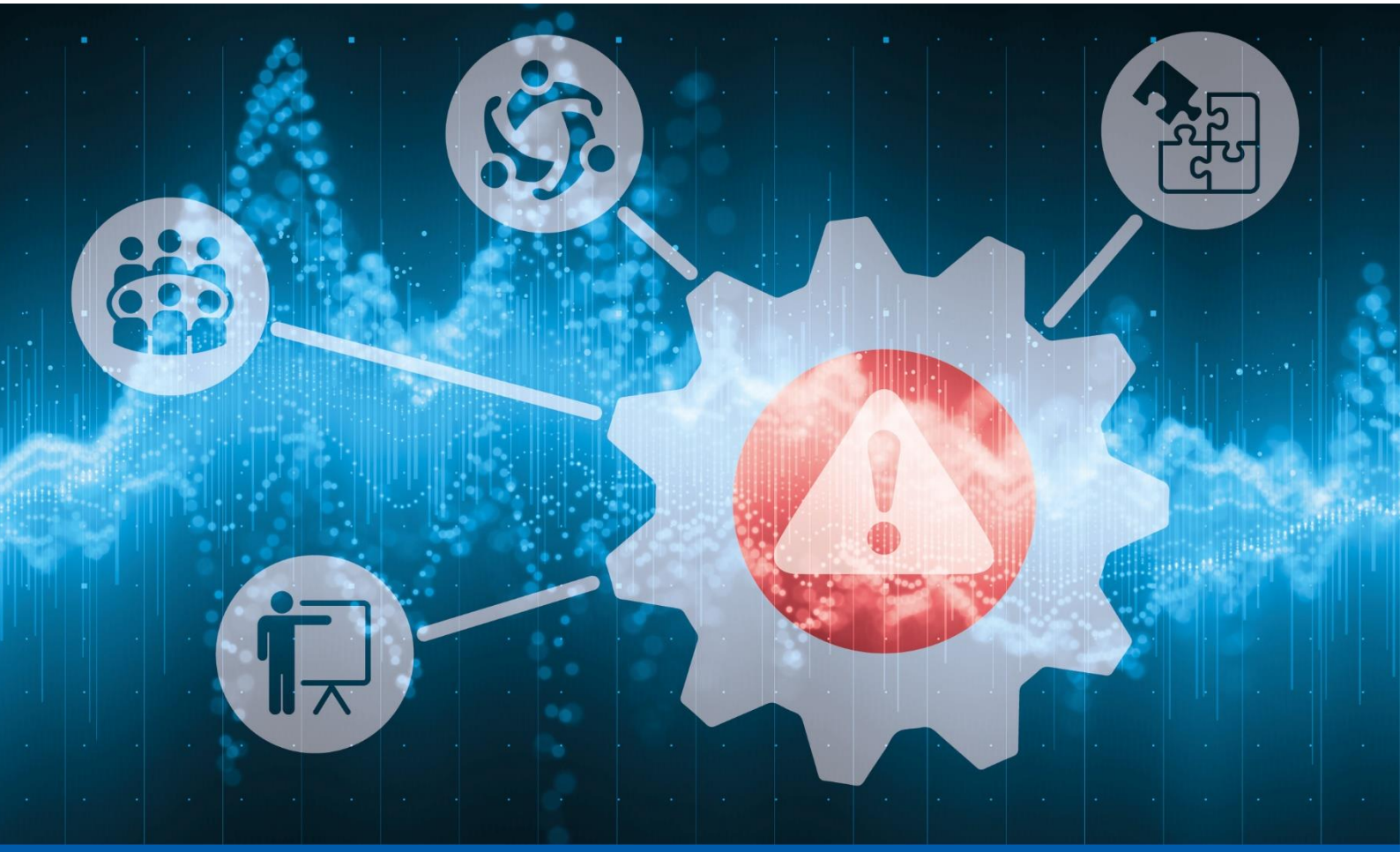
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



INTEROPERABLE EU RISK MANAGEMENT FRAMEWORK

Methodology for and assessment of interoperability among risk management frameworks and methodologies

JANUARY 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 proposes a methodology for assessing the potential interoperability of risk management (RM) frameworks and methodologies and presents related results. The methodology used to evaluate interoperability stemmed from extensive research of the literature, resulting in the use of certain RM framework features which were singled out for this purpose.

