knowledge base for risk assessment processes. The **functional components** bridge the gaps between the various risk assessment methods by aligning the respective RM functions to the EU RM toolbox. The **knowledge base** provides all the necessary information to the functional components to perform the mapping of risk scenarios to the RM methods and report risk levels.

2.3.1. Knowledge base

The EU RM toolbox **knowledge base**, also referred to as **definitions**, has all the information required to align RM efforts with the main functions that comprise such a process. The knowledge base comprises:

- terminology
- assets classification

- threats taxonomy
- impact/risk scale.

Although this initial version of the EU RM toolbox provides foundational information towards interoperable risk assessment activities, it is expected that this knowledge base will be enriched with additional information that will further facilitate interoperability. Such information includes new categories of assets that fall outside this initial categorisation, emerging threats or threats that are related to specific environments (e.g. in industrial environments), and lists of security measures, as also explained in Section 4.

Complementary to the definitions adopted by the toolbox are the **mappings** of those definitions to the respective components of the various RM methods. For a given RM methodology X, such mappings are anticipated to exist between the toolbox's terminology and X's terms, and between the toolbox's asset classification and X's assets categories. Similar mappings are expected for the threats taxonomy and the risk levels. These mappings are materialised in the form of **libraries**, and like the knowledge base will be enriched, through the functional components, and will be used by interested parties to provide interoperable RM results. More information about the toolbox's functional components is provided in Section 2.3.2.

2.3.1.1. Terminology

The main objective of the toolbox terminology component is to achieve a common understanding of the terms related to RM and to facilitate the interoperability among methodologies that use different terms for similar issues.

Annex I lists the basic set of terms commonly used by various risk analysis frameworks/methodologies. The meaning of each term is also documented in the form of a glossary. The set of terms, together with their meanings, form the toolbox terminology or, in other words, the way each term is interpreted by the toolbox.

To decide which terms will be adopted by the toolbox, the terms, and definitions of ISO/IEC 27005:2018 and ITSRM[2] were extensively studied in order to cover, consolidate and link all the terms mentioned by these standards.

2.3.1.2. Assets classification

The identification of the assets that need protection in an information system and the estimation of their value (in terms of the impact that the organisation will suffer in the event of an incident) are of crucial importance during a risk analysis. To this respect, the toolbox proposes specific asset categories (Annex II), explaining at the same time the assets included in each category, as follows.

Primary assets

- All core business processes and functions together with services provided to external parties.
- Information/data serving a specific business process or activity of the organisation.

Supporting assets

- Hardware, devices, and equipment, including computing devices, network devices, media, internet of things (IoT) devices, operational technology (OT) devices, telecommunication devices, peripherals and storage devices.
- Software and applications, such as system software and operating systems, firmware, middleware, package software and business / end user applications. Personnel, referring to roles involved in business processes and functions, user support, software development and maintenance, hardware support, delivery of services and information/data management.

- Location and utilities, including all relevant premises, such as buildings, rooms, offices, and containers, together with essential services and utilities provided by external operators/providers, power and water supply.
- Organisational infrastructure, including policies, procedures and supporting information and communications technology (ICT) services (e.g. telecommunications, network, cloud, hosting).

Achieving consensus on such an asset classification supports easier identification of threats per asset category, and thus on each member of that asset category. In addition, in terms of interoperability, it allows interested parties to easily map the assets of their organisation to the asset categories proposed by the toolbox.

Similarly to the toolbox terminology, the choice of each asset category and its members was based on the categories adopted by ISO/IEC 27005:2018 and ITSRM[2], although adapted to the needs of the toolbox. For instance, there is not a distinct category in the toolbox terminology for network components since they have been included as members of the 'Hardware' category. Also, IoT and OT devices have been classified as hardware components.

It is worth mentioning that the 'Organisational infrastructure (including ICT services)' category accommodates organisational roles, policies and procedures, along with ICT services such as telecommunications, network, cloud and hosting.

Another important differentiation of the assets is that of primary assets and supporting assets. The primary assets are the business processes, functions and services, as well as any form of data. All the rest are considered as supporting assets. As such, they are considered as the asset that can be used to process and manage the primary assets, and are therefore the means by which a primary asset can be reached.

2.3.1.3. Threats taxonomy

The toolbox also proposes a threat taxonomy (Annex III) that also draws on the directions provided in ISO/IEC 27005:2018 and ITSRM[2].

Similarly to the approach followed for building the asset classification, the main threat categories that were identified are:

- natural threats;
- industrial threats;
- errors and unintentional failures;
- wilful attacks;
- service-related threats (cloud services, services provided by third parties).

Following the identification of threat categories, each individual threat has been included in a specific category. Furthermore, each threat is associated with the asset categories that it can affect (for instance, a threat may affect a hardware device but not a software application) and with the consequences that it may cause in terms of confidentiality, integrity and availability. Finally, the origin of the threat (deliberate, accidental, environmental) is accounted for.

2.3.1.4. Impact/risk scales

The information security risk level is an indicator of the degree to which an organisation is affected by a potential cybersecurity event, and **it is determined by the likelihood of the threat occurring and its impact on the organisation's assets.** There are typically three types of information security risk assessment methodologies: **quantitative**, **qualitative**, and **semi-quantitative**. A **qualitative** risk assessment makes use of knowledge and experience to establish risk likelihood, while a **quantitative** risk assessment makes use of objective,

quantifiable facts to give insights into the RM process. A **semi-quantitative** risk assessment method typically utilises descriptive or numerical ratings.

The risk calculation method of the EU RM toolbox adopts widely accepted approaches and considers impact and probability levels to calculate the information security risk according to the following equation.

$$Risk = (probability\ of\ occurence\ of\ a\ threat) \times (impact\ of\ a\ threat)$$

The probability of occurrence of a threat represents the assessment of the likelihood that a particular threat may exploit a specific vulnerability or collection of vulnerabilities. The probability of occurrence is used as one of the main factors in risk calculation, by the majority of the existing methods. However, it is not a standard value; it depends on the utilised method. For example, ITSRM[2] adopts the following levels for the probability of occurrence for non-intentional threats: (i) every day; (ii) every month; (iii) once in a year; (iv) once in 10 years; and (v) once in a century. On the other hand, the risk management method Magerit[1] adopts a four-level scale for the estimation of the likelihood of occurrence of a threat: (i) Daily; (ii) Monthly; (iii) Annually; and (iv) Every few years.

The EU RM toolbox defines five discrete levels for the probability of occurrence of a threat. The **probability levels** are the following.

- Very high: a threat event is almost highly likely to occur.
    - A threat event is highly likely to materialise because there are associated vulnerabilities that can be exploited and no adequate security measures to defend them are in place.
- High: a threat event is likely to occur.
    - A threat event is likely to materialise because there are associated vulnerabilities that can be exploited, and ineffective or obsolete security measures to defend them are in place.
- Moderate: a threat event could potentially occur.
    - A threat event could potentially materialise since there are vulnerabilities that can be exploited, and despite having been covered with security measures, better security measures could have been implemented.
- Low: a threat event is unlikely to occur.
    - A threat event is not likely to materialise since all associated vulnerabilities have been covered with appropriate security measures.
- Very low: a threat event is highly unlikely to occur.
    - A threat event is highly unlikely to materialise since all associated vulnerabilities have been covered with effective security measures.

The impact level is the second parameter that influences the result of the information security risk. In general, impact is the level of damage that may be assessed as a result of various actions including, but not limited to, the repercussions of illegal information disclosure, unlawful information modification, unauthorised information destruction, or loss of information or information system availability. The impact is used by the majority of the existing methods that aim to calculate the information security risk. However, as with the probability of occurrence, impact is also not a standard value; it depends on the utilised method. For instance, the impact scale in ITSRM[2] has 10 distinct levels. In addition, the value depends on 10 discrete parameters, such as the financial loss due to an event. On the other hand, the risk management method Monarc[2] scores the impact from 0 to 4, and its value depends on the impact of various

[1] https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en
[2] https://www.monarc.lu/

parameters (such as confidentiality, integrity, availability, reputation, operational, legal, financial and personal) that may be affected after the event of a cybersecurity incident.

The EU RM toolbox defines the following five impact levels, which are further detailed in terms of operational, legal, financial and other implications in Annex IV.

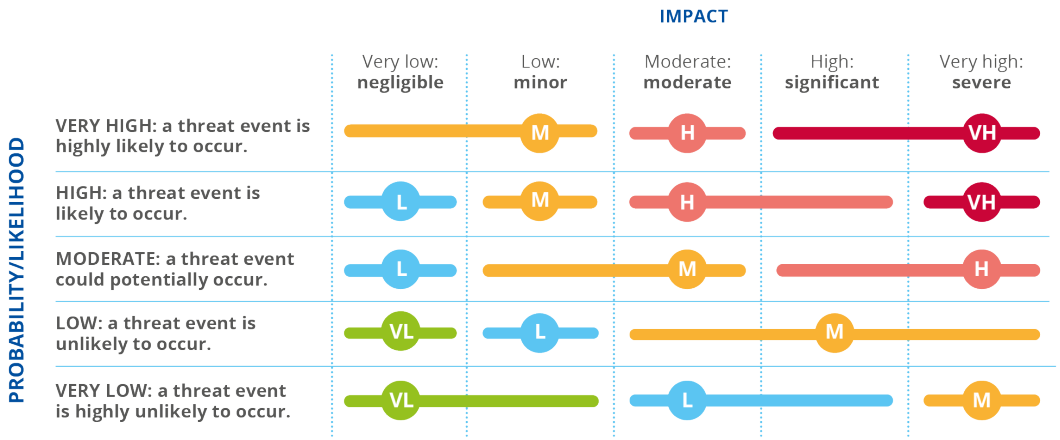
- Very high: severe – the impact for the organisation is considered severe as it is expected to have extreme consequences and implications.
- High: significant – the impact for the organisation is considered critical as it is expected to have major consequences and implications.
- Moderate: moderate – the impact for the organisation is considered moderate, as it is expected to have moderate consequences and implications.
- Low: minor – the impact for the organisation is considered minor, as it is expected to have marginal consequences and implications.
- Very low: negligible – the impact for the organisation is considered negligible, as it is expected to have insignificant consequences and implications.

Note that, depending on the RM methodology, the impact levels might be considered during the early stages of the risk assessment method, where the valuation of the assets for the organisation is being calculated.

Having considered the impact level for the organisation's assets and the probability of occurrence of a threat event, the calculation of the risk levels follows, in a non-standardised manner. The various RM methods follow different approaches. For instance, ITSRM[2] calculates the risk that fluctuates from 1 to 50 separating it in five discrete ranges. On the other hand, Monarc assesses the risk from 0 to 16 within three ranges.

