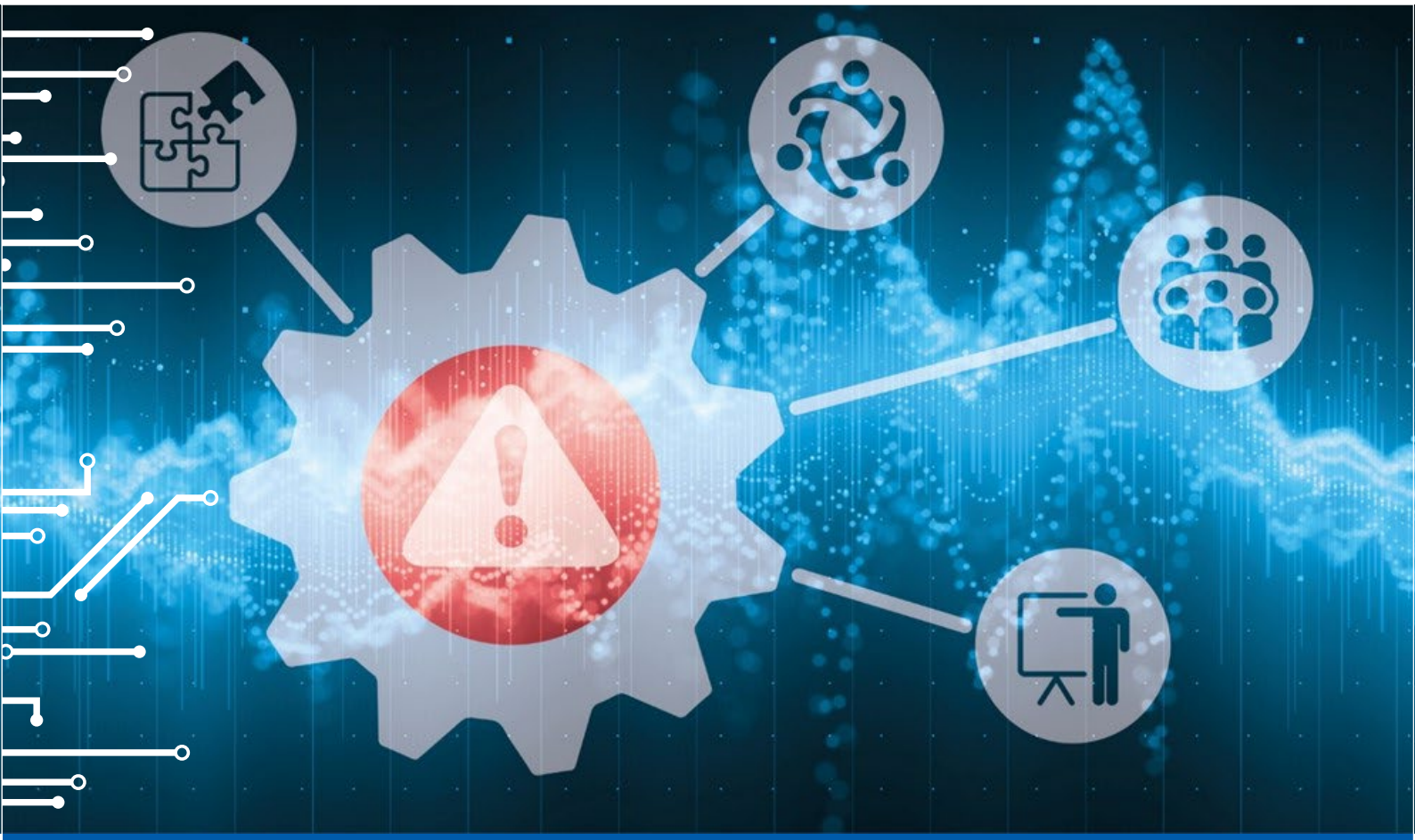
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



INTEROPERABLE EU RISK MANAGEMENT FRAMEWORK

Methodology for assessment of interoperability among risk management frameworks and methodologies

UPDATED REPORT, DECEMBER 2022

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity 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 Union'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.

CONTACT

To contact the authors, please use CBU@ENISA.EUROPA.EU

For media enquiries about this paper, please use PRESS@ENISA.EUROPA.EU

AUTHORS

Costas Lambrinoudakis, Stefanos Gritzalis, Christos Xenakis, Sokratis Katsikas, Maria Karyda, Aggeliki Tsochou of University of Piraeus

Kostas Papadatos, Konstantinos Rantos, Yiannis Pavlosoglou, Stelios Gasparinatos, Anastasios Pantazis of CyberNoesis

Alexandros Zacharis of ENISA

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-553-1 DOI:10.2824/07253 Catalogue Nr: TP-01-22-004-EN-N

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report is an update of the report “Interoperable EU Risk Management Framework” published by ENISA in January 2022. The “Interoperable EU Risk Management Framework” proposes a methodology for assessing the potential interoperability of risk management (RM) frameworks and methods and presents related results. The methods included in this report have been selected as prominent, based on their interoperability features, after evaluating an extended list of risk management frameworks and methods (included in the Compendium of Risk Management Frameworks with Potential Interoperability, ENISA, January 2002) which has been published as Supplement to the Interoperable EU Risk Management.

The “Interoperable EU Risk Management Framework” describes and evaluates the interoperability features for prominent risk management frameworks and methods, by employing a four-level scale to evaluate their interoperability level. The features assessed to evaluate the interoperability level include the approach used by the RM method (i.e. to whether it is asset-based or scenario-based), whether risk assessment is quantitative or qualitative, as well as other characteristics such as the use of asset taxonomies, valuation methods, the cataloguing of threats and vulnerabilities, the method of risk calculation etc. It also provides an overview of possible collaborative combinations between them.

The update of “Interoperable EU Risk Management Framework” was based on desktop research and analysis, which resulted in:

- Identifying new risk management methods, which were evaluated with regard to their interoperability potential and included in the ““Interoperable EU Risk Management Framework”. These are the following:
    - SERIMA
    - CIRCULAR CSSF 20/750

- Updating the features and evaluation of the following RM methods which were already included in the Framework:
    - MONARC
    - ITSRM²
    - THE OPEN GROUP STANDARD, RISK ANALYSIS

Finally, no updates were identified for the following:

- ISO/IEC 27005:2018
- NIST SP 800-37
- NIST SP 800-30
- NIST SP 800-39
- BSI STANDARD 200-2
- OCTAVE-S
- OCTAVE ALLEGRO
- OCTAVE FORTE
- ETSI TS 102 165-1(TVRA)
- EBIOS Risk Manager
- MAGERIT v.3
- MEHARI
- GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

1. INTRODUCTION

1.1 PURPOSE AND SCOPE

This report presents an updated analysis of the interoperability features of prominent RM frameworks and methodologies, as this was initially presented in the **Interoperable EU Risk Management Framework** published by ENISA in January 2022, along with the method followed to determine their interoperability potential. A presentation and brief description of the RM methods is provided in the "Compendium of Risk Management Frameworks"[1] .