These features, which were identified as relevant for the assessment of interoperability, are thoroughly described and analysed for each framework/methodology. More specifically, for certain functional features we make use of a four-level scale to evaluate the interoperability level for each method and each set of combined features.

To evaluate interoperability among RM frameworks and methodologies, the inherent interoperability level of each framework is initially considered regarding its corresponding functional features. These features contribute to the interoperability of the identification, estimation and treatment of risk, and are further analysed to provide a thorough evaluation. The results are shown in detail through tables for all the frameworks or methodologies identified.

The information used to determine the levels of interoperability refers to whether a framework is asset-based or scenario-based, whether the approach followed is quantitative or qualitative, as well as the asset taxonomy and valuation methodologies, the cataloguing of threats and vulnerabilities, how the risk was calculated and how the corresponding calculations regarding measures and residual risks were undertaken. The potential for interoperability among the frameworks is summarised, providing an overview of possible collaborative combinations between them.

Finally, the report provides recommendations in the area of Interoperable EU Risk Management for ENISA to be considered for the Work Programme for 2022 and thereafter.

1. INTRODUCTION

1.1 PURPOSE AND SCOPE

This report presents a preliminary analysis of the prominent RM frameworks and methodologies described in the "Compendium of Risk Management Frameworks"[1], along with the appropriate method followed to determine their potential for interoperability. A detailed evaluation regarding the potential for interoperability of the RM frameworks, based on their features as identified and a defined evaluation model, are also included. The corresponding results are provided. These show the potential for forming a coherent RM framework through various possible combinations 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 such as the NIST RM framework. The definition of the methodology used to draw our conclusions was the result of meticulous research of the related literature provided by professionals involved in both the academic sector and organisations that engage in RM-related activities and research. The work carried out in the context of creating this document has resulted in the documentation of a detailed analysis of prominent RM frameworks and methodologies, based on their characteristics as identified, along with a defined method for the corresponding analysis of their potential for interoperability.

Furthermore, this report provides recommendations for the ENISA Work Programme for 2022 in the area of Risk Management (RM), including new and emerging trends in RM, best practices to address new types of cyberthreats and/or the vulnerabilities of systems. It also contributes to the field of special sectorial supports and highlights further possibilities for the support of cross-border and cross sectoral cooperation by organisations in different Member States (MS). The recommendations have been based on: (a) an analysis of the data national and sectorial RM frameworks have collected and the use of interoperability characteristics as a framework for the analysis; and (b) the comments, recommendations and insights provided by key stakeholders and other reviewers (Appendix).

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. METHODOLOGY

To identify the methodology needed to assess the interoperability of risk management frameworks and methodologies, we analysed the relevant literature to identify assessment models with similar characteristics. Relevant examples include an assessment of readiness regarding information technology and information assurance. Through a review of the literature, we identified assessment models. This indicates that one valid approach is to identify features that correspond to an assessed characteristic. Some assessment models also define levels to grade an overall characteristic or to grade each corresponding feature.

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 has to be 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

Functional 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 Evaluation	Does the framework or methodology use or describe specific guidelines for the evaluation 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?
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 of 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.

3. RESULTS

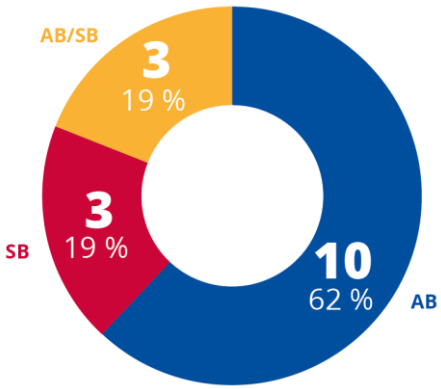
3.1 ANALYSIS OF LEVEL OF INTEROPERABILITY FOR EACH RISK MANAGEMENT FRAMEWORK AND FEATURE

The following table presents the application of the methodology for the evaluation of identified risk assessment frameworks and methodologies. Each framework or methodology is assessed regarding all features and the resulting scores. Justifications are given in the following figures.

Note that not all available risk management solutions are analysed in this chapter which instead focuses on well-established and recognised frameworks and methodologies that exhibit the characteristics of a risk management solution, and that have also been identified, after an initial screening, to have the potential to interoperate with other frameworks or methodologies.