Although many methods do not classify or map risk values to levels, for the common understanding of the corresponding risk values and the levels of risks the organisation experiences for specific threats, the toolbox defines a scale that comprises five such risk levels that would facilitate the interoperable evaluation of the risk values reported by the organisations. These levels are heavily affected by the various levels of impact and probability, as demonstrated by the risk matrix shown in Figure 2. The details of the risk levels – very low (VL), low (L), moderate (M), high (H) and very high (VH) – are analysed in Annex V. We can observe that the five discrete cybersecurity risk levels come from specific scenarios that combine various levels of impact and probability.

Figure 2: EU RM toolbox risk matrix



2.3.2. Functional components

The functional components of the EU RM toolbox provide the mappings between the toolbox's knowledge base (terminology, assets, threats, risk scale) and the respective components adopted by the various RM methodologies. More specifically, the anticipated contribution of the EU RM toolbox functional components is to support the comparison of the results produced by different RM methodologies and to facilitate the common understanding of the various terms adopted by them.

The functional components of the EU RM toolbox are the following:

- terminology mapping
- assets mapping
- threats mapping
- risk levels mapping.

As already presented, through the knowledge base, the toolbox proposes specific RM terms, asset categories, threat categories and risk levels. The functionality provided by the aforementioned components enables the mapping of the toolbox's terms/meanings/categories with the respective ones used by other RM methodologies. This mapping has already been performed between the toolbox's proposals and the ISO/IEC 27005:2018 and ITSRM[2]. However, it is expected that the toolbox's knowledge base will be continuously enhanced. This is anticipated to be accomplished by the community during the assessment of risk scenarios using, for instance, methodologies that have not been considered so far, and therefore not included in the toolbox's knowledge base. In this case, the involved parties have to undertake the effort to conduct this interoperability mapping between the respective components, and the result can feed the toolbox's libraries and knowledge base, to be used by subsequent activities.

3. Method of use

This section outlines the way in which the EU RM toolbox will be used by stakeholders, which include, but are not limited to, the following groups.

- Computer security incident response teams, and national or other competent authorities, such as a Member State's network and information systems (NIS) competent authority, at a Member State, EU or international level, who have a (legitimate) interest to assess organisations' risk levels or readiness against specific threats. These entities might operate in a specific domain or geographical area.
- Collaborating organisations in a specific domain or geographical area, with similar concerns and interests.
- Single organisations who might utilise different risk assessment tools over time.

The EU RM toolbox can help the above entities establish common grounds on the way they assess risks in their environment and have a common understanding on their respective risk levels and comparable results.

Once the competent authority or organisation decides upon deploying the EU RM toolbox to address RM interoperability concerns, it has to incorporate the EU RM toolbox methodology into their RM strategy. This integration is not anticipated to affect its existing risk assessment practices, as the toolbox and its respective components only encapsulate existing RM processes to provide interoperable findings.

The role of each of the toolbox components in this process is affected by the usage scenario. There are two main usage scenarios anticipated for the toolbox.

1. The evaluation of organisations' readiness against a specific threat. In this case, the EU RM toolbox will be used for a specific set of risk scenarios.
2. The evaluation of organisations', either overall or for a specific service, security posture. In this case, the organisations will run the risk assessment process, develop various risk scenarios and assess risks for each one of these, and focus only on the toolbox's risk levels component to report the outcomes.

In the following section we provide details about the first scenario, which involves the use of all the toolbox's components.

3.1. Basic concepts and terms

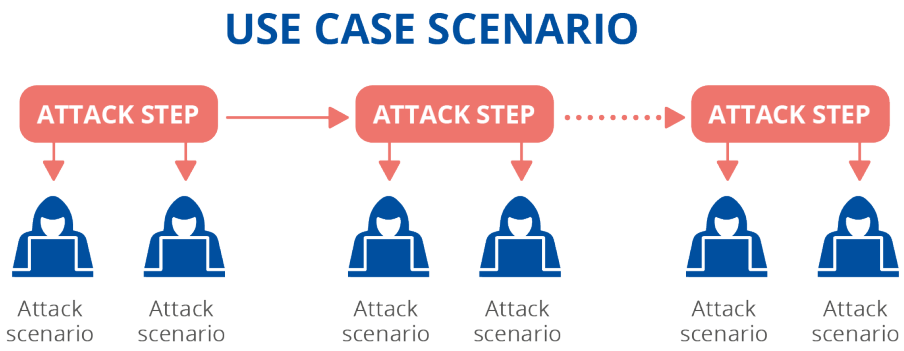
The EU RM toolbox (also referred to in this document as the 'toolbox') provides the means to assess risk levels associated with adverse events adapted to the organisations' environments and the distinctive features of the respective RM approaches adopted by organisations. Prior to providing details about the EU RM toolbox, it is useful to provide a description of the basic concepts and terms that are used throughout this document.

The terms **risk scenario** and **attack scenario** are used interchangeably to denote the description of a possible adverse event that can affect the organisation's strategy and objectives. The **attack scenario** describes the assets that are at risk or involved in the risk scenario, the actual threat, and the assets' security dimension that this threat can affect.

The EU RM toolbox has been designed to consider risk scenarios, or a set of them, that are associated with a specific **attack step** and are part of a **use case scenario**. This approach is mostly appropriate when malicious activities associated with a campaign, bound to comprise a set of attack scenarios, need to be considered by interested parties. This does not, however, preclude the use of the toolbox for the assessment of single attack scenarios that are related to granular attack techniques and specific assets.

Each attack scenario is typically part of the **attack step**, as shown in Figure 3. Likewise, the **use case scenario** might comprise several attack steps that the organisations should assess.

Figure 3: Use case scenarios, attack steps and attack scenarios



3.2. Risk evaluation against a specific threat

Let's assume that a NIS competent authority, the NIS Cooperation Group or another competent authority wants to identify risk levels across the EU against an emerged threat. The details of this threat and the types of systems that it targets form the so-called **incident scenario** that the competent authority wants to assess. The competent authority is keen to identify risk levels for a specific group of organisations that belong to the target group of the threat actors.

To be able to compare the reported results, the organisations have to provide comparable results to the competent authority using a common reference framework, as opposed to the respective results provided by their corresponding RM tools. At the same time, in order to have a common understanding of the scenarios they have to consider, the organisations have to be able to unambiguously adapt the scenario described by the competent authority to their own tools and environment, so that all the related **attack/risk scenarios** that are part of the overall incident scenario are examined.

Considering that the incident scenario entails many **attack/risk scenarios** (see Section 3.1) that map to the attack path, the competent authority wants to know risk levels associated with each step of this path. This typically implies that each **attack scenario** should be represented as a set of triplets, each comprising of **<asset(s), threat(s), impact>** that will be used as the basis to calculate the corresponding risk levels. While the impact reflects to the well-established security dimensions (confidentiality (C), integrity (I) and availability (A)), the **assets** and **threats** do not enjoy commonly accepted taxonomies and lists. The toolbox corresponding components will be used to define the risk scenarios, which then need to be adapted to each RM method with the help of the toolbox mappings. Having said that, the use of the EU RM toolbox requires the following steps.

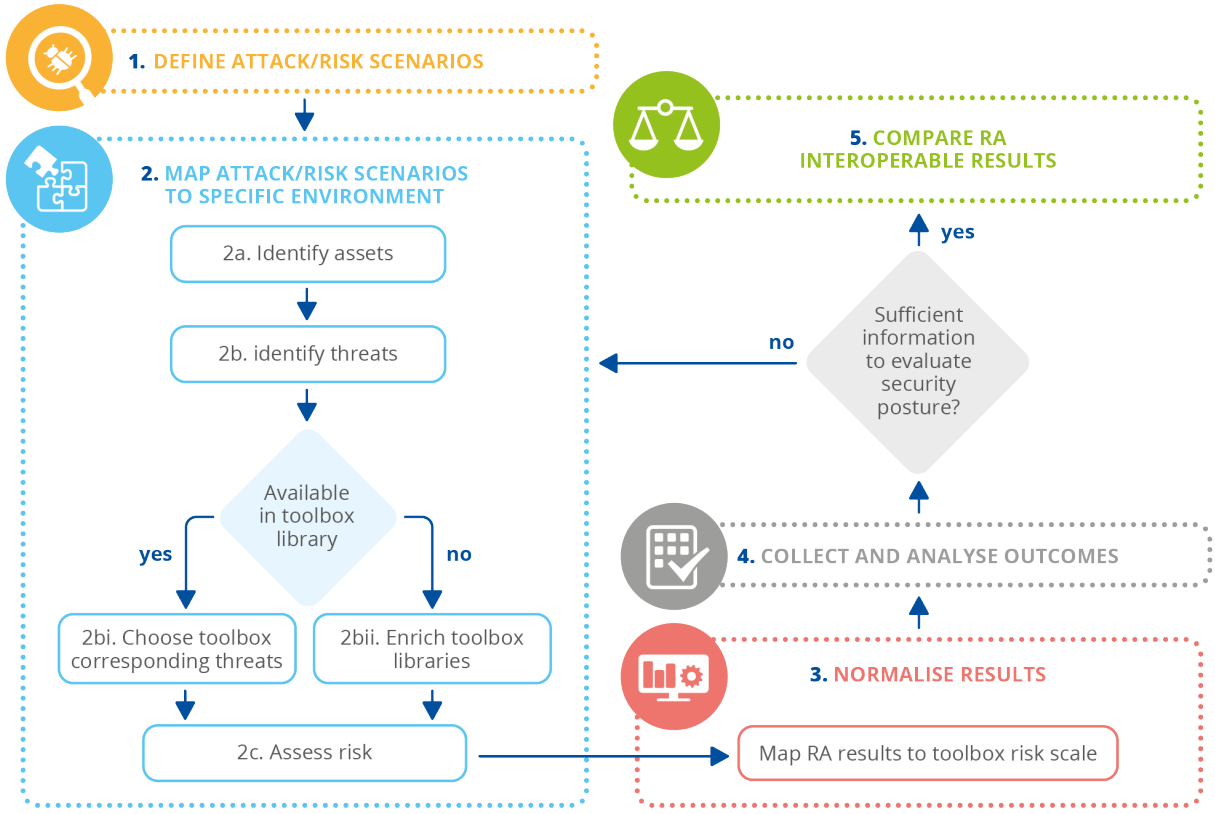
1. The competent authority establishes a set of **attack/risk scenarios** that either map to the attack path of the emerged threat, or the competent authority considers essential to evaluate. The **attack scenarios** should use the toolbox terms, list of assets and list of threats.