The updated version of the **Interoperable EU Risk Management Framework** presented in this report includes a) new RM methods, and b) newer versions of already identified RM frameworks and methods. A detailed evaluation regarding the potential for interoperability of the RM frameworks, based on their features and an evaluation model, is also included. The corresponding results show the potential for forming a coherent RM framework through various possible combinations of the features of the aforementioned frameworks.

The detailed analysis of the RM frameworks and methodologies, the methodology used to evaluate them and the results of this process, aim at the provision of a clear outcome in regard to potentially forming a coherent RM framework that could support information risk management in different organisations and sectors across EU.

The methodology for evaluating the interoperability potential of different RM methods upon which the Interoperable Framework is based, was the result of meticulous research and analysis carried out by professionals involved in both the academic sector and organisations that engage in RM-related activities and research, informed by the comments, recommendations and insights provided by key stakeholders. The output of this work is a method for evaluating the potential for interoperability of different RM frameworks and tools, along with the results of this evaluation, for a list of prominent RM methods.

1.2 DEFINITION OF ACRONYMS

The acronyms used in this document and recurring definitions are listed below.

Acronym	Definition
RM	Risk Management
MS	Member States
ITSRM	IT Security Risk Management Methodology
AB	Asset based
SB	Scenario based
QT	Quantitative
QL	Qualitative

[1] https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks

2. METHOD OF WORK

The methodology for assessing the interoperability of risk management frameworks and methodologies, mainly draws on assessment models. Gilsinn and Schierholz (2010) developed an assessment model for information assurance for a given information technology, which comprises seven features (e.g. access control, resource availability) that are relevant to information assurance. Using those features the assessment model classifies a given technology into four levels of increasing security (i.e. protection against casual or coincidental violation, protection against intentional violation using simple means, protection against intentional violation using sophisticated means, protection against intentional violation using sophisticated means with extended resources).

In another example, ENISA (2016) developed an assessment model to assess the readiness of information technology (and specifically privacy-enhancing technologies). The model identifies nine features that are relevant to the quality and readiness of an information technology (i.e., Protection, Trust assumptions, Side effects, Reliability, Performance efficiency, Operability, Maintainability, Transferability and Scope). Each technology receives a grade for each feature using a five-level scale (very poor, poor, satisfactory, good, very good). Depending on the assessment of each feature, the model classifies a given privacy-enhancing technology into one of six levels (Idea, Research, Proof-of-concept, Pilot, Product, Outdated).

In this chapter we describe the features that we identified as relevant for the assessment of the interoperability features of risk management frameworks and methodologies. Further, for the functional features we describe a four-level scale to evaluate the interoperability level of each RM framework. Finally, we propose a three-level scale for the potential interoperability for each framework and for combined features.

2.1 FEATURES OF INTEROPERABILITY

The risk management area is characterised by a plethora of frameworks, methodologies and methods, each of them with their own characteristics and following their own approach in managing risks. During the risk management lifecycle, practitioners might want to reuse information provided by other methodologies or consider comparing results among frameworks. This typically requires the methodologies to be able to share information and therefore provide capabilities for interoperability.

There is no single definition of interoperability in the literature, as this is a generic term that can be applied to many sectors and disciplines. As such, it strongly depends on the context in which it is applied, satisfying its peculiarities and specific demands. In the ICT sector, interoperability is considered as the ability of two or more systems or components to exchange information and to use the information that has been exchanged.
ISO/IEC 2382 defines interoperability as *the capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units*.

The IEEE Standard Computer Dictionary also places emphasis on the required effort thus defining interoperability as the *ability of a system or a product to work with other systems or products without special effort on the part of the customer*. This definition is also adopted by ISO 23903 regarding interoperability in the health sector.

The European Interoperability Framework defines interoperability as *“the ability of organisations to interact towards mutually beneficial goals, involving the sharing of information and knowledge*

between these organisations, through the business processes they support, by means of the exchange of data between their ICT systems.

Considering the above definitions as well as the structure of management frameworks for cyber risks and the targets of their individual functional characteristics, the interoperability of risk management frameworks and methodologies can be defined as *the ability of a risk management component or methods to reuse information provided by the risk management components or methods of other frameworks with equal ease and with the same interfaces, towards the same goals*.

A risk management framework or methodology should address at least the following phases (ISO 27005, EU ITSRM) which can be considered as its main functional components:

- Risk Identification (Assets, Threats and Vulnerabilities)
- Risk Assessment (Risk Calculation and Evaluation),
- Risk Treatment (Selection and Implementation of Security Controls, and Calculation of Residual Risk),
- Risk Monitoring (Assess effectiveness of measures and monitor risks).

From the above functional components, Risk Monitoring is a process that, although essential for efficient risk management, is independent of the rest of the phases and can typically be conducted using any assessment methodology, process or tool. As such, it is considered outside the scope of this report which focuses on the other three phases instead, i.e. Risk Identification, Risk Assessment and Risk Treatment.

Overall, there are many characteristics (governance, compliance, privacy) that constitute integral parts of risk frameworks but not all of them affect interoperability. Considering the aforementioned definition and the above functional components, we could argue that interoperability in risk management can be achieved if these components can be addressed by the components of other frameworks, with similar effectiveness and ease. This essentially means that **interoperability can be achieved at various levels, and we will consider the functional and non-functional characteristics** of the evaluated frameworks.

As such, **regarding the functional characteristics**, the interoperability between risk management frameworks can be evaluated against the following levels: Generic aspects, Risk Identification, Risk Assessment and Risk Treatment, which are further analysed to a set of features that typically stem from the above functional components.

- **Generic aspects**: At this aspect we consider some generic features of the frameworks, which are:
    - **Asset based or Scenario based**: this indicates whether a risk management framework or methodology adopts an asset-based approach or is guided by a risk scenario. These approaches could be combined. Therefore, our analysis includes frameworks or methodologies that distinctly follow either an asset-based or a scenario-based approach, as well as methodologies that adopt both or a combination of these approaches.
    - **Quantitative or Qualitative**: this indicates whether the risk management framework or methodology adopts a risk assessment method that is based on quantitative or qualitative criteria. This does not exclude a third category that is used for risk assessment, the semi-quantitative method, in which case the method examined is categorised as either quantitative or qualitative, whichever is closer.
- **Risk Identification**: risk management frameworks are considered interoperable if they can use each other's asset taxonomy and valuation, threat and vulnerability catalogues, with equivalent results and without negatively affecting subsequent steps. At this level we consider the following features:
    - **Asset Taxonomy**: it indicates whether the framework or methodology requires the use of a specific asset taxonomy.