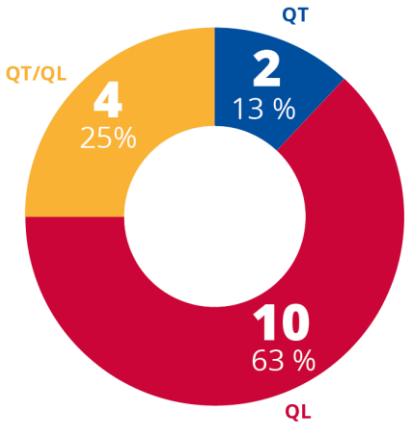
Thus, a total of 16 methodologies of various types were analysed. Ten of them are asset-based while three are considered as scenario-based, while the remaining three bear both asset-based and scenario-based characteristics.

Figure 1: Asset-based vs Scenario-based



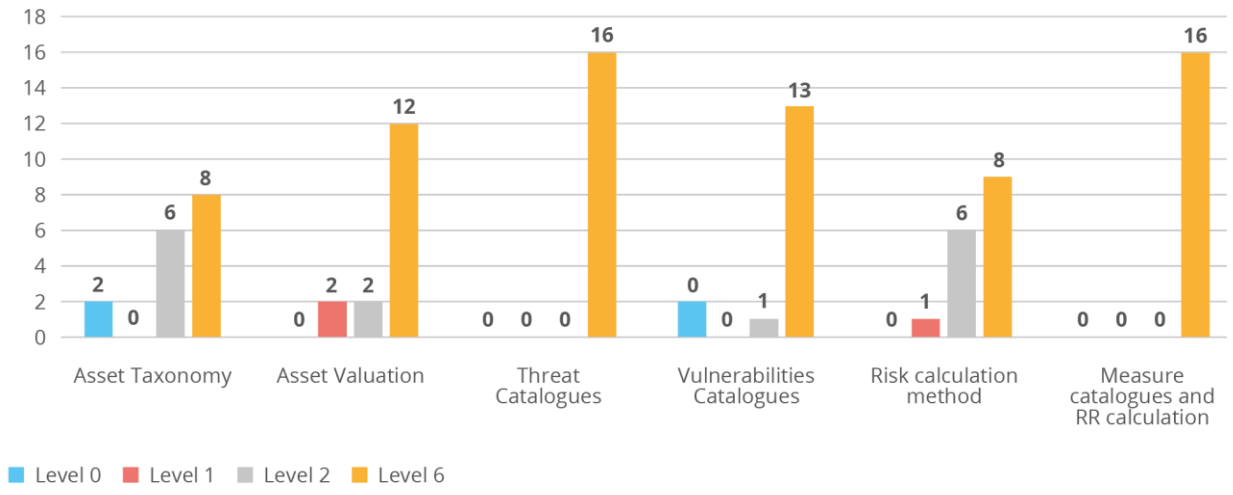
Similarly, the subset of methods of analyse included both quantitative (only 2 out of 16) and qualitative (10 out of 16) methodologies, while 4 of them have the characteristics of both categories.

Figure 2: Quantitative vs Qualitative



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, 9 of the 16 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 16 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