2. The participating organisations have to map the defined **attack/risk scenarios** to their environment to allow them to assess the corresponding risks using their own respective methodology. This process requires the use of the toolbox libraries, which might already have mappings about the organisation's chosen RM methodology. If such mappings are not available, they have to be enriched accordingly. In each of these steps the organisation has to consult the toolbox terms to unambiguously interpret each of the attack/risk scenarios.
    a. More specifically, the organisation establishes the context for the examined incident scenario. That is, it has to identify the assets that are involved in the attack/risk scenarios and map them to their environment and the types of assets that their methodology defines. As noted above, the toolbox libraries might already provide the mapping of the toolbox assets to the organisation's methodology types of assets. If not, the participating experts have to propose their mapping and enrich the toolbox libraries.
    b. Following the context establishment and the identified assets, the organisation has to unambiguously identify the threats addressed by the attack/risk scenarios of the incident scenario. The list of threats that the incident scenario addresses are from the toolbox's threats taxonomy, which do not necessarily directly map to the organisation's methodology threats taxonomy. To bridge this gap, a threats mapping library for the corresponding risk methodology must be developed, if none already exist. This threats mapping library will be gradually enriched. Note that during this process, new threats or threat categories can also be introduced to the toolbox threat taxonomy. So, as with the list of assets, there are two cases.
        i. A mapping between the toolbox-adopted list of threats and the organisation's chosen methodology list of threats is already available in the toolbox's library. In this case, the organisation has to choose the corresponding threats for the attack/risk scenarios.
        ii. There is no available mapping, and therefore the organisation has to run this task internally and, as a result, enrich the toolbox libraries.
    c. Having identified and mapped the list of assets and threats, the organisation has to assess risks for each of the requested attack/risk scenarios. If the method considers vulnerabilities in the risk assessment process, these have to be properly identified for the involved assets and used in the risk calculation process.

3. The calculated risk values for the corresponding risk scenarios provide valuable information to the organisation that has been using the specific methodologies. This information, however, is not meaningful to the competent authority that does not want or have to know the peculiarities of each RM method. The last step in the toolbox usage process is to normalise risk assessment results to the toolbox risk scales. This can be done using the toolbox libraries if such a mapping between the toolbox risk scales and the organisation's RM methodology's scales exist. If not, the organisation has to undertake the mapping process and enrich the toolbox libraries.
4. The competent authority collects the outcomes of the above process conducted in the organisation's environment and based on the reported results, it either has the information it needs to evaluate the organisations' security posture or has to conduct the last step itself.

Note that in this process, not all of the initially defined **attack/risk scenarios** are necessarily applicable to all environments. Depending on the system modelling of the organisation and the dependencies between a threat and primary assets and how a threat can affect a primary asset through other additional supporting assets, the organisation will decide the applicability of each of the **attack/risk scenarios**.

Figure 1: EU RM toolbox processes diagram



3.3. Use case development process

The toolbox can be used by a competent authority to assess organisations' risk levels against an incident scenario. An **incident scenario**, as previously defined, is used by a competent authority to describe a set of threats against which the participating organisations will assess their posture. It aims to guide the organisations in considering specific threats and narrow down the scope of the attack path and the number of attack/risk scenarios that the participating organisations have to consider. Therefore, an incident scenario is anticipated to include the following information.

1. **Description of the scenario.** This outlines the incident scenario that the competent authority addresses in the scenario.
2. **Indicative assets in scope.** The scenario has to provide a list of assets, primary or supporting, that are affected or used by the threat actors during their campaign.
3. **Attack path.** This outlines the steps that are typically followed by the threat actors to give the participating entities a better understanding about the incident scenario and the set of threats that are being examined.
4. **Attack scenarios.** They form a list of triplets about the involved or affected assets, the considered threat and the corresponding impact (i.e. the security dimension that is affected by this threat) for the corresponding steps outlined in the attack path.

A use case example can be found in Annex VIII.

4. Toolbox evolvement

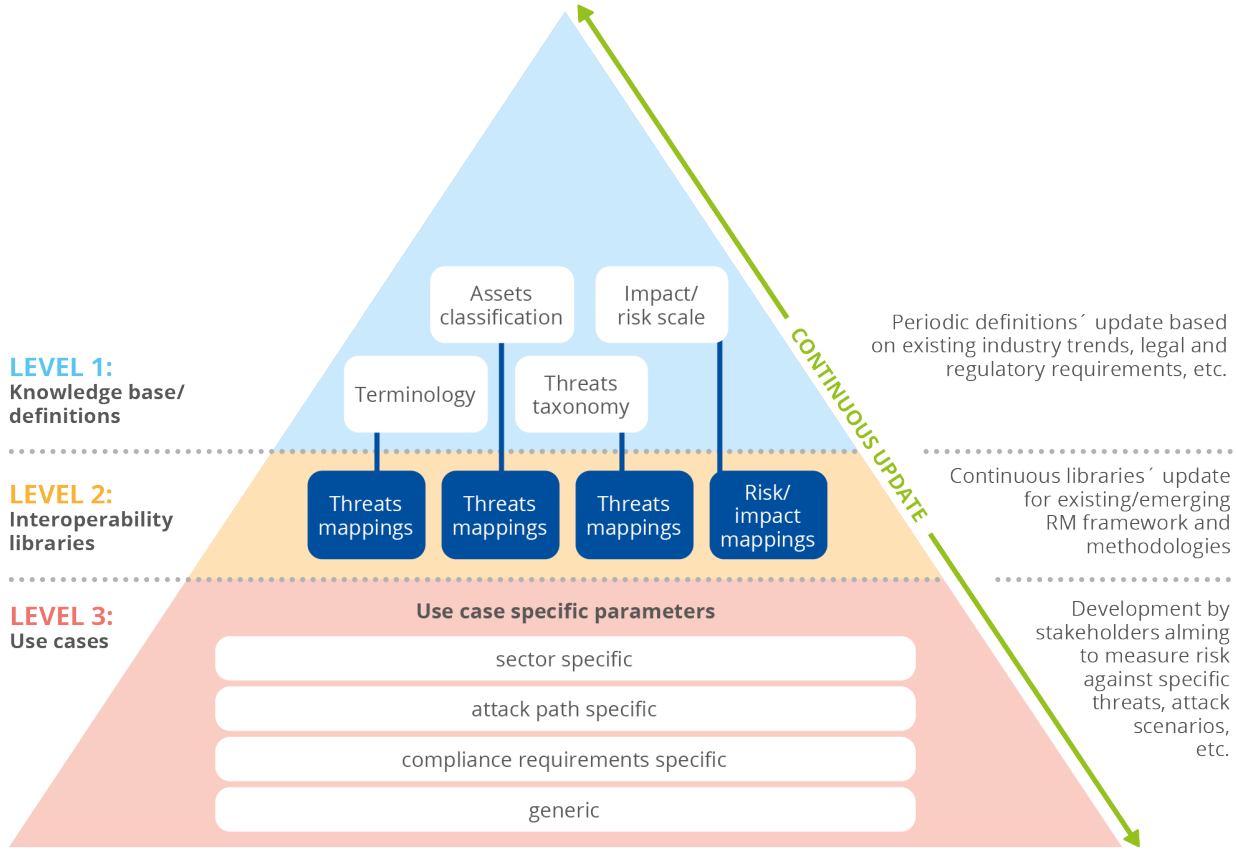
The EU RM toolbox is envisioned as a reference tool that will be enriched with additional information to achieve its objectives. This is anticipated to occur at various levels that correspond to the toolbox's knowledge base, which comprises the set of toolbox definitions (i.e. terminology, assets classification, threats taxonomy and impact/risk scale), but also the mappings to other methodologies' components, as shown in Figure 5.

The toolbox's definitions are expected to be reviewed and enriched by the community so that the needs of all the domains that will adopt the EU RM toolbox will be addressed. Examples of these enhancements include impact justifications for the various levels that are adapted to specific domains, such as the energy domain, or set of threats that are more meaningful to the specific domain.

Another important component of the EU RM toolbox is the set of interoperability libraries, which will provide the mappings of the toolbox definitions to other RM methodologies. These libraries can be the result of the use of the toolbox by the community, where the involved parties will undergo the process of conducting this mapping between the toolbox and their own RM methodology components, if these are not already available, and provide their feedback to enrich the toolbox libraries. This will help subsequent efforts or users and will result in an integrated tool that will help organisations compare their risk levels.

Similarly to the definitions and the interoperability libraries, a third set of valuable information that will complement the toolbox is the use cases descriptions, which can act either as templates for subsequent risk assessment processes, or as specific scenarios that can be applied on domains or organisations.

Figure 2: EU RM toolbox evolvement



5. Conclusions

This deliverable has presented the main components of the EU RM toolbox, which serves as a reference framework for aligning different RM efforts and thus achieving a common understanding about risks and associated risk levels, regardless of the RM approach adopted and the tool(s) used by organisations.

Through the proposed EU RM toolbox, different stakeholders will be able to compare their RM results, for specific risk scenarios, with other organisations that may use different RM methods/tools. Furthermore, regulatory and supervisory bodies will be supported with regard to the overall view of the risk levels and the security posture of organisations in a specific sector or across various sectors.

The main RM functions supported by the EU RM toolbox are:

- the establishment of a common understanding on the activities undertaken during the RM process;
- a definition of the scope of the environment in which the risk assessment process will be applied;
- the identification of risk scenarios related to a specific threat or threats that are being investigated;
- mapping of the calculated risk levels to those defined by a common risk scale.

It is vital to stress that the knowledge base provided by the toolbox (sets of terms, classification of assets and threats) will be dynamically enriched to cover additional methods and tools, along with other domains.

Moreover, subsequent versions of the toolbox can seek the development of a common set of measures that will also be mapped to the various methods, to facilitate the proper and unified risk treatment.

A Annex I – Toolbox terminology

This annex contains a list of terms that form the **toolbox terminology**.