    - **Asset Valuation**: it indicates whether the framework or methodology requires the use of a specific asset valuation method.
    - **Threat catalogues**: these indicate whether the framework or methodology requires the use of a specific set of threats.
    - **Vulnerability catalogues**: these indicate whether the framework or methodology requires the use of a specific catalogue of vulnerabilities.
- **Risk Assessment**: risk management frameworks are considered interoperable if they use the same methodology for risk assessment, or their methods can provide results that can be easily mapped to the results of other frameworks. At this level we consider the following features:
    - **Risk Calculation method**: it provides information about the method used for risk calculation. e.g. Risk = Impact x Likelihood; Risk = Impact x Threat Likelihood x Vulnerability Level.
- **Risk Treatment**: risk management frameworks are considered interoperable if they result in the same set of measures or a set of measures with an equal contribution to reducing levels of risk. At this level we consider the following features:
    - **Measures catalogue**: it indicates whether the framework or methodology requires the use of a specific catalogue of measures. If so, it also considers whether the two catalogues can be mapped to each other.
    - **Residual Risk Calculation**: it considers the chosen measures to evaluate the remaining levels of risk. This process is typically affected by both the risk calculation method and the impact of the chosen security measure(s) on a risk scenario.

Non-functional characteristics that can also be used for assessing the interoperability of risk management frameworks include:

- **Supported languages:** An English version of the methodology is an advantage.
- **Compliance** with other risk-related frameworks (e.g. ISO 27005). Such compliance is likely to promote interoperability among frameworks.
- **Risk Management Life-Cycle Coverage**: the level of coverage of the above functional components of a risk management framework.
- **Licensing** costs that might hinder interoperability.

The **overall interoperability potential** of risk management frameworks and methodologies will be evaluated using a weighted approach on some of the above aspects of interoperability since some of them might prohibit the interoperability of the frameworks, while others might simply hinder it. For example, language issues are considered an obstacle that can be bypassed, while different approaches in risk calculation will not allow the two frameworks to use components of the other's method.

Similarly, some of the above features are considered to be exclusive, i.e. if the feature is not satisfied then interoperability cannot be achieved at any of the aforementioned levels. Such exclusive features are the 'Asset based or Scenario-based' and 'Quantitative or Qualitative' based features.

A framework or methodology that does not require, define or dictate specific methods for the above functional components is obviously considered highly interoperable. Such frameworks can accommodate risk management components from various methods. For example, the NIST 800-37 risk management framework can typically use any threats, vulnerabilities and catalogue of measures, and can accommodate any method for calculating the risk. In this respect, it is considered a highly interoperable framework. Similarly, BSI Standard 200-2 (IT-Grunschutz Methodology) integrates components from the IT-Grundschutz Compendium, and specifically accommodates the asset typology, the threat list and the catalogue of controls.

If a methodology has strict requirements regarding the above functional components, its interoperability is bound to be restricted. For example, if risk assessment is tightly coupled with a specific threat or vulnerability catalogue, its ability to adopt an alternative catalogue provided by another method, is restricted.

On the other hand, risk management methodologies that do require following specific, predefined characteristics (e.g. an asset taxonomy or a calculation method) could provide a

high potential for interoperability if these characteristics are described in detail so that other methodologies or frameworks can accommodate them.

2.2 INTEROPERABILITY EVALUATION MODEL

2.2.1 Methodology and levels of interoperability

For the evaluation of potential interoperability among risk management frameworks and methodologies, we initially consider the **inherent level of interoperability of the framework or methodology** regarding functional features. This shows whether a specific framework allows interoperability with other frameworks with regards to these specific features. Regarding the features that contribute to the interoperability of the identification, estimation and treatment of risk, a four-level scale was used:

- **Non Applicable:** the framework or methodology does not use or support this feature.
- **Low Level of Interoperability:** the framework or methodology requires a proprietary solution for this feature, provided by the framework itself.
- **Medium Level of Interoperability:** the framework or methodology provides details but are not compulsory, and therefore the proposed solution is modifiable.
- **High Level of Interoperability**: the framework or methodology uses this feature, but it either does not provide any suggestions or it can adopt the features of a third framework, e.g. a standardised or a proprietary solution.

We have applied this evaluation methodology for the functional requirements and specifically for the following features:

- **Risk Identification**
  - **Asset Taxonomy**
  - **Asset Evaluation**
  - **Threat Catalogues**
  - **Vulnerability Catalogues**
- **Risk Calculation**
- **Risk Treatment**
  - **Measure Catalogues**
  - **Calculation of Residual Risk**

To evaluate the **potential interoperability** of each risk management framework or methodology, we first determine the **level of interoperability** of the Risk Identification, Risk Calculation and Risk Treatment functional components. More specifically, the following Table provides the main parameters that are evaluated for each functional characteristic of the risk management framework or methodology.

Table 1: Parameters evaluated for each functional characteristic

Characteristics	Parameters to Check
Asset Taxonomy	Does the framework or methodology use or describe specific categories of assets?
	Is the taxonomy used modifiable?
	Can the analyst introduce new categories of assets or import taxonomies from other sources?
Asset Valuation	Does the framework or methodology use or describe specific guidelines for the valuation of assets (i.e. scale and criteria for assessment of asset value and impact)?
	Are the proposed scales or criteria modifiable?
	Can the analyst introduce new scales or criteria?

Characteristics	Parameters to Check
Threat Catalogues	Does the framework or methodology use or describe specific threat catalogues and/or threat categories?
	Are the proposed threat catalogues and/or threat categories modifiable?
	Can the analyst introduce new threats and/or threat categories and import them from other sources?
Vulnerability Catalogues	Does the framework or methodology describe specific vulnerability catalogues and/or categories of vulnerabilities?
	Are the proposed vulnerability catalogues and/or categories of vulnerabilities modifiable?
	Can the analyst introduce new vulnerabilities and/or categories of vulnerabilities and import them from other sources?
Risk Calculation	Does the framework or methodology describe specific guidelines for the calculation of risk (i.e. formulas, scale, matrix)?
	Is the proposed calculation method modifiable?
	Can the analyst introduce or import (from other sources) new methods of calculation?
Measure Catalogues & Calculation of Residual Risk	Does the framework or methodology describe specific control catalogues and/or categories of controls?
	Are the proposed control catalogues and/or categories of controls modifiable?
	Can the analyst introduce new controls and/or categories of controls and import them from other sources?
	Is the Calculation of Residual Risk (either on a Calculation of Residual Risk formula or on an Impact of Measures formula) modifiable?