Frameworks and Methodologies	Generic Aspects		FUNCTIONAL						NON-FUNCTIONAL	
			Risk Identification				Risk Assessment	Risk Treatment		
	Asset based (AB)/ Scenario based (SB)	Quantitative (QT) / Qualitative approach (QL)	Asset Taxonomy	Asset valuation	Threat catalogues	Vulnerability catalogues	Risk Calculation method	Measure catalogues & Calculation of Residual Risk	Supported languages	Supports other risk-related frameworks
1.ISO/IEC 27005:2018	AB	QT, QL Both can be used to apply the methods described in the document	It supports two main categories: primary and supporting assets (ANNEX B); provides info on primary and supporting assets. New assets can be imported *Interoperability Level:2*	ANNEX B provides criteria and scale suggestions to evaluate assets but scale depends on organisation. New criteria can be imported. *Interoperability Level: 3*	ANNEX C provides examples of typical threats. New threats and threat categories can be added. *Interoperability Level: 3*	ANNEX D provides vulnerabilities and methods for vulnerability assessment. New vulnerabilities and vulnerability catalogues can be imported. *Interoperability Level: 3*	Matrix is used for risk calculation with modifiable scales. ANNEX E provides examples for risk assessment. Other calculation methods can be used. *Interoperability Level: 3*	Measure catalogues are not included. This standard relies on ISO 27002 or other methods to import measure catalogues. Flexibility in RR calculation. No specific one given. *Interoperability Level: 3*	EN, FR	Significant compatibility with other frameworks and standards.
2.NIST SP 800-37	AB	QL	No specific categories of assets provided. As a framework, it can accommodate any asset taxonomy. Extensive references to other NIST SPs, NIST CSF, frameworks such as COBIT as sources of techniques and catalogues. *Interoperability Level: 3*	No specific asset valuation criteria given. As a framework, it can accommodate any evaluation method. Extensive references to other NIST SPs, NIST CSF, frameworks such as COBIT as sources of techniques and catalogues. *Interoperability Level: 3*	No specific threat catalogue given. Extensive references to other NIST SPs, NIST CSF, frameworks such as COBIT as sources of techniques and catalogues. *Interoperability Level: 3*	No catalogue provided. Extensive references to other NIST SPs, NIST CSF, frameworks such as COBIT as sources of techniques and catalogues. *Interoperability Level: 3*	No catalogue provided. Extensive references to other NIST SPs, NIST CSF, frameworks such as COBIT as sources of techniques and catalogues. *Interoperability Level: 3*	No catalogue provided. Extensive references to other NIST SPs, NIST CSF, frameworks such as COBIT as sources of techniques and catalogues. RR calculation is flexible. *Interoperability Level: 3*	EN	As a generic method, it can accommodate any risk assessment method.

Frameworks and Methodologies	Generic Aspects		FUNCTIONAL						NON-FUNCTIONAL	
			Risk Identification				Risk Assessment	Risk Treatment		
	Asset based (AB)/ Scenario based (SB)	Quantitative (QT) / Qualitative approach (QL)	Asset Taxonomy	Asset valuation	Threat catalogues	Vulnerability catalogues	Risk Calculation method	Measure catalogues & Calculation of Residual Risk	Supported languages	Supports other risk-related frameworks
3.NIST SP 800-30	SB	QT, QL	No asset taxonomy provided. As a generic method it can accommodate any asset taxonomy. *Interoperability Level: 3*	Appendix H provides a series of tables for calculating adverse impacts. The criteria provided can be modified but new ones cannot be imported. *Interoperability Level: 3*	Specific modifiable threat catalogues provided. Appendix D provides a series of tables for identifying threat sources. New threat categories can be imported. *Interoperability Level: 3*	Appendix F provides a series of tables that can be used to identify vulnerabilities. The vulnerability catalogues provided can be modified and expanded with new vulnerabilities. *Interoperability Level: 3*	The risk is calculated as a combination of likelihood and impact. The risk calculation method can be modified. *Interoperability Level: 3*	No measure catalogue provided. Provides references to other sources implying the support of other catalogues. RR calculation is flexible. No calculation is provided. *Interoperability Level: 3*	EN	NIST RMF, ISO/IEC standards
4.NIST SP 800-39	AB	QL	NIST SP800-39 provides a structured, yet flexible approach for managing information security risk that is intentionally broad-based. New asset categories can be imported. *Interoperability Level: 3*	NIST SP800-39 provides a structured, yet flexible approach for managing information security risk that is intentionally broad-based. New asset valuation criteria can be imported. *Interoperability Level: 3*	No catalogues provided. New threat catalogues can be imported. *Interoperability Level: 3*	No catalogues provided. New vulnerability catalogues can be imported. *Interoperability level: 3*	NIST SP800-39 provides a structured, yet flexible approach for managing the risk to information security that is intentionally broad-based. New calculation methods can be imported. *Interoperability Level: 3*	No catalogues provided. Control categories are listed in Grundschutz Compendium. Calculation of residual risk is flexible. *Interoperability Level: 3*	EN	NIST RMF, ISO 27005