Table 1: Interoperable EU RM toolbox terminology

Frameworks and methodologies / terminology	Toolbox glossary	Related terms
Access control	Means to ensure that access to assets is authorised and restricted based on business and security requirements.	-
Asset	An asset is anything that has value to the organisation and therefore requires protection. For the identification of assets, it should be borne in mind that an information system consists of more than hardware and software.	-
Asset owner	An asset owner should be identified for each asset to provide responsibility and accountability for the asset. The asset owner perhaps does not have property rights to the asset, but has responsibility for its production, development, maintenance, use and security as appropriate. The asset owner is often the most suitable person to determine the asset's value to the organisation.	System owner
Asset value	Value of the asset assessed in terms of the maximum impact (business or data protection) in the event of loss of security dimensions (confidentiality, integrity, availability); this is also known as the security need.	Information technology (IT) security need
Attack path	Set of deliberate actions to realise a threat scenario.	-
Attack scenario	See 'Risk scenario'.	Risk scenario
Attack step	A set of attack scenarios related to a malicious activity.	-
Attack	Attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an asset.	-
Audit	Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.	-
Audit events	Ensure that activity on the system leaves a record that provides reliable after-the-fact investigations of security incidents.	-
Audit scope	Extent and boundaries of an audit.	-
Authentication	Provision of assurance that a claimed characteristic of an entity is correct.	-
Authenticity	Property that an entity is what it claims to be.	-

Frameworks and methodologies / terminology	Toolbox glossary	Related terms
Availability	Property of being accessible and usable upon request by an authorised entity.	-
Base measure	Measure defined in terms of an attribute and the method for quantifying it.	-
Business manager	Role responsible for ensuring that an organisation's function fulfils the business and user needs.	-
Competence	Ability to apply knowledge and skills to achieve intended results.	-
Communication and information system (CIS)	Any system enabling the handling of information in electronic form, including all assets required for its operation, along with infrastructure, organisation, personnel and information resources. This definition includes business applications, shared IT services, outsourced systems and end user devices.	Information system
Confidentiality	Property that information is not made available or disclosed to unauthorised individuals, entities or processes.	-
Conformity	Fulfilment of a requirement.	-
Consequence	Outcome of an event affecting objectives.	-
Continual improvement	Recurring activity to enhance performance.	Information security continuity
Control	Measure that modifies risk – control is also used as a synonym to safeguard or countermeasure.	Measure-security measure
Control objective	Statement describing what is to be achieved as a result of implementing controls.	-
Correction	Action to eliminate a detected nonconformity.	-
Corrective action	Action to eliminate the cause of a nonconformity and to prevent recurrence.	-
Data controller	The natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data.	-
Data owner	The individual responsible for ensuring the protection and use of a specific dataset handled by a CIS.	-
Dataset	A set of information that serves a specific business process or activity.	-
Data subject	Any person whose personal data is being collected, held or processed.	-
Derived measure	Measure that is defined as a function of two or more values of base measures.	-

Frameworks and methodologies / terminology	Toolbox glossary	Related terms
Documented information	Information required to be controlled and maintained by an organisation and the medium on which it is contained.	-
Easiness	Valuation of the effort required to materialise a given intentional threat.	-
Effectiveness	Extent to which planned activities are realised and planned results achieved.	-
Event	Occurrence or change of a particular set of circumstances. An event can sometimes be referred to as an incident or accident.	Incident
External context	External environment in which the organisation seeks to achieve its objectives.	-
Frequency	Description of the quantitative or qualitative values used to express the periodicity of accidental threats from materialising.	-
Function	The processing of information comprises all functions of a CIS with regard to datasets, including creation, modification, display, storage, transmission, deletion and archiving of information. Processing of information can be provided by a CIS as a set of functionalities to users and as IT services to other CIS.	-
Governance of information security	System by which an organisation's information security activities are directed and controlled.	-
Governing body	Person or group of people who are accountable for the performance and conformity of the organisation.	-
Impact	Adverse change to the level of business objectives achieved.	-
Impact scenario	Combination of primary asset, security dimension (confidentiality, integrity or availability), impact type, effects and level related to the worst-case scenarios described by the organisation to determine the primary asset values.	-
Incident	An event that has been assessed as having an actual or potentially adverse effect on the security or performance of a system. An event can sometimes be referred to as an incident or accident.	Event
Incident scenario	An incident scenario is the description of a threat exploiting a certain vulnerability or set of vulnerabilities in an information security incident. The impact of the incident scenarios is to be determined considering impact criteria defined during the context establishment activity. It can affect one or more assets or part of an asset. Thus, assets can have assigned values both for their financial cost and because of the business consequences if they are damaged or compromised. Consequences can be of a temporary nature or permanent as in the case of the destruction of an asset.	-

Frameworks and methodologies / terminology	Toolbox glossary	Related terms
Indicator	Measure that provides an estimate or evaluation.	-
Inherent risk	The risk without taking any security measure into account. Inherent risk represents the amount of risk that exists in the absence of controls (FAIR Institute). Inherent risk is the current risk level given the existing set of controls rather than the hypothetical notion of an absence of any controls (FAIR Institute). ISO does not define the notion of inherent risk, but it could be defined by opposition to the notion of residual risk as: risk existing before risk treatment.	-
Information need	Insight necessary to manage objectives, goals, risks and problems.	-
Information processing facilities	Any information processing system, service or infrastructure, or the physical location housing it.	-
Information security	Preservation of confidentiality, integrity and availability of information.	-
Information security continuity	Processes and procedures for ensuring continued information security operations.	Continual improvement
Information security event	Identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that can be security relevant.	-
Information security incident	Event that could adversely affect the confidentiality, integrity or availability of a CIS.	-
Information security incident management	Set of processes for detecting, reporting, assessing, responding to, dealing with and learning from information security incidents.	-
Information security management system professional	Person who establishes, implements, maintains and continuously improves one or more information security management system processes.	Security risk manager
Information sharing community	Group of organisations that agree to share information.	-
Information system	Set of applications, services, IT assets or other information-handling components.	CIS
Integrity	Property of accuracy and completeness.	-
Interest	The level of interest of an adversary to commit a threat on a given primary asset.	-
Interested party (preferred term) –	Person or organisation that can affect, be affected by or perceive itself to be affected by a decision or activity.	Stakeholders organisation

Frameworks and methodologies / terminology	Toolbox glossary	Related terms
stakeholder (admitted term)		
Internal context	Internal environment in which the organisation seeks to achieve its objectives.	-
IT security need	See 'Asset value'.	Asset value
IT security risk	See 'Risk'.	Risk
Level of risk	Magnitude of a risk expressed in terms of the combination of consequences and their likelihood.	-
Likelihood	Chance of something happening.	-
Local informatics security officer	Officer who is responsible for IT security liaison for a commission department.	-
Management system	Set of interrelated or interacting elements of an organisation to establish policies and objectives and processes to achieve those objectives.	-
Measure	See 'Security measure'.	Security measure – control
Measurement	Process to determine a value.	-
Measurement function	Algorithm or calculation performed to combine two or more base measures.	-
Measurement method	Logical sequence of operations, described generically, used in quantifying an attribute with respect to a specified scale.	-
Mitigation factor	Percentage of the risk (likelihood and/or consequence) that is reduced by a security measure.	-
Monitoring	Determining the status of a system, a process or an activity.	-
Nonconformity	Non-fulfilment of a requirement.	-
Non-repudiation	Ensure that actors who have carried out specific types of actions cannot falsely deny later that they have carried them out.	-
Objective	Result to be achieved.	-
Organisation	See 'Interested party' and 'Stakeholder'.	Interested party – stakeholder
Outsource	Make an arrangement where an external organisation performs part of an organisation's function or process.	-
Performance	Measurable result.	-
Personal data	Any information relating to an identified or identifiable natural person (data subject).	-

Frameworks and methodologies / terminology	Toolbox glossary	Related terms
Policy	Intentions and direction of an organisation, as formally expressed by its top management.	-
Potential adversary	Individual or group interested in provoking loss of confidentiality, integrity and/or availability of an organisation's assets.	-
Power	The combination of a potential adversary knowledge, its capabilities and the resources to perform an attack successfully.	-
Primary asset	Data and business processes/functions.	-
Process	Set of interrelated or interacting activities that transforms inputs into outputs.	-
Reliability	Property of consistent intended behaviour and results.	-
Requirement	Need or expectation that is stated, generally implied or obligatory.	-
Residual risk	Risk remaining after risk treatment.	-
Review	Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives.	-
Review object	Specific item being reviewed.	-
Review objective	Statement describing what is to be achieved as a result of a review.	-
Risk	Effect of uncertainty on objectives.	IT security risk
Risk acceptance	Terms of reference against which a risk is accepted.	-
Risk acceptance criteria	Criteria used for accepting a risk.	-
Risk analysis	Process to comprehend the nature of risk and to determine the level of risk.	-
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation.	-
Risk avoidance	The activity or condition that gives rise to the particular risk that should be avoided.	-
Risk communication and consultation	Set of continual and iterative processes that an organisation conducts to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management of risk.	-
Risk criteria	Terms of reference against which the significance of risk is evaluated.	-

Frameworks and methodologies / terminology	Toolbox glossary	Related terms
Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.	-
Risk identification	Process of finding, recognising and describing risks.	-
Risk management	Coordinated activities to direct and control an organisation with regard to risk.	-
Risk management process	Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk.	-
Risk mitigation	Risk treatments that deal with negative consequences.	-
Risk modification	A process where the level of risk is managed by introducing, removing or altering controls so that the residual risk can be reassessed as being acceptable.	-
Risk owner	Person or entity with the accountability and authority to manage a risk.	-
Risk reduction	Actions taken to lessen the probability, negative consequences, or both, associated with a risk.	-
Risk retention	A risk treatment option where the risk is retained without further action.	-
Risk scenario	A combination of involved assets, threat and affected security dimension.	Attack scenario
Risk sharing	Sharing the risk with another party that can most effectively manage the particular risk depending on risk evaluation.	-
Risk study	Set of information gathered and results obtained when performing RM activities. It mainly consists of: — a description of the CIS and its environment; — the risks with inherent and residual levels; — the security measures.	-
Risk transfer	Sharing with another party the burden of loss or benefit of gain, for a risk. Replaced by 'Risk sharing'.	-
Risk treatment	Process to modify risk. It can involve: — avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; — taking or increasing risk in order to pursue an opportunity; — removing the risk source; — changing the likelihood;	-

Frameworks and methodologies / terminology	Toolbox glossary	Related terms
	— changing the consequences; — sharing the risk with another party or parties (including contracts and risk financing); — retaining the risk by informed choice.	
Security measure	Actionable control that can be implemented according to a priority level to mitigate a risk.	Measure – control
Security risk manager	The person responsible for the RM activities.	Information security management system professional
Scale	Ordered set of values, continuous or discrete, or a set of categories to which the attribute is mapped.	-
Service	A service is a means of delivering data processing (datasets and functions) to customers, internally or externally. An IT service is made up of a combination of IT products (hardware and software), people and locations.	-
Shared service	A service is shared when its risk study is published, entirely or partially, by its service provider to be reused in risk studies of CIS that are using the service.	-
Stakeholders	Internal and external organisations or people with an interest in the target system data and functions.	Interested party – organisation
Sophistication level	Scale used to measure the technical level of implementation (effectiveness) of security measures.	-
Supporting asset	Assets used or involved in the processing of the data and functions/services provided by the target system.	-
System model	Representation of the architecture of the system in relation to the supporting assets used to manage the data and functions (primary assets) managed by the target system.	-
System owner	Individual responsible for the overall procurement, development, integration, modification, operation, maintenance and retirement of a CIS.	Asset owner
System security officer	Advises the system owner, system manager and project manager on the IT security approach, and takes an active role as IT security expert to define IT security requirements and assists in the architecture, design, implementation and verification activities of IT security.	-
Security implementation standard	Document specifying authorised ways for realising security.	-
Target of a security measure	The place where the measure can be actually implemented. Such target can be the organisation (e.g. a general security policy), the system (e.g. RM, code review, vulnerability scan) or a particular supporting asset (e.g. encryption on a data link or a hard disk, access control to an operating system).	-

Frameworks and methodologies / terminology	Toolbox glossary	Related terms
Target system	The specific CIS subject to the execution of an RM process.	-
Threat	Potential cause of an unwanted incident, which can result in harm to a system or organisation.	-
Threat scenario	A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time.	-
Top management	Person or group of people who direct and control an organisation at the highest level.	-
Trusted information communication entity	Autonomous organisation supporting information exchange within an information sharing community.	-
User	Any individual who uses a functionality provided by a CIS, whether inside or outside the organisation.	-
Use case scenario	Use case description of the sequence of events from the user's perspective to perform a task in a specified context.	-
Vulnerability	Weakness of an asset or control that can be exploited by one or more threats.	-

B Annex II – Toolbox asset classification

This annex provides the classification of assets adopted by the EU RM toolbox.