Based on the information collected and on how the aforementioned parameters were satisfied or not, we estimate the level of interoperability (No interoperability, Low, Medium or High level of interoperability) for each functional component (Risk Identification, Risk Assessment, Risk Treatment) for each risk management framework or methodology.

The higher the level of interoperability that a functional component holds, the more likely it is that the framework is interoperable with other frameworks regarding a specific feature or functionality (i.e. combined features).

As an example, a risk assessment framework regarding the feature 'Vulnerability Catalogues', will be evaluated as shown next.

- **Non applicable**, if the framework does not use vulnerabilities in the calculation of risk, hence interoperability with another framework, such as using another framework's catalogues as provided, is not applicable.
- **Low Level of Interoperability**, if the framework or methodology uses a proprietary vulnerability catalogue that cannot be modified or replaced by another one.
- **Medium Level of Interoperability**: if the framework or methodology uses a proprietary catalogue of vulnerabilities that can be modified.
- **High Level of Interoperability**: if the framework uses a proprietary vulnerability catalogue that can be modified and that can also accommodate other catalogues, and also where the framework or methodology might not use a proprietary vulnerability catalogue but can accommodate any other catalogue.

2.2.2 Scoring model for potential interoperability

After assessing the level of interoperability that each framework holds for each functional feature, we also evaluated the collective potential for interoperability for features that when combined result in specific functional components (e.g. risk identification). Specifically, for risk identification, we combined the assessment of the levels of interoperability regarding the

features of Asset Taxonomy, Asset Valuation, Threat Catalogues and Vulnerability Catalogues. Then to calculate the potential interoperability of the Risk Identification functional component of a given risk management framework or methodology, we applied the following weighting factors:

- Asset Taxonomy, Weighting factor: 30%
- Asset Valuation, Weighting factor: 50%
- Threat Catalogues, Weighting factor: 10%
- Vulnerability Catalogues, Weighting factor: 10%

Thus, the interoperability potential for the Risk Identification functional component will be:

- 30% * Interoperability Level for Asset Taxonomy +
- 50% * Interoperability Level for Asset Valuation +
- 10% * Interoperability Level for Threat Catalogues +
- 10% * Interoperability Level for Vulnerability Catalogues.

The above weights reflect the importance of each functional feature for the potential interoperability of the framework or methodology in relation to the rest of the functional features, as evaluated by the security experts who compose the project team (i.e. practical and research knowledge).

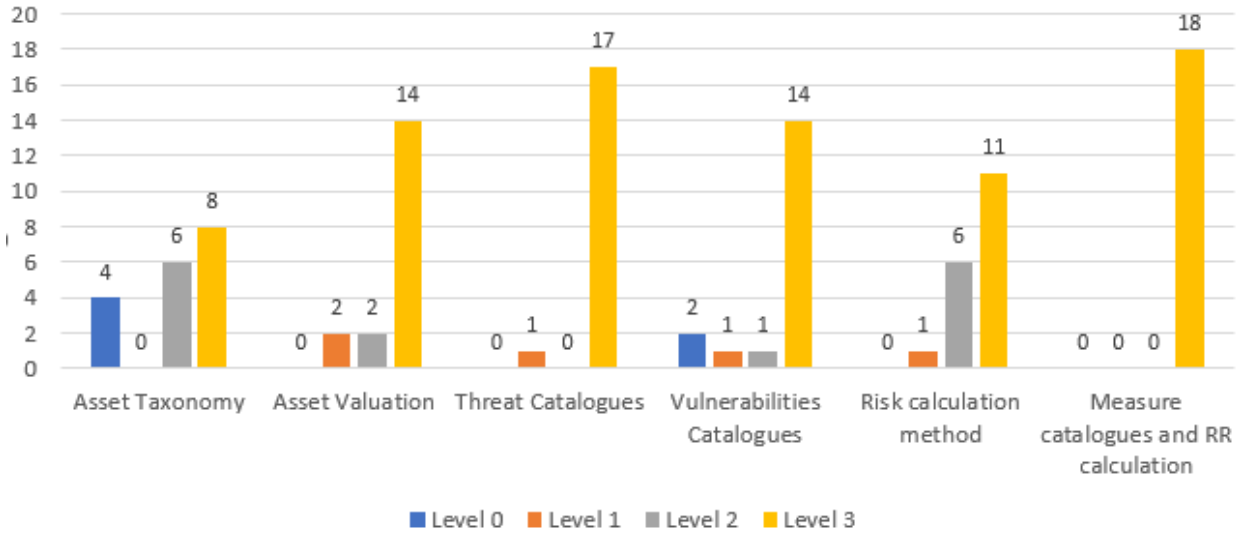
The potential interoperability of a given framework in terms of Risk Assessment and of the Risk Treatment process, is equal to their assessed levels of interoperability.

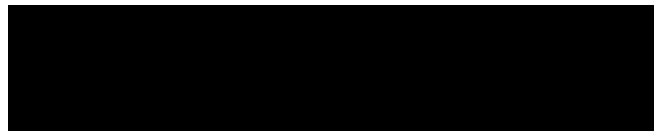
The fact that the potential interoperability for the Risk Identification, Risk Assessment and Risk Treatment process is presented separately, serves someone's need to interact with a framework only within one of the three distinct functional components. For example, it is possible that a framework could have a high potential for interoperability for risk identification but not for the risk treatment process.

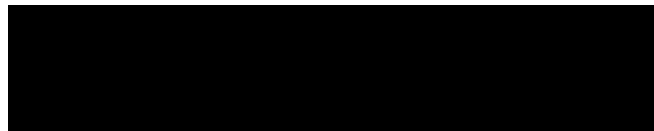
Finally, the overall potential interoperability of a Risk Management framework is calculated as the average of the interoperability potentials calculated for the Risk Identification, Risk Calculation and Risk Treatment functional components of the framework.

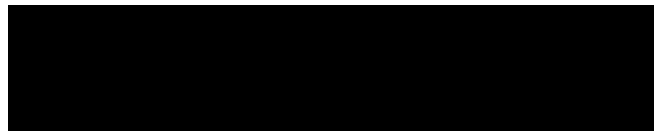
Regarding the potential interoperability of the methods that were analysed, all of them appear to be highly interoperable on threats and measures, hence allowing the adoption of additional catalogues provided by other methods or the alteration of their existing ones. Three of the methodologies analysed do not consider vulnerabilities in their approach to risk assessment. Moreover, 11 of the 18 methodologies are considered highly interoperable with respect to their approach to risk calculation and therefore more open to the adoption of alternatives, while 7 out of the 18 methodologies allow modification of the proposed method of risk calculation, typically in term of the scales that are used. The levels of interoperability of the methodologies analysed are summarised in the following table.