Frameworks and Methodologies	Generic Aspects		FUNCTIONAL						NON-FUNCTIONAL	
			Risk Identification				Risk Assessment	Risk Treatment		
	Asset based (AB)/ Scenario based (SB)	Quantitative (QT) / Qualitative approach (QL)	Asset Taxonomy	Asset valuation	Threat catalogues	Vulnerability catalogues	Risk Calculation method	Measure catalogues & Calculation of Residual Risk	Supported languages	Supports other risk-related frameworks
5. BSI STANDARD 200-2	AB/SB	QL	Assets are classified according to the IT-Grundschutz Compendium (2021). New assets can be imported according to IT-Grundschutz Compendium *Interoperability Level:3*	Assets are classified according to the IT-Grundschutz Compendium (2021). Non-modifiable scales (Low, Medium, High) for CIA properties. *Interoperability Level: 3*	Threats, modules and safeguards listed in the IT-Grundschutz Catalogues. New threats can be imported. *Interoperability Level:3*	Threats, modules and safeguards listed in the IT-Grundschutz Catalogues. New vulnerabilities can be imported. *Interoperability level:3*	Risks are only conceptually assessed taking into consideration existing safeguards and their reliability and effectiveness. Therefore, there is no specific scale for measuring risk. *Interoperability Level: 3*	Threats, modules and safeguards listed in the IT-Grundschutz Catalogues. New measure categories can be imported. RR calculation is flexible. It is eliminated by working out and implementing supplementary security measures to counteract a threat. *Interoperability Level: 3*	EN	ISO 27001
6.OCTAVE-S	AB/SB	QL	A default list of asset categories is provided, but a custom list can be added. Existing list can be modified. *Interoperability Level: 3*	Volume 1 provides worksheets and examples. The criteria can be modified to the organisation's needs with new impact areas able to be imported. *Interoperability Level: 3*	Under each threat profile, a custom list of threat categories can be added. Existing catalogues can be modified. *Interoperability Level: 3*	Protection Strategy worksheet provides expandable categories of potential vulnerabilities. (12. Vulnerability management). *Interoperability Level: 3*	Low to High risk based on high level criteria. Criteria can be modified. Addition of new ones is supported. *Interoperability Level: 3*	Protection Strategy worksheet provides expandable categories of potential safeguards. Impact evaluation criteria worksheet allows for additional impact types to be considered. No specific RR calculation formula. *Interoperability Level: 3*	EN	

Frameworks and Methodologies	Generic Aspects		FUNCTIONAL						NON-FUNCTIONAL	
			Risk Identification				Risk Assessment	Risk Treatment		
	Asset based (AB)/ Scenario based (SB)	Quantitative (QT) / Qualitative approach (QL)	Asset Taxonomy	Asset valuation	Threat catalogues	Vulnerability catalogues	Risk Calculation method	Measure catalogues & Calculation of Residual Risk	Supported languages	Supports other risk-related frameworks
7.OCTAVE ALLEGRO	AB	QL	The method focuses mainly on information assets. Other assets are linked to information assets via worksheets and are indirectly protected by measures aimed at protecting information assets. *Interoperability Level:3*	Provides expandable worksheets and examples but no specific scales, apart from low-medium-high on impact levels. No specific way to calculate importance of levels or assets. It depends on the organisation and the biases of the security team. *Interoperability Level: 3*	Provides worksheets and examples but no extensive catalogues. New threat catalogues can be imported. *Interoperability Level: 3*	Provides worksheets and examples but no extensive catalogues. New vulnerability catalogues can be imported. *Interoperability Level: 3*	Provides modifiable, expandable worksheets and examples that can be suited f use case *Interoperability Level: 3*	Provides worksheets and examples but no extensive catalogues. Example of RR calculation using risk scores suggested by the RMF. RR calculation is flexible since organisations can choose their own approach towards risk matrix and risk scores. *Interoperability Level: 3*	EN	HIPAA
8.OCTAVE FORTE	AB	QL	There are at least four primary categories into which assets can be classified (People, Information, Technology, Facilities). Each of these categories can be considered from an internal or external asset perspective. *Interoperability Level: 3*	Examples for identifying resilience requirements of assets are provided. CIA criteria is used for asset evaluation. New criteria can be imported. *Interoperability Level: 3*	No threat catalogues provided. Documents propose STRIDE, PASTA and hTMM as sources of extra catalogues. *Interoperability Level: 3*	No vulnerability catalogues provided. New vulnerability catalogues can be imported. *Interoperability Level: 3*	Risk is calculated in terms of impact and likelihood. As an alternative FAIR method is proposed. *Interoperability Level: 3*	No measures catalogue provided. Samples of risk appetite statements are provided. One of the samples focuses on categories (Revenue, Safety, etc) and the other on likelihood range. So, there is flexibility. *Interoperability Level: 3*	EN	COSO, ISO 31000, NIST CSF, NIST SP 800-39, NIST SP 800-37, CERT-RMM, FAIR