Table 2: Interoperable EU RM toolbox assets

Assets Primary assets: generic description	RM toolbox Definition	RM toolbox Subcategories/examples
Business processes, functions, services	Business processes, functions and services.	Include all core business processes and functions, and services provided to external parties.
Information/data	Information and data in all forms (storage, transmission, etc.) that are of value.	A set of information/data that serves a specific business process or activity of the organisation.
Supporting assets: generic description		
Hardware, devices and equipment	All physical elements/devices and equipment supporting business processes, functions and services.	Computing devices (e.g. endpoint devices, servers), network devices and media, **IoT devices**, **OT devices**, telecommunication devices, peripherals and storage devices.
Software and applications	Software and applications.	System software (e.g. operating systems), firmware, middleware, package software, business / end user applications.
Personnel	Personnel with roles involved in business processes and functions, user support, software development and maintenance, hardware support, delivery of services and information / data management.	Decision-makers, users, developers, administrators, operators, maintenance personnel, contractors.
Location and utilities	Premises containing / related to primary and supporting assets.	Locations and premises, such as buildings, rooms, offices and containers. Mobile platforms such as trucks, cars, ships. Essential services and utilities provided by external operators/providers, power and water supply, etc.
Organisational infrastructure (including ICT services)	Roles, management and supporting activities and ICT services.	Organisational infrastructure including roles, policies, procedures and ICT services (telecommunications, network, cloud, hosting, etc.).

C Annex III – Toolbox threat taxonomy

This annex provides the threat taxonomy adopted by EU RM toolbox.
NB: A short description of each threat can be found in Table 4 of this annex.

Table 3: Interoperable EU RM toolbox threat catalogue

Threat category	Threat	Security dimensions (confidentiality, integrity and availability)			Origin (deliberate, accidental, environmental)			Supporting asset categories				
		C	I	A	D	A	E	Hardware, devices, equipment	Software/applications	Personnel	Locations and utilities	Organisational infrastructure (including ICT services)
Natural	Fire			X			X	X			X	
Natural	Flood			X			X	X			X	
Natural	Major accident			X			X	X			X	
Natural	Other natural disasters			X			X	X			X	
Industrial	Fire			X	X	X		X			X	
Industrial	Water damage			X	X	X		X			X	
Industrial	Other industrial disasters			X	X	X		X			X	
Industrial	Environmental pollution			X	X	X	X	X			X	
Industrial	Electromagnetic / thermal radiation			X	X	X	X	X			X	
Industrial	Hardware or software failure			X	X	X		X	X			
Industrial	Power interruption			X	X	X	X	X				
Industrial	Unsuitable temperature or humidity conditions			X	X	X	X	X				
Industrial	Communications services failure			X	X	X						X
Industrial	Interruption of other services or essential supplies			X	X	X					X	X
Industrial	Media/equipment degradation			X	X	X		X				
Industrial	Electromagnetic emanations	X			X			X			X	

Threat category	Threat	Security dimensions (confidentiality, integrity and availability)			Origin (deliberate, accidental, environmental)			Supporting asset categories				
		C	I	A	D	A	E	Hardware, devices, equipment	Software/applications	Personnel	Locations and utilities	Organisational infrastructure (including ICT services)
Errors and unintentional failures	User errors	X	X	X		X		X	X			X
Errors and unintentional failures	System/security administrator errors	X	X	X		X		X	X			X
Errors and unintentional failures	Monitoring errors (logs)		X			X		X	X			X
Errors and unintentional failures	Configuration errors	X	X	X		X		X	X			X
Errors and unintentional failures	Organisational deficiencies			X		X				X		
Errors and unintentional failures	Malware diffusion	X	X	X		X			X			
Errors and unintentional failures	(Re)routing errors	X				X			X			X
Errors and unintentional failures	Sequence errors		X			X			X			X
Errors and unintentional failures	Accidental alteration of the information		X			X		X	X	X	X	X
Errors and unintentional failures	Destruction of information			X		X		X	X	X	X	X
Errors and unintentional failures	Information leaks	X				X		X	X	X	X	X
Errors and unintentional failures	Software vulnerabilities	X	X	X		X			X			
Errors and unintentional failures	Defects in software maintenance / updating		X	X		X			X			
Errors and unintentional failures	Defects in hardware maintenance / updating			X		X		X				
Errors and unintentional failures	System failure due to exhaustion of resources			X		X		X				X
Errors and unintentional failures	Retrieval of recycled or discarded media	X		X		X		X				
Errors and unintentional failures	Breach of personnel availability			X		X				X		
Wilful attacks	Manipulation of activity records (log)		X		X			X	X			X
Wilful attacks	Manipulation of the configuration files	X	X	X	X			X	X			X
Wilful attacks	Masquerading of identity	X	X		X				X			X
Wilful attacks	Abuse of access privileges	X	X	X	X				X		X	X
Wilful attacks	Misuse	X	X	X	X				X		X	X

Threat category	Threat	Security dimensions (confidentiality, integrity and availability)			Origin (deliberate, accidental, environmental)			Supporting asset categories				
		C	I	A	D	A	E	Hardware, devices, equipment	Software/applications	Personnel	Locations and utilities	Organisational infrastructure (including ICT services)
Wilful attacks	Malware diffusion	X	X	X	X				X			
Wilful attacks	(Re)routing of messages	X			X				X			X
Wilful attacks	Sequence alteration		X		X				X			X
Wilful attacks	Unauthorised access	X	X		X			X	X		X	X
Wilful attacks	Traffic analysis	X			X							X
Wilful attacks	Repudiation (denial of actions)		X		X							X
Wilful attacks	Eavesdropping	X			X							X
Wilful attacks	Deliberate alteration of information		X		X			X	X	X	X	X
Wilful attacks	Destruction of information			X	X			X	X	X	X	X
Wilful attacks	Disclosure of information	X			X				X	X	X	X
Wilful attacks	Tampering with software	X	X	X	X	X			X			
Wilful attacks	Tampering with hardware	X			X			X				
Wilful attacks	Denial of services			X	X			X				X
Wilful attacks	Theft of media or documents	X		X	X			X				
Wilful attacks	Theft of equipment	X		X	X			X				
Wilful attacks	Destructive attack			X	X			X			X	
Wilful attacks	Enemy overrun	X		X	X						X	
Wilful attacks	Staff shortage			X	X					X		
Wilful attacks	Extortion	X	X	X	X					X		
Wilful attacks	Social engineering	X	X	X	X					X		
Service-related threats (cloud services, services provided by third parties)	Loss of governance			X	X	X						X
Service-related threats (cloud services, services provided by third parties)	Lock-in			X		X						X
Service-related threats (cloud services, services provided by third parties)	Isolation failure	X	X	X	X	X						X

Threat category	Threat	Security dimensions (confidentiality, integrity and availability)			Origin (deliberate, accidental, environmental)			Supporting asset categories				
		C	I	A	D	A	E	Hardware, devices, equipment	Software/applications	Personnel	Locations and utilities	Organisational infrastructure (including ICT services)
Service-related threats (cloud services, services provided by third parties)	Management interface compromise			X	X	X						X
Service-related threats (cloud services, services provided by third parties)	Insecure or ineffective deletion of data	X			X	X						X
Service-related threats (cloud services, services provided by third parties)	Compromise of service engine	X	X	X	X	X						X
Service-related threats (cloud services, services provided by third parties)	Subpoena and e-discovery	X		X	X	X						X
Service-related threats (cloud services, services provided by third parties)	Risk from changes of jurisdiction	X		X	X	X						X
Service-related threats (cloud services, services provided by third parties)	Data protection risks	X				X						X
Service-related threats (cloud services, services provided by third parties)	User privacy and secondary usage of data	X										X
Service-related threats (cloud services, services provided by third parties)	Incidence analysis and forensic support	X	X	X								X
Service-related threats (cloud services, services provided by third parties)	Insecure interfaces and application programming interfaces (APIs)	X	X	X		X						X

Table 4: Interoperable EU RM toolbox threat description

Threat category	Threat	Threat description
Natural	**Fire**	Possibility that the fire destroys system resources.
Natural	**Flood**	Possibility that the water destroys system resources.
Natural	**Major accident**	Incidents that occur without human involvement (lightning, electric storm, earthquake, cyclone, etc.).
Natural	**Other natural disasters**	External event or damage linked to the natural environment close to the assets and capable of causing them very serious physical damage.
Industrial	**Fire**	Possibility that the fire destroys system resources (terrorism, vandalism, etc.).
Industrial	**Water damage**	Possibility that the water destroys the system's resources (leaks, floods, terrorism, vandalism, etc.).
Industrial	**Other industrial disasters**	Accidental disasters due to human activity (explosions, collapses, chemical pollution, electrical overloads, electrical fluctuations, etc.).
Industrial	**Environmental pollution**	Presence of dust, vapours, corrosive or toxic gases in the ambient air.
Industrial	**Electromagnetic/thermal radiation**	Radio interference, magnetic fields, ultraviolet light, etc. Thermal effect caused by damage or exceptional weather conditions. Damage causing an exceptional electromagnetic effect.
Industrial	**Hardware or software failure**	Failures in the equipment and/or programmes.
Industrial	**Power interruption**	Failure, shutdown or incorrect sizing of the power supply to the assets arising either from the supplier's service or from the internal distribution system. Sabotage or disturbance of the electrical installation.
Industrial	**Unsuitable temperature or humidity conditions**	Deficiencies in the air conditioning of the premises that exceed the working limits for the equipment (excess heat, excess cold, excess humidity, etc.).
Industrial	**Communications services failure**	A cut in the capability to transmit data from one place to another.
Industrial	**Interruption of other services or essential supplies**	Interruption of services or resources on which the operation of the equipment depends.
Industrial	**Media/equipment degradation**	A logical or physical event causing an equipment item to malfunction or as the result of the passing of time.
Industrial	**Electromagnetic emanations**	Almost all electrical devices emit radiation to the exterior that can be intercepted by other equipment (radio receivers), causing a leak of information.
Errors and unintentional failures	**User errors**	Mistakes made by people when using the services, data, etc. A person commits an operating error, input error or utilisation error on hardware or software.
Errors and unintentional failures	**System/security administrator errors**	Mistakes made by people with installation and operation responsibilities of the system / system's security. A system/security administrator commits an operating error, input error or utilisation error on hardware or software.
Errors and unintentional failures	**Monitoring errors (logs)**	Lack of records, incomplete records, incorrectly dated records, incorrectly attributed records, etc.
Errors and unintentional failures	**Configuration errors**	Entry of erroneous configuration data. Almost all assets depend on their configuration, and this depends on the diligence of the administrator (access privileges, activity flows, activity records, routing, etc.).