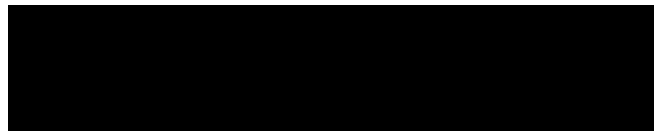
Figure 3: Levels of Interoperability

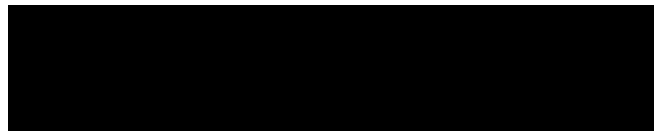


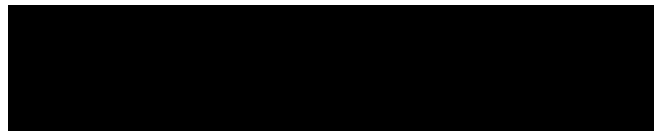


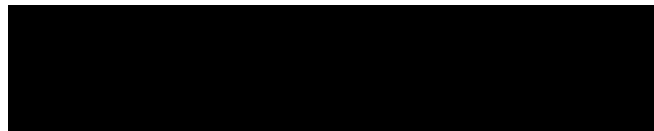


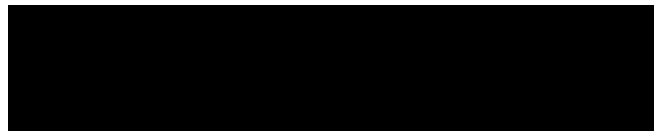


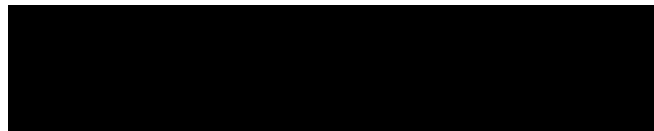


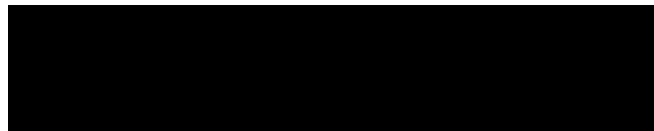


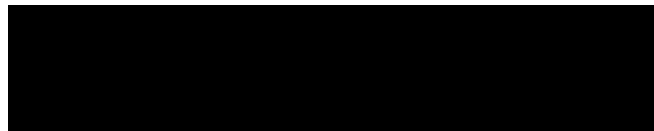


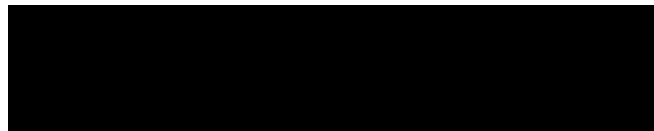








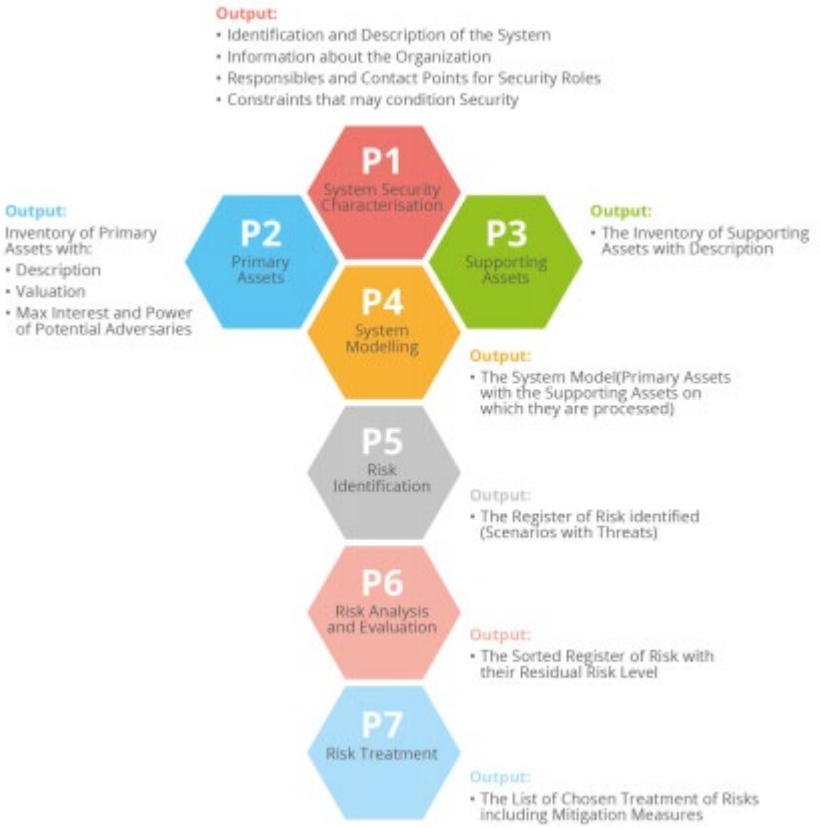




4. INTEGRATION OF INTEROPERABILITY IN THE RM PROCESSES BASED ON ITSRM2

Based on the analysis of RM frameworks and methodologies performed in in accompanying "Compendium of Risk Management Frameworks"3, two RM frameworks provide a thorough description of the typical RM processes, covering the overall RM lifecycle. These are ISO 27005 and ITSRM[2].
In this Chapter we provide recommendations regarding interoperability for the ENISA Work Programme for 2022 and thereafter in the area of Risk Management (RM), using ITSRM2 as a reference framework. The rationale behind this choice is that ITSRM2 is process-oriented and offers a detailed presentation of the inputs and outputs for each RM process, providing us with the grounding needed to discuss the recommendations for opportunities in interoperability. Figure 4 presents the ITSRM2 RM processes.

Figure 4: The ITSRM$_2$ processes



Before initiating the analysis for each RM process, one high-level recommendation for the facilitation of interoperability concerns the terminology. In particular, the problem exists in two cases: 1) using the same (English) term with different meanings, or 2) translating a term,

usually from the language in which the RM framework was developed, into other languages. In both cases, interoperability is hindered.
Therefore, we recommend working towards a: **Common terminology and translation of terms** in the languages of MS and supporting their integration into the RM frameworks. Next, we identify recommendations across the RM processes based on ITSRM2.