Frameworks and Methodologies	Generic Aspects		FUNCTIONAL						NON-FUNCTIONAL	
			Risk Identification				Risk Assessment	Risk Treatment		
	Asset based (AB)/ Scenario based (SB)	Quantitative (QT) / Qualitative approach (QL)	Asset Taxonomy	Asset valuation	Threat catalogues	Vulnerability catalogues	Risk Calculation method	Measure catalogues & Calculation of Residual Risk	Supported languages	Supports other risk-related frameworks
9.ETSI TS 102 165-1(TVRA)	AB	QL	Only conceptual with three high-level types of assets: physical assets, human assets, logical assets. The taxonomy provided can be modified. *Interoperability Level: 2*	High-level description (low - value 1, medium - value 2, high - value 3). New criteria can be imported. *Interoperability Level: 3*	Threats are linked to CIAAA (CIA+ Authenticity + Accountability). The following threat groups are provided: Interception (eavesdropping), Unauthorised access, Masquerade, Forgery, Loss or corruption of information, Repudiation and Denial of service. As long as new threat catalogues are mapped to CIIAA they can be imported. *Interoperability Level: 3*	No vulnerability catalogues provided. New ones can be imported. *Interoperability Level: 3*	Risk = Occurrence likelihood x Impact value. Likelihood levels result from vulnerability ratings and threat levels. Impact values result from 'asset impact' and 'attack intensity'. Three levels of risk: minor, major and critical risk. ANNEX G provides an Excel sheet to calculate risk and the calculation process is analysed in step 6 of the document. Some calculation parameters in step 6 can be ignored if organisation decides to. *Interoperability Level: 2*	No measure catalogues provided. New measures can be imported. RR calculation method is flexible. *Interoperability Level: 3*	EN	ISO 25408

Frameworks and Methodologies	Generic Aspects		FUNCTIONAL						NON-FUNCTIONAL	
			Risk Identification				Risk Assessment	Risk Treatment		
	Asset based (AB)/ Scenario based (SB)	Quantitative (QT) / Qualitative approach (QL)	Asset Taxonomy	Asset valuation	Threat catalogues	Vulnerability catalogues	Risk Calculation method	Measure catalogues & Calculation of Residual Risk	Supported languages	Supports other risk-related frameworks
10.MONARC	AB	QL	Monarch identifies primary and secondary assets. Assets are modifiable and expandable. *Interoperability Level: 3*	The value of the CIA criteria is automatically inferred based on the consequences of the ROLFP. Impact level ranges from 0, non-existing impact, to 4, unbearable information leaks, for each category. It is possible to customise valuation scales and redefine impact and consequences. *Interoperability Level: 3*	MONARC provides a pre-determined threat list that may be evaluated and modified. Existing list can be modified and expanded with new threats. *Interoperability Level: 3*	MONARC provides a pre-determined list of vulnerabilities that may be evaluated and modified. Existing list can be modified and expanded with new vulnerabilities. *Interoperability Level: 3*	The following formula is always used to calculate the level of risk: Threat x Vulnerability x Impact = Risk. Scales can be modified. *Interoperability Level: 3*	It does not provide a measures catalogue, but it can import references from standards like ISO 27005 to use them as safeguards. RR calculation is flexible. *Interoperability Level: 3*	EN, FR, NL, DE	ISO 31000, ISO 27005: 2013, ISO 27001, NIST SP 800
11.EBIOS Risk Manager (RM)	AB/SB	QL/QT	It supports 2 asset types: business (information & processes) and supporting assets (assets that support business assets). The value of impact is assessed according to a severity scale that makes it possible to rank feared events *Interoperability Level: 3*	Examples of assets and their impact levels for feared events. Criteria/scales are modifiable and expandable with new ones. *Interoperability Level: 3*	General examples. New ones can be added manually *Interoperability Level: 3*	No vulnerability catalogues are provided. New ones cannot be imported. Vulnerabilities are identified when assessing conformity to the security baseline that takes into account best practices and sectoral regulations. *Interoperability Level: 3*	No strict requirements on the levels of impact and likelihood parameters. A severity scale (G1-G4) is used. Other methods mentioned use scales with 4 or 5 levels. *Interoperability Level: 3*	No strict requirements on the parameters for levels of impact and likelihood. New measure catalogues can be imported. RR calculation is flexible. *Interoperability Level: 3*	FR, EN, SP, DE	ISO 31000:2018, ISO 27000, ISO 13335, ISO 27002, 27005