Threat category	Threat	Threat description
Errors and unintentional failures	**Organisational deficiencies**	When it is not clear who must do exactly what and when, including taking measures on the assets or reporting to the management hierarchy.
Errors and unintentional failures	**Malware diffusion**	Unintentional propagation of viruses, spyware, worms, Trojans, logic bombs, etc.
Errors and unintentional failures	**(Re)routing errors**	The sending of information via a system or network using, accidentally, an incorrect route that sends the information to the wrong destination. These could be messages sent to/by people, processes or both.
Errors and unintentional failures	**Sequence errors**	The accidental alteration of the order of the messages sent.
Errors and unintentional failures	**Accidental alteration of the information**	The accidental alteration of the information.
Errors and unintentional failures	**Destruction of information**	The accidental loss of the information.
Errors and unintentional failures	**Information leaks**	Disclosure due to indiscretion (verbal indiscretion, electronic media, hard copies, etc.).
Errors and unintentional failures	**Software vulnerabilities**	Defects in the code that cause a defective operation without intention on the part of the user but with consequences to the data confidentiality, integrity, availability or to its capacity to operate.
Errors and unintentional failures	**Defects in software maintenance / updating**	Defects in the procedures or controls for updating the code that allow programmes with known defects that have been repaired by the manufacturer to continue to be used.
Errors and unintentional failures	**Defects in hardware maintenance / updating**	Defects in the procedures or controls for updating equipment that allow it to operate under normal circumstances. Lack of expertise in the system making retrofitting and upgrading impossible.
Errors and unintentional failures	**System failure due to exhaustion of resources**	The lack of sufficient resources causes the system failure when the workload is excessive. Overload of storage space (e.g. backup space, mailbox storage, work area, etc.).
Errors and unintentional failures	**Retrieval of recycled or discarded media**	The loss of equipment directly causes the lack of means to provide services, that is, their service's unavailability.
Errors and unintentional failures	**Breach of personnel availability**	Accidental absence from the work post (illness, disturbances in public order, bacteriological warfare, etc.). Absence of qualified or authorised personnel held up for reasons beyond their control.
Wilful attacks	**Manipulation of activity records (log)**	Manipulation of activity records to remove any evidence or traces.
Wilful attacks	**Manipulation of the configuration files**	The entry of erroneous configuration data.
Wilful attacks	**Masquerading of identity**	When attackers manage to appear as authorised users, they enjoy the users' privileges for their own purposes.
Wilful attacks	**Abuse of access privileges**	When users abuse their privilege level to carry out tasks that are not their responsibility, there are problems.
Wilful attacks	**Misuse**	The use of system resources for unplanned purposes, typically of personal interest (games, personal searches on the internet, personal databases, personal programmes, storage of personal data, etc.).
Wilful attacks	**Malware diffusion**	Intentional propagation of viruses, spyware, worms, Trojans, logic bombs, etc.
Wilful attacks	**(Re)routing of messages**	The sending of information via a system or network using, deliberately, an incorrect route that sent the information to the wrong destination.
Wilful attacks	**Sequence alteration**	The alteration of the order of the messages sent. The idea is that the new order changes the meaning of the group of messages, prejudicing the integrity of the affected data.
Wilful attacks	**Unauthorised access**	An attacker manages to access the system's resources without authorisation for doing so, typically taking advantage of a failure in the identification and authorisation system.

Threat category	Threat	Threat description
Wilful attacks	**Traffic analysis**	Without needing to analyse the contents of communications, the attacker can reach conclusions based on the analysis of the origin, destination, volume and frequency of the exchanges.
Wilful attacks	**Repudiation (denial of actions)**	An entity denies being involved in an exchange with a third party or carrying out an operation. The later rejection of actions or undertakings acquired in the past.
Wilful attacks	**Eavesdropping**	Attackers have access to information that is not theirs, without the information itself being altered.
Wilful attacks	**Deliberate alteration of information**	Intentional alteration of the information to obtain a benefit or cause damage.
Wilful attacks	**Destruction of information**	The intentional deletion of information to obtain a benefit or cause damage.
Wilful attacks	**Disclosure of information**	Intentional disclosure of information.
Wilful attacks	**Tampering with software**	The intentional alteration of the operation of a programme to obtain an indirect benefit when an authorised person uses it.
Wilful attacks	**Tampering with hardware**	The intentional alteration of the operation of hardware to obtain an indirect benefit when an authorised person uses it.
Wilful attacks	**Denial of services**	The lack of sufficient resources causes the system failure when the workload is too high.
Wilful attacks	**Theft of media or documents**	Theft of media directly causes a lack of resources to provide the services, that is, non-availability.
Wilful attacks	**Theft of equipment**	Theft of equipment directly causes a lack of resources to provide the services, that is, non-availability.
Wilful attacks	**Destructive attack**	Vandalism, terrorism, military action, etc.
Wilful attacks	**Enemy overrun**	When the premises have been invaded and control is lost over the means of work.
Wilful attacks	**Staff shortage**	Deliberate absence from the work post (strikes, labour absenteeism, unjustified absences, the blocking of accesses, etc.).
Wilful attacks	**Extortion**	Pressure with threats, on people, to oblige them to act in a certain way.
Wilful attacks	**Social engineering**	Taking advantage of the good will of some people to make them carry out activities of interest to a third party.
Service-related threats (cloud services, services provided by third parties)	**Loss of governance**	The loss of governance and control could have a potentially severe impact on the organisation's strategy and therefore on the capacity to meet its mission and goals.
Service-related threats (cloud services, services provided by third parties)	**Lock-in**	Relying strongly on the services of one provider can lead to severe difficulties in changing the provider.
Service-related threats (cloud services, services provided by third parties)	**Isolation failure**	Failure of mechanisms separating storage, memory, routing and even reputation between different tenants of the shared infrastructure.
Service-related threats (cloud services, services provided by third parties)	**Management interface compromise**	A management interface is compromised.
Service-related threats (cloud services, services provided by third parties)	**Insecure or ineffective deletion of data**	Deleting data from storage does not in fact mean that the data is permanently removed from the storage. The data could be accessed at a later time by another customer of an outsourcing partner/provider.

Threat category	Threat	Threat description
Service-related threats (cloud services, services provided by third parties)	**Compromise of service engine**	A compromise of the service engine will give an attacker access to the data of all customers, resulting in a potential complete loss of data or denial of service.
Service-related threats (cloud services, services provided by third parties)	**Subpoena and e-discovery**	Law enforcement authorities may ask operators of IT infrastructures to provide information pertaining to criminal cases, or information may have to be provided during civil lawsuits.
Service-related threats (cloud services, services provided by third parties)	**Risk from changes of jurisdiction**	When data is stored or processed in a data centre located in a country other than the customer country, there are numerous ways in which the change in jurisdiction could affect the security of the information.
Service-related threats (cloud services, services provided by third parties)	**Data protection risks**	Data protection law is based on the premise that it is always clear where personal data is located, who processes it and who is responsible for data processing. Distributed environments appear to conflict with this evidence.
Service-related threats (cloud services, services provided by third parties)	**User privacy and secondary usage of data**	Customers need to be informed about what data might be used by the providers for secondary purposes. This includes data that can be mined directly from user data by providers or indirectly based on user behaviour (clicks, etc.).
Service-related threats (cloud services, services provided by third parties)	**Incidence analysis and forensic support**	In the event of a security incident, applications and services hosted at a provider are difficult to investigate, as logging may be distributed across multiple hosts and data centres, in various countries.
Service-related threats (cloud services, services provided by third parties)	**Insecure interfaces and APIs**	Provisioning, management, orchestration and monitoring are all performed through APIs. The security and availability of general services is dependent on the security of these interfaces.

D Annex IV – Toolbox impact scale

The EU RM toolbox impact scale comprises five levels, which are: (i) very high; (ii) high; (iii) moderate; (iv) low; and (v) very low. The impact that corresponds to each of these levels is detailed below to help stakeholders to identify corresponding levels that best fit to their environment.

- Very high: disastrous.
  - A threat event leads to disastrous business impacts.
  - A threat event leads to financial loss that is bigger than 5 % of the organisation's annual turnover/budget.
  - Information leaks might threaten the organisation's survival.
  - A threat event leads to corruption that is irrecoverable or causes permanent downtime.
  - Unavailability that takes extreme efforts to regain, or that is permanent.
  - Negative impact on the reputation of the organisation or its employees with global media coverage.
  - A threat event leads to discontinuation of all organisational services.
  - The organisation might receive a harsh penalty, which might bring some lethal costs close to being insurmountable.
  - Significant repercussions that are almost irreversible and cannot be surpassed (e.g. death, working impossibility).
- High: critical.
  - A threat event leads to critical business impacts.
  - A threat event leads to financial loss that ranges from 2 % to 5 % of the organisation's annual turnover/budget.
  - Information leaks severely undermine the interests of an organisation.
  - A threat event leads to corruption that imposes a substantial burden on the stakeholders.
  - Intense unavailability that causes significant inconvenience for stakeholders.
  - Significant decline in the organisation's reputation with repeated media criticism.
  - A threat event leads to complete departmental disruption. Indictment against the business.
  - A threat event costs the organisation a considerable amount of money in fees.
  - Significant outcomes that might be surpassed, but with considerable challenges (e.g. bank ban).
- Moderate: average.
  - A threat event leads to average business impacts.
  - A threat event leads to financial loss that ranges from 0.05 % to 2 % of the organisation's annual turnover/budget.
  - Information leaks undermine the interests of the organisation.
  - A threat event leads to corruption that causes difficulty for the affected parties, nevertheless, the recovery is simple.
  - Limited availability causes difficulty for the concerned stakeholders.
  - A threat event leads to temporary damage to the reputation of the organisation with occasional media criticism.
  - A threat event leads to isolated events with minimal consumer/citizen effect.
  - A threat event leads to possible penalties for the organisation and might introduce non-marginal charges.

    - Significant difficulty that might be compounded by a few complications (e.g. denial of access to commercial delivery).
- Low: marginal.
    - A threat event leads to marginal business impacts.
    - A threat event leads to financial loss that ranges from 0.01 % to 0.05 % of the organisation's annual turnover/budget.
    - Leaks of information are detrimental to the overall interests of the organisation.
    - Eradicating the corruption would not have any negative repercussions.
    - Lack of availability that causes inconvenience but does not seriously compromise the interests of the stakeholders.
    - A threat event leads to infrequent media criticism.
    - A threat event leads to minor occurrences that had no effect on their service users.
    - A threat event introduces some supplemental charges. A very low chance of any sentences, or perhaps a very minor possibility of one.
    - A little setback that can be easily overcome (e.g. time waste).
- Very low: negligible.
    - A threat event leads to negligible business impacts.
    - A threat event leads to financial loss that is less than or equal to 0.01 % of the organisation's annual turnover/budget.