4.1 PROCESS P1 SYSTEM SECURITY CHARACTERISATION

4.1.1 Description of process

4.3.2 Recommendations and integration of interoperability features

To find the potential for interoperability in this process, it is advisable to work towards promoting standard representation techniques of the system model (e.g. all supporting assets required for the processing of primary assets, software architecture, logical model) to allow process P5 to use it regardless of the RM framework applied.

4.4 PROCESS P5 RISK IDENTIFICATION

4.4.1 Description of process

The objective of the P5 Risk Identification task is to build the risk scenarios that will be analysed. The risk scenarios are used to represent the risks for the organisation and the Primary assets regarding the consequences of potential threats in relation to the confidentiality, integrity and availability of the Supporting Assets.
To identify the threats that the Primary and Supporting assets of a specific information system are facing, this task will use the system model (output of P4). More specifically, the system model will provide useful information in order to identify which threats are most likely to occur for each triplet 'Primary Asset / Security Dimension (CIA) / Supporting Asset'. Another important parameter during the risk identification process is the identification of the vulnerabilities exhibited by the Supporting assets which can be explored by the relevant threats to harm the confidentiality or integrity or availability of a Primary asset.
The output of the process P5 Risk Identification will be a list of risk scenarios that will be evaluated in P6 Risk Analysis and Evaluation.
This process is part of the Risk Identification step of ISO 27005.

4.4.2 Recommendations and integration of interoperability features

Interoperability requires that, for the same system, two different RM frameworks should produce comparable risk scenarios or, for different systems, the risk scenarios produced by different RM frameworks are comparable. To achieve interoperability among different RM frameworks during the risk identification process, it is necessary to work towards the following.

- **Common threat repositories** that will feed the applicable (common) threats to the risk identification process of different RM frameworks. These repositories should:
    - classify threats in categories, depending on commonly accepted threat types (e.g. physical threats, malware, denial of service, failures etc.);
    - classify threats according to the sector to which they are applicable (e.g. threats for health organisations, threats for financial institutions etc.);
    - support a hierarchical structure for each threat category, starting from a high level threat description and continuing with lower-level technical details (instances) of each threat; this hierarchical structure will facilitate the interoperability of frameworks working with high-level threats (low-threat granularity) with frameworks considering threats at a much lower technical level (high threat granularity).
- **Risk scenarios** should take into consideration both the business perspective and the system perspective. They should also support the association of threats with Supporting assets (i.e. which threat is applicable to which Supporting asset).
- **Common vulnerability repositories** that will feed the applicable (common) vulnerabilities to the risk identification process of different RM frameworks. These repositories should also support the association of vulnerabilities and Supporting assets (i.e. which vulnerability is applicable to which Supporting asset).

The existence of the common repositories for threats and vulnerabilities will also support global awareness about new threats and vulnerabilities, allowing all RM frameworks to take them into account automatically.

4.5 PROCESS P6 RISK ANALYSIS AND EVALUATION

4.5.1 Description of process

The objective of the P6 Risk Analysis and Evaluation process is the computation of the residual risk level for each risk identified in P5 Risk Identification, based on the list of Security Measures identified to mitigate these risks.
The P6 Risk Analysis and Evaluation process uses as input the Primary asset inventory (from P2), the risk scenarios (from P5), the catalogue of threats (provided by the methodology), the risk scale (provided by the methodology), the treatment register (from P7, if it exists from past RMs), and the security measures register (from P7, if it exists from past RMs).
The output of the P6 Risk Analysis and Evaluation process is the risk register which guides decisions on the treatment of risk. For the analysis of risk, the analyst takes into consideration the likelihood of threats (based on types of threats and potential adversaries, provided by the methodology) and the consequences of a potential incident. A risk matrix is provided by the methodology, which calculates the inherent level of risk by combining the likelihood with the levels of consequences. The residual risk level is calculated after considering existing or planned security measures to mitigate the risk. Finally, the risk evaluation process provides an ordered list of risks from the highest to the lowest levels of risk.
This stage is mapped with the ISO 27005 Risk Analysis and Risk Evaluation processes.

4.5.2 Recommendations and integration of interoperability features

Based on the analysis performed in Chapters 2 and 3, we can identify two types of potential for interoperability. Firstly, the potential for enabling interoperability when an RM analyst performs RM using the same RM framework but in systems that function for organisations in different sectors. Secondly, the potential for enabling interoperability when an RM analyst performs RM using different RM frameworks in systems either in the same or different sectors.
For both options, the key stakeholders and specialists noted that it is important to work in the future in the direction of creating guidelines for the interpretation and alignment of RM results, so that the various RM outputs can be compared with each other (i.e. from different RM methodologies or from the same RM methodology in different sectors). The components of the P6 Risk Analysis and Evaluation process, which draw attention for the above purposes are:
- the threat likelihood scale component
- the risk scale component
- the risk matrix component.

Based on the analysis performed in Chapters 2 and 3 and comments from key stakeholders, future work should focus on allowing interpretation of the outputs from risk analysis that result from different RMs so that risk levels are comparable. Such provisions can be very beneficial for organisations in Member States that aim to collaborate or exchange information and services. In such circumstances, auditors or security specialists are troubled when comparing various RM results and trying to evaluate whether risk levels are equivalent (e.g. a risk level 18 using ITSRM2 compared with a risk level 4 using TVRA).
Therefore, to achieve interoperability it is necessary to work towards the following.

- **Common or Comparative Risk Scales** that will be used by analysts to evaluate the risk scenarios produced by the risk identification process.
    - The risk scales could be qualitative or quantitative. However, there should be guidelines on the way analysts can interpret the results of each RM framework as a comparison to another RM framework
    - It would be useful to identify (if possible) reference values for each organisational size, sector, region or nation, etc.

4.6 PROCESS P7 RISK TREATMENT

4.6.1 Description of process

The objective of P7 Risk Treatment is the selection of the risk treatment options that are most appropriate for handling the risks identified taking into consideration the constraints on the organisation. Risk mitigation, avoidance, sharing or acceptance are considered as potential options for treatment. The process takes the results from the previous processes as input and the catalogue of security measures provided by the framework. The process results in a risk treatment register that gathers all the information related to the risk treatment options and applicable security measures if mitigation is chosen.

The process is mapped with the Risk Treatment step of ISO 27005.