E Annex V – Toolbox risk scale

The EU RM toolbox risk scale comprises five levels, which are: (i) very high; (ii) high; (iii) moderate; (iv) low; and (v) very low. These levels are affected by the levels of impact and probability, as demonstrated by the risk matrix shown in Figure 2 and detailed below.

- Very high.
  - A threat event leading to disastrous (very high impact) business impacts is predicted as almost certain (very high probability) to materialise.
  - A threat event leading to disastrous (very high impact) business impacts is predicted as very likely (high probability) to materialise.
  - A threat event leading to critical (high impact) business impacts is predicted as almost certain (very high probability) to materialise.
- High.
  - A threat event leading to disastrous (very high impact) business impacts is predicted as unlikely (low probability) to materialise.
  - A threat event leading to disastrous (very high impact) business impacts is predicted to potentially (moderate probability) materialise.
  - A threat event leading to critical (high impact) business impacts is predicted as almost certain (very high probability) to materialise.
  - A threat event leading to critical (high impact) business impacts is predicted as very likely (very high probability) to materialise.
  - A threat event leading to average (moderate impact) business impacts is predicted as very likely (high probability) to materialise.
  - A threat event leading to average (moderate impact) business impacts is predicted as almost certain (very high probability) to materialise.
  - A threat event leading to marginal (low impact) business impacts is predicted as almost certain (very high probability) to materialise.
- Moderate.
  - A threat event leading to disastrous (very high impact) business impacts is predicted as very unlikely (very low probability) to materialise.
  - A threat event leading to critical (high impact) business impacts is predicted as unlikely (low probability) to materialise.
  - A threat event leading to average (moderate impact) business impacts is predicted as unlikely (low probability) to materialise.
  - A threat event leading to average (moderate impact) business impacts is predicted to potentially (moderate probability) materialise.
  - A threat event leading to marginal (low impact) business impacts is predicted to potentially (moderate probability) materialise.
  - A threat event leading to marginal (low impact) business impacts is predicted as very likely (high probability) to materialise.
  - A threat event leading to negligible (very low impact) business impacts is predicted as almost certain (very high probability) to materialise.
- Low.
  - A threat event leading to critical (high impact) business impacts is predicted as very unlikely (very low probability) to materialise.
  - A threat event leading to average (moderate impact) business impact is predicted as very unlikely (very low probability) to materialise.
  - A threat event leading to marginal (low impact) business impact is predicted as unlikely (low probability) to materialise.

- A threat event leading to negligible (very low impact) business impacts is predicted to potentially (moderate probability) materialise.
- A threat event leading to negligible (very low impact) business impacts is predicted as very likely (high probability) to materialise.

- Very low.
  - A threat event leading to marginal (low impact) business impacts is predicted as very unlikely (very low probability) to materialise.
  - A threat event leading to negligible (very low impact) business impacts is predicted as very unlikely (very low probability) to materialise.
  - A threat event leading to negligible (very low impact) business impacts is predicted as unlikely (low probability) to materialise.

F ANNEX VI – Risk calculation interoperability samples

This annex presents two experiments that prove the interoperability among various methodologies and the proposed toolbox. We have to note that the toolbox seamlessly works with ITSRM^2, Monarc, EBIOS (expression of needs and identification of security objectives) and Magerit. The toolbox is equipped with **dropdown** lists that contain, in a numerical approach, the impact and probability level of the aforementioned methodologies. ITSRM^2 has been harmonised in 5 levels instead of 10 based on the approach that is proposed in the corresponding guideline. EBIOS and Magerit are methodologies that support the five cybersecurity risk scaling. While Monarc supports a three cybersecurity risk scaling (high, medium and low). To prove the aforementioned feature of interoperability, we performed two experiments with Monarc and Magerit.

Experiment 1.

We assume that the final user is an organisation that works within the energy sector and performs risk per threat following the Monarc method. At this point, we will calculate the risk of this organisation against the threat of the denial of service. On the one hand, the impact coming from Monarc depends on parameters including the impact of threat in confidentiality, integrity, availability, reputation, operational, legal, financial and personal. The overall impact scores 4 out of 4. On the other hand, the probability of a threat depending on existing system vulnerabilities and likelihood of occurrence of the corresponding threat scores 4 out of 4. The overall risk due to the Monarc approach is considered as high. However, based on the toolbox approach, the risk of the corresponding organisation is considered as very high.

Experiment 2.

We assume that the final user is an organisation that works within the healthcare sector and performs risk per threat following the Magerit method. At this point, we will calculate the risk of this organisation against the threat of the denial of service. On the one hand, the impact coming from Magerit depends on parameters that are directly related to economical loss. The overall impact scores 4 out of 5 (less than 1 000 000 000.00 monetary units). On the other hand, the frequency of occurrence of a threat scores 3 out of 5 (less than a year). The overall risk due to the Monarc approach is considered as high. Following this experiment, the toolbox agrees with the initial result that entitled it as high risk.

G Annex VII – Toolbox libraries

This annex provides the list of toolbox libraries.

- EU RM Toolbox Library 01 – Terms Mappings v1.0
- EU RM Toolbox Library 02 – Assets Mappings v1.0
- EU RM Toolbox Library 03 – Threats Mappings v1.0
- EU RM Toolbox Library 04 – Risk-Impact Levels Mappings v1.0

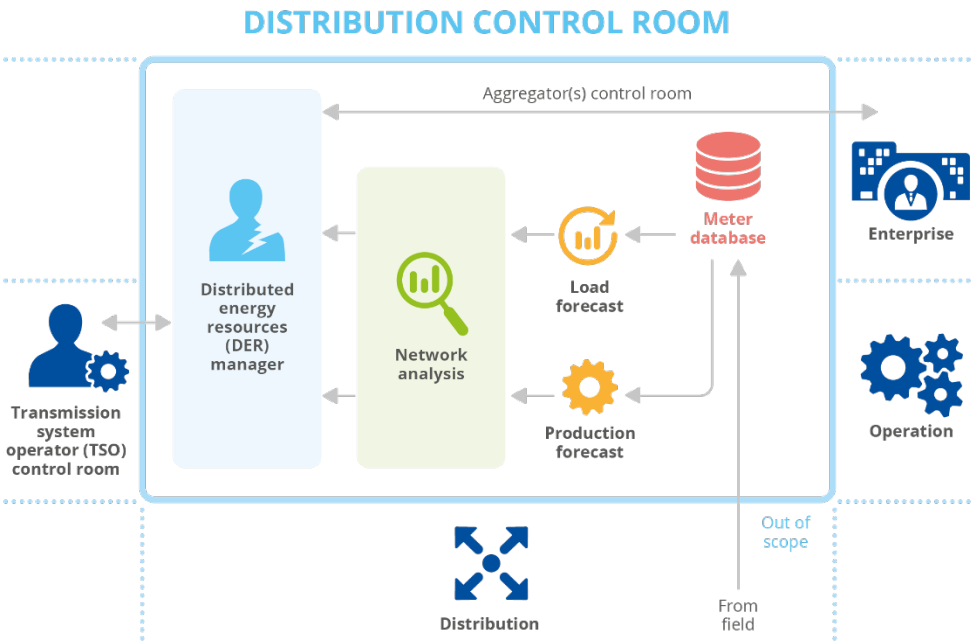
H Annex VIII – Use case example

This annex provides an example of a use case that has been developed in the context of a competent authority wishing to have an overview of the risk levels faced by an organisation in a specific sector.

Scenario description

A NIS competent authority wants to identify risk exposures at the national level against an emerged threat that is related to the spread of a ransomware that targets mainly distribution system operators (DSOs) in the energy sector. More specifically, the attack aims to encrypt the databases of distributed energy resources management systems, thus disabling load and production forecasting and the grid network operations at distribution level (see Figure 6). The attackers initially infect a DSO's network with malicious loaders through updates of several backup server suites deployed in DSOs' networks.

Figure 3: Logical architecture of the targeted DSO network



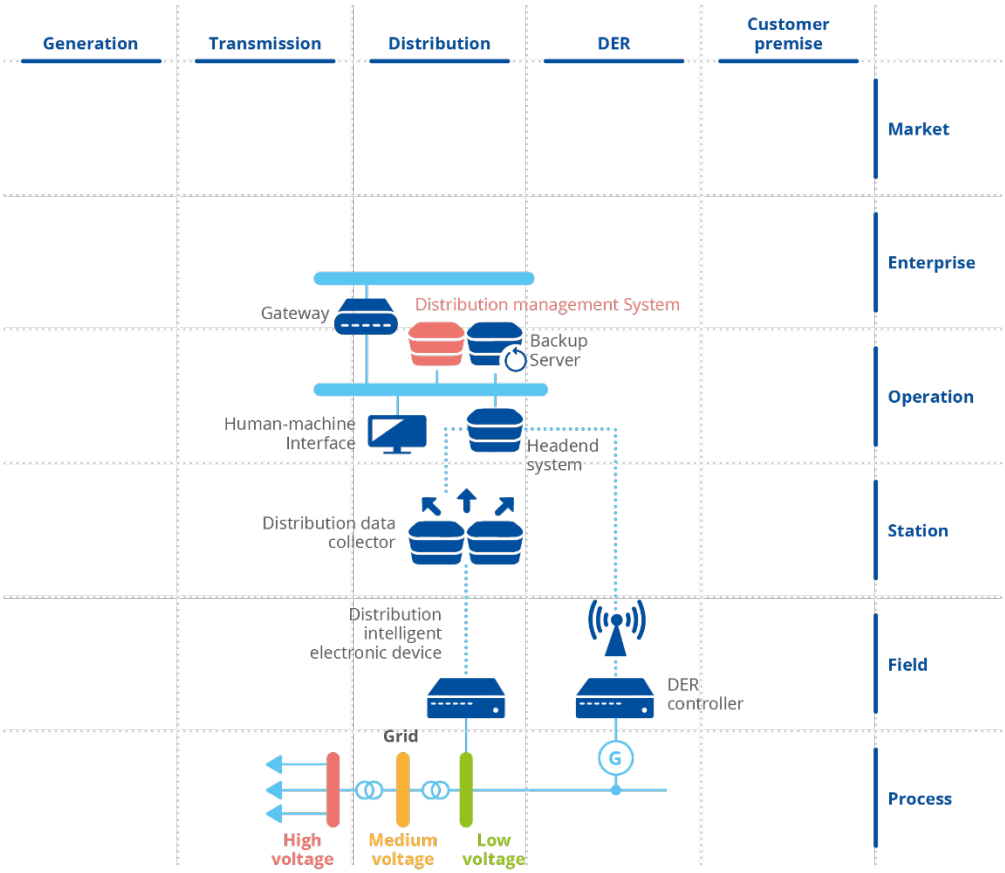
Indicative assets in scope

This section lists indicative assets that are involved in the incident scenario. The typical relationship of the involved tangible assets is depicted in Figure 7, although the DSOs' architectures are expected to vary. In parentheses is the type of assets according to the toolbox's asset classification: **data, function, software, hardware, IT services, personnel, location.**

Use case's indicative involved assets:

Distribution management system (DMS) data (data) / DMS backup data (data) / load forecast (function) / production forecast (function) / backup server (software) / backup server (hardware) / networking devices (IT services) / DMS server (software/hardware).

Figure 4: Assets involved in the incident scenario mapped to the smart grid architecture model



Attack path

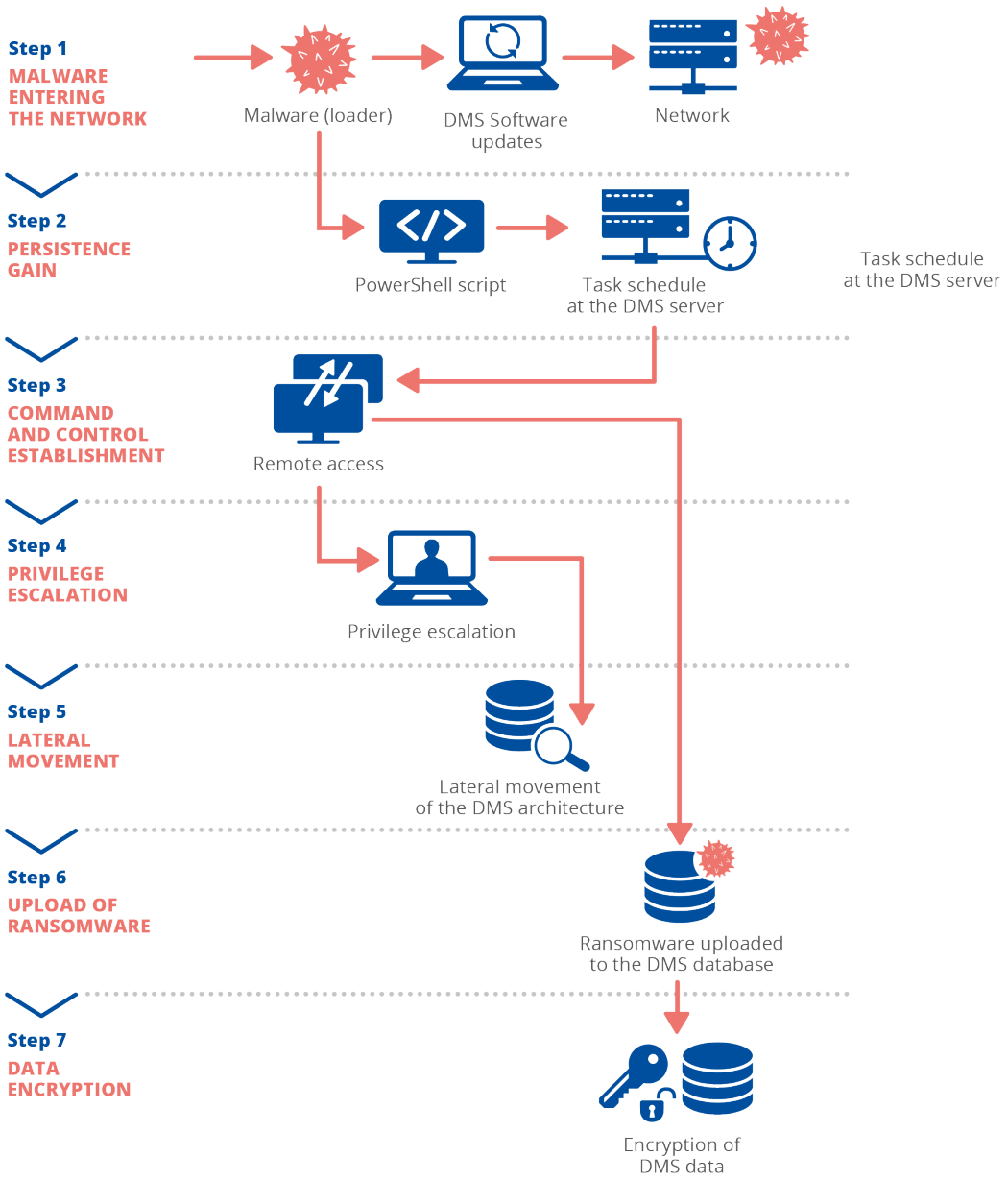
The attack path for the ransomware incident scenario comprises the following steps.

1. **Attack path step 1.** An initial malware (loader) enters the network through the software update channel of the backup software (located at the organisation's operation network).
2. **Attack path step 2.** The loader executes a PowerShell script to create a scheduled task at the backup server and gain persistence to the target network.
3. **Attack path step 3.** The scheduled task is executed daily and creates a command-and-control channel between the adversary-controlled remote server and the victim's system.
4. **Attack path step 4.** The malware gains access to an admin's valid local accounts to use the admin's privileges in lateral movement.
5. **Attack path step 5.** The malware conducts remote system discovery for lateral movement.
6. **Attack path step 6.** Ransomware is uploaded through the command-and-control channel to DMS.
7. **Attack path step 7.** The attacker obtains access to a backup server / destroys backups.

8. **Attack path step 8.** The ransomware encrypts the database of the distribution system.

The above steps are depicted in Figure 8.

Figure 5: Attack path steps



Attack scenarios

In this section, we describe the attack scenarios per attack step, each comprising of **<assets, threats, impact>**. The list of involved assets includes targeted assets, such as the DMS data, and assets that are part of the attack surface or the attack vector. Moreover, the list of threats is indicative, and additional threats can also be examined.

Table 5: Indicative attack scenarios

Attack steps	Attack scenario (ID v description)	Indicative involved assets (type)	Indicative threat scenarios	MITRE ATT&CK® framework	Impact / affected security dimension (confidentiality, integrity, availability)
1. Initial malware (loader) enters the network	1.1. Malware gains foothold through software updates (supply chain attack)	DMS backup data (data) / load forecast (service) / production forecast (service) / backup server (software) / backup server (hardware)	Unintentional malware diffusion	Initial access (T1195 supply chain compromise)	C-I-A
2. Attacker gains persistence	2.1. PowerShell script is executed and scheduled task is created	DMS backup data (data) / load forecast (service) / production forecast (service) / backup server operating system (software)	Manipulation of the configuration files	Execution (T1204 user execution, T1059 command and scripting interpreter)	C-I-A
3. Command-and-control channel is established	3.1. The C2 channel enables communication with adversary-controlled servers	DMS backup data (data) / backup server operating system (software) / networking devices (IT services)	Manipulation of the configuration files	Command and control (T1071 application layer protocol, T1219 remote access software)	C-I-A
4. Privilege escalation	4.1. Adversaries use stolen valid accounts during lateral movement	DMS data (data) / backup server operating system (software)	Masquerading of identity	Privilege escalation (T1078 valid accounts)	C-I
5. Discovery	5.1. Adversaries attempt to discover details of the DMS architecture	DMS data (data) / load forecast (service) / production forecast (service) / networking devices (IT services)	Unauthorised access (network)	Discovery (T1083 file and directory discovery)	C
6. Lateral movement	6.1. Ransomware uploaded to the DMS database	DMS data (data) / load forecast (service) / production forecast (service) / DMS server (software/hardware)	Intentional malware diffusion	Lateral movement (T1210 exploitation of remote services), command and control (T1105 ingress tool transfer)	C-I-A
7. Backups are deleted	7.1. Adversary deletes all backups at the backup server	DMS backup data (data) / backup server	Destruction of information	Impact (T1485 data destruction)	A

Attack steps	Attack scenario (ID v description)	Indicative involved assets (type)	Indicative threat scenarios	MITRE ATT&CK® framework	Impact / affected security dimension (confidentiality, integrity, availability)
8. Data is encrypted	8.1. The DMS data is encrypted using the uploaded ransomware	DMS data (data) / load forecast (service) / production forecast (service) / DMS server (software)	Unauthorised access	Impact (T565 data manipulation)	C-I-A

Deliverables

The participants are expected to provide the results of the risk assessment for all the risk scenarios that they will run in the form of a list. Moreover, they have to name the method and/or tool they have used for the risk assessment. The provided information will allow the toolbox to be used to normalise risk values and compare results.

Important NB: To avoid the unintentional disclosure of sensitive information regarding the participants' environments, the participants are kindly asked to provide biased information that does not necessarily reflect the actual status, as this is not the aim of this task.

6. Bibliography/references

ENISA (2021) Interoperable EU Risk Management Framework [Online]. Available at: https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework

International Standardization Organisation, 2018. ISO/IEC 27005:2018 *Information technology — Security techniques — Information security risk management*

European Commission Directorate-General for Communication, Security standards applying to all European Commission information systems. EU ITSRM, IT SECURITY RISK MANAGEMENT METHODOLOGY V1.2. [Online]. Available at: https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_en

International Standardization Organisation, 2018. ISO/IEC 27000:2018, Information technology – Security techniques – Information security management systems – Overview and vocabulary, s.l.: International Standardisation Organisation.

ISO/IEC 2382-1:1993 Information Technology – Vocabulary – Part 1: Fundamental terms. International Organisation for Standardization (ISO). [Online]. Available: http://www.iso.org/iso/catalogue_detail.htm?csnumber=7229

Joint Task Force Transformation Initiative, 2012. Guide for Conducting Risk Assessments. [Online]. Available at: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

Joint Task Force, 2018. Risk Management Framework for Information Systems and Organisations: A System Life Cycle Approach for Security and Privacy. [Online]. Available at: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

Standard Computer Dictionary IEEE, A Compilation of IEEE Standard Computer Glossaries. IEEE, New York, NY, 1990 https://www.standardsuniversity.org/article/standards-glossary/#I

Lars Fischer, Mathias Uslar (OFFIS), Doug Morrill (Navigant), Michael Döring, Edwin Haesen (Ecofys), 2018. Study on the Evaluation of Risks of Cyber-Incidents and on Costs of Preventing Cyber-Incidents in the Energy Sector. [Online]. Available at: https://energy.ec.europa.eu/study-evaluation-risks-cyber-incidents-and-costs-preventing-cyber-incidents-energy-sector_en

Lockheed Martin, 2021. The Cyber Kill Chain. [Online]. Available at: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

MITRE, 2015-2021. *MITRE ATT&CK*. [Online]. Available at: https://attack.mitre.org/

TP-04-22-275-EN-C

About ENISA

The European Union Agency for Cybersecurity (ENISA) is the EU's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the EU's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-609-5