4.6.2 Recommendations and integration of interoperability features

Achieving interoperability among different RM frameworks during the risk treatment process is important especially given that RM is a continuous and repetitive process. Therefore, it is common that organisations might perform RM using different methodologies in due course. Further, it is important because organisations may select collaborators based on their appetite for risk management and treatment as well as status, since collaboration commonly involves the exchange of information and the interconnection of systems. Therefore, organisations desire to be able to compare the results of risk treatment produced for the same system by two different RM frameworks or the results produced by different RM frameworks for different systems. For this, it is necessary to work towards the following objectives.

- **Baseline security measures and the levels of risk maturity** associated with various categories of risk and levels of risk maturity. Organisations could initially aim to achieve the minimum level of baseline security and further improve risk maturity by carrying out risk assessments and identifying further risks and appropriate controls.
- **Guidelines for comparing risk appetite**. Top management selects among the available risk treatment options, thus selecting risk mitigation, risk acceptance, risk avoidance or risk sharing. The decisions concerning risk treatment are related to the risk appetite of top management and could be a valuable criterion that organisations might use for selecting collaborators and developing service level agreements. Assuming there are comparative scales for risk, it would be useful to work towards guidelines for evaluating and comparing risk management appetites.

5. SYNOPSIS

The RM frameworks and methodologies presented in this report have undergone an in-depth analysis regarding certain attributes and characteristics which was essential in determining the corresponding levels of their potential interoperability. To this end, a scoring model was followed which produced the sought-after results. Each framework's features initially achieved an interoperability score, which in turn was used to evaluate the overall potential interoperability from the features' categories. Chapter 3 presents the interoperability features of the prominent RM methods and frameworks including the ones identified through the current work as well as updates to the ones identified in the previous version of the Report. (Chapter 6 includes a list of all RM frameworks and methods identified and updates made), while Chapter 4 presents recommendations for incorporating compatibility into the RM processes following ITSRM2.

Conclusively, there are a number of scenario-based methods that do not support all the characteristics that we used in our evaluation process, e.g. asset identification or evaluation, and therefore the overall score is not directly comparable to the scores of others.
It should also be noted that, due to the differing scopes and objectives of the RM frameworks and methodologies, a direct comparison of their score for potential interoperability might lead to erroneous conclusions. RM Frameworks (inc. ISO 27005, NIST SP 800 – 30/37/39) provide broad directions and guidelines and pose less constraints on the steps or processes to follow during RM. Well-structured methodologies, on the other hand (such as EBIOS RM, Magerit, and Monarc), prescribe in a higher level of detail the steps to be followed and support all phases of an RM process.
Finally, we should mention that RM frameworks, being essentially the guidelines for performing an assessment, can be integrated seamlessly with the processes derived from corresponding methodologies that have achieved the required evaluation of interoperability. For example, NIST 800-37 is a framework that only acts as an umbrella for risk management functional components and does not provide any details for each of them. As such, it has the capacity to accommodate any risk management functional component and, therefore, is highly interoperable but it cannot be used by its own as a methodology for managing levels of risk.

6. UPDATES ON THE PROMINENT RISK MANAGEMENT FRAMEWORKS AND METHODOLOGIES

This section describes the updates to the most prominent, currently in use RM frameworks and methods, as they have been identified in the report **Interoperable EU Risk Management Framework**.

6.1 MONARC

(https://www.monarc.lu/, Cyber Security Agency, Luxemburg)

MONARC (Méthode Optimisée d'analyse des risques CASES - Method for an Optimised Analysis of Risks by CASES) (CASES, 2013) is a tool and a method allowing precise and repeatable risk assessments to take place. It was created in 2013 by the Cyberworld Awareness Security Enhancement Services (CASES) department of the Cybersecurity Agency for the Luxembourg Economy and Municipalities in Luxembourg.

Since the publication of the report **Interoperable EU Risk Management Framework**, MONARC has incorporated an update of the risk treatment phase via the addition of security controls catalogue which are aligned with ISO/IEC 27002:2022 controls. This demonstrates the interoperability potential of MONARC, given that new features can be incorporated into specific RM stages. Moreover, in the previous version, the provided control catalogue is not obligatory, and it is possible to import referential catalogues from other sources (e.g., standards).

6.2 EU ITSRM², IT SECURITY RISK MANAGEMENT METHODOLOGY V1.2

(https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_en, EU, DG DIGIT)

The second version of ITSRM² IT Security Risk Management Methodology (2020, version 2.0) (European Commission Directorate-General for Communication, Security standards applying to all European Commission information systems) is a methodology provided by DG DIGIT and the European Commission, as part of a set of standards for information security which were updated in November 2021. The methodology comprises phases and steps that are mapped onto ISO 27005, including Context Establishment, Risk assessment and Risk Treatment. The main changes in the methodology include:

- flagging of personal data in the inventory of primary assets,
- asset valuation is extended to consider impact on data subject for personal data, and not only impact on business (i.e., Impact Scales were divided into Business Impact Scale and Data Protection Impact Scale)
- Measures catalogues included all measures from NIST SP800-53r4, but categorised as 1) Mitigating measures, 2) Supporting Measures, and 3) Corporate Measures.

6.3 THE AML/CFT NATIONAL RISK ASSESSMENT METHODOLOGY

(https://pubs.opengroup.org/security/o-ra/, The Open Group)

A new version of the methodology provided by the Open Group Standard for Risk Analysis (The Open Group, 2021) was published (version 2.0.1). The document is associated with the updated version of the Risk Taxonomy Standard (Risk Taxonomy (O-RT) Standard, Version 3.0.1, the Open Group Standard (C20B, November 2021)).

The main updates in the version 2.0.1 are:

- The "Confidence Level in the Most Likely Value" as a parameter to model estimates is discontinued and replaced by the choice of distribution that would determine it
- The quantitative example that utilized a qualitative scale has been removed
- Open FAIR terms and definitions have been clarified
- The Loss Scenario is decomposed and explained utilizing accompanying figures, including guidance on selecting the distribution to use and Risk Factor to model

6.4 THE AML/CFT NATIONAL RISK ASSESSMENT METHODOLOGY

(https://www.rahandusministeerium.ee/et/system/files_force/document_files/l2._nra_methodology_report.pdf?download=1, Ministry of Finance of the Republic of Estonia)

The AML/CFT methodology is developed by the Ministry of Finance of the Republic of Estonia. The purpose of this RM framework is to identify, assess and understand the risks, threats and vulnerabilities of money laundering and terrorist financing. Although, the specific threats are not necessarily cybersecurity risks, the methodology is strongly oriented towards the realization of the threats through the cyberspace and computer systems infrastructures.

The risk management process includes risk identification, risk analysis, risk evaluation & re-assessment. Risk identification includes among others, understanding the threats and vulnerabilities; risk analysis includes among others risk and vulnerability rating; and risk evaluation and re-assessment includes action planning and re-assessment of risks. The methodology provides an indicative taxonomy of threats and vulnerabilities, as well as rating guidelines related to a five-level scale for threat probability and vulnerability level and a five-level scaling for risk rating. For example a level 1 risk is associated with "insignificant impact on national security systems", a level 4 risk is associated with "high cybercrime attacks on computer infrastructure and databases, involving losses in confidential information", and a level 5 risk with "Significant cybercrime attacks on computer infrastructure and databases, involving disclosure of National Secrets (classified information), increased damage on national operation level on information, computer and telecommunication system". For the risk evaluation & re-assessment stage, three strategies are proposed for action planning: risk acceptance, risk avoidance and risk mitigation.

6.5 CIRCULAR CSSF 20/750

(https://www.cssf.lu/wp-content/uploads/cssf20_750eng.pdf, Commission de Surveillance du Secteur Financier (CSSF) of Luxemburg)

Circular CSSF 20/750 is developed by the Commission de Surveillance du Secteur Financier (CSSF) of Luxemburg and provides guidelines on information and computer technology (ICT) and security risk management, which are specifically targeted to the financial sector. The guidelines explain at high-level how financial institutions should manage the ICT and security risks that they are exposed to. The RM framework includes the following main steps:

- Organization and objectives

- Identification of functions, processes and assets
- Classification and risk assessment
- Risk mitigation
- Reporting
- Audit

The Guidelines state that the ICT and security risk management framework should include processes in place to:

- determine the risk appetite for ICT and security risks, in accordance with the risk appetite of the financial institution
- identify and assess the ICT and security risks to which a financial institution is exposed
- define mitigation measures, including controls, to mitigate ICT and security risks
- monitor the effectiveness of these measures as well as the number of reported incidents,
  including for PSPs the incidents reported in accordance with Article 96 of PSD2 affecting
- the ICT-related activities, and take action to correct the measures where necessary report to the management body on the ICT and security risks and controls
- identify and assess whether there are any ICT and security risks resulting from any major
- change in ICT system or ICT services, processes or procedures, and/or after any significant operational or security incident.

The Guidelines also define certain security areas that financial institutions should address with safeguards, including information security policy, logical security, physical security, ICT operations security, security monitoring, etc.

6.6 SERIMA

The Luxemburg Institute of Science and Technology developed a prototype and created a regulation platform called SERIMA (SEcurity RIsk Management), which allows telecommunication operators to carry out risk analyses, particularly in the telecommunications sector. This initiative is expected to assist operators in having a common methodology for carrying out risk analyses and report incidents according to the regulations in force. Therefore, tackling differences in format, methodology, data reconciliation or data comparison and analysis.

SERIMA is not analysed further in this report, due to lack of publicly available information.

6.7 ISO/IEC 27005:2018

(https://www.iso.org/standard/75281.html, International Organization for Standardization)

No updates.

6.8 NIST SP 800-37 REV. 2

(https://www.nist.gov/cyberframework/risk-management-framework, USA)

No updates.

6.9 NIST SP 800–30 REV.1

(https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final, USA)

No updates.

6.10 NIST SP 800–39

(https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final, USA)

No updates.

6.11 BSI STANDARD 200-2

(https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2002_en_pdf.html)

No updates.

6.12 OCTAVE-S

(https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6795, Carnegie Mellon University / Software Engineering Institute - USA)

No updates.

6.13 OCTAVE ALLEGRO

(https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419, Carnegie Mellon University / Software Engineering Institute - USA)

No updates.

6.14 OCTAVE FORTE (OCTAVE FOR THE ENTERPRISE)

(https://search.cmu.edu/?q=octave+fort&siteSearch=&site=&ie=UTF-8, Carnegie Mellon University / Software Engineering Institute - USA)

No updates.

6.15 ETSI TS 102 165-1, THREAT VULNERABILITY AND RISK ANALYSIS (TVRA)

(https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/05.02.03_60/ts_10216501v050203p.pdf, ETSI Technical Committee Cyber Security)

No updates.

6.16 EBIOS RISK MANAGER (EXPRESSION DES BESOINS ET IDENTIFICATION DES OBJECTIFS DE SECURITE - EXPRESSION OF NEEDS AND IDENTIFICATION OF SECURITY OBJECTIVES)

(https://www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method/, ANSSI, France)

No updates.

6.17 MAGERIT V.3: ANALYSIS AND RISK MANAGEMENT INFORMATION SYSTEMS

(https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en, Spanish Ministry for Public Administrations, Spain)

No updates.

6.18 MEHARI

(https://clusif.fr/management-des-risques-cooperation-de-mehari-et-ebios-risk-manager/ https://clusif.fr/module-mehari-manager-bc/, CLUSIF, France)

No updates.

6.19 GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

(https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/ANNEX%20Guidelines%20on%20Cyber%20Security%20Onboard%20Ships%20v.4.pdf, BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, OCIMF, IUMI and WORLD SHIPPING COUNCIL)

No updates.

7. BIBLIOGRAPHY/ REFERENCES

Higgins, J. and Thomas, J., *Cochrane Handbook for Systematic Reviews of Interventions*, 2021, Version 6.2.

Weidt, F. and Silva, R., *Systematic Literature Review in Computer Science-A Practical Guide*, Relatórios Técnicos do DCC/UFJF, vol. 1, no. 0, pp. 1–7, 2016, doi: 10.1027/1016-9040.11.3.244

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

Standard Computer Dictionary IEEE, A Compilation of IEEE Standard Computer Glossaries. IEEE, New York, NY, 1990 https://www.standardsuniversity.org/article/standards-glossary/#I
ISO 23903:2021 *Health informatics — Interoperability and integration reference architecture — Model and framework*

ISO/IEC 27000:2018 *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

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-europeancommission-information-systems_en

Lazarinis, F., Green, S., Pearson, E. (Eds.), (2011). *Handbook of Research on E-Learning Standards and Interoperability: Frameworks and Issues*. IGI Global. https://doi.org/10.4018/978-1-61692-789-9

Gilsinn, J. and Schierholz, R. (2010), *Security Assurance Levels: A Vector Approach to Describing* Security *Requirements*, Other, National Institute of Standards and Technology, Gaithersburg, MD, (accessed June 29, 2022)

ENISA (2016) *Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies*, https://www.enisa.europa.eu/publications/pets (accessed June 29, 2022)

ENISA (2021) *Interoperable EU Risk Management Framework*, https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework (accessed June 29, 2022

TP-01-22-004-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity 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 Union'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 978-92-9204-553-1
DOI: 10.2824/07253