Frameworks and Methodologies	Generic Aspects		FUNCTIONAL						NON-FUNCTIONAL	
			Risk Identification				Risk Assessment	Risk Treatment		
	Asset based (AB)/ Scenario based (SB)	Quantitative (QT) / Qualitative approach (QL)	Asset Taxonomy	Asset valuation	Threat catalogues	Vulnerability catalogues	Risk Calculation method	Measure catalogues & Calculation of Residual Risk	Supported languages	Supports other risk-related frameworks
12. MAGERIT v.3	AB	QT/QL	Chapter 2 in Book 2 of Magerit provides a list of asset types. Each asset can be associated with more than 1 type. New assets can be imported. New asset types cannot be imported. *Interoperability Level: 3*	Chapter 4 of book 2 analyses the valuation criteria. The value for each dimension is 0, minimal, to 10, very high. Criteria can be modified. Both quantitative and qualitative methods are provided. New dimensions can be added. *Interoperability Level: 3*	Threats are included in chapter 5 of Book 2. New threat and threat catalogues can be imported. *Interoperability Level: 3*	Threats and vulnerabilities are included in chapter 5 of Book 2. There is no clear distinction in the catalogues. Vulnerabilities are not used anymore. They were used in Magerit v1.0) *Interoperability Level: 3*	Volume 3 of Magerit v3 includes techniques that can be used both in a qualitative and quantitative way through mathematical formulas to assess asset value, safeguard efficiency and risk management in general. Volume 3 includes all the methods mentioned for calculating risks so new ones cannot be imported. *Interoperability Level: 3*	Chapter 6 of Book 2 includes a list of suitable safeguards New safeguards can be imported. Impact and safeguard valuation is done via methods provided in Volume 3. Table or algorithmic analysis can be used. *Interoperability Level: 3*	SP/Partial EN	ISO/IEC 27001:2005, ISO/IEC 15408:2005, ISO/IEC 17799:2005, ISO/IEC 13335:2004

Frameworks and Methodologies	Generic Aspects		FUNCTIONAL						NON-FUNCTIONAL	
			Risk Identification				Risk Assessment	Risk Treatment		
	Asset based (AB)/ Scenario based (SB)	Quantitative (QT) / Qualitative approach (QL)	Asset Taxonomy	Asset valuation	Threat catalogues	Vulnerability catalogues	Risk Calculation method	Measure catalogues & Calculation of Residual Risk	Supported languages	Supports other risk-related frameworks
13.ITSRM²	AB	QT, QL	Primary, Secondary assets and Catalogue of Supporting assets. Existing catalogue is modifiable but new types cannot be added. *Interoperability Level: 2*	Recommends assessing value based on Business Impact Analysis, Proposes a scale 1-10. Different options are provided. Evaluation based on impact, or by hypothesis if something (like data) processed is not known in advance. *Interoperability Level: 3*	Catalogue from Magerit/Pilar. New threats and threat catalogues can be imported. *Interoperability Level: 3*	Vulnerabilities are only considered as an independent functional component and are not used elsewhere. *Interoperability Level: 3*	Risk = Threat x Consequence Threat involves assessment of frequency, power of adversary, easiness of infiltration. Risk matrixes can be customised, but formula remains the same. *Interoperability Level: 3*	Catalogue from NIST SP800-53r4. New safeguards and safeguards catalogues can be imported. Strict method for RR calculation so no flexibility. *Interoperability Level: 3*	EN	Magerit / PILAR / NIST SP800-53r4
14.MEHARI	AB/SB	QL	Primary (needs for activity), Secondary (media, dependencies). Provides asset catalogue. New assets and asset categories can be imported. *Interoperability Level: 3*	At least one of the consequence criteria should be defined for each asset (Confidentiality, Integrity, Availability). Impact and Intrinsic Impact *Interoperability Level: 3*	Mehari covers threat categories and types (App. C1), as well as actor classifications (App. C2). A list of event types is given along with their descriptions. New threats and threat categories can be imported. *Interoperability Level: 3*	Vulnerability catalogue provided in Appendix B. New vulnerabilities and vulnerability catalogues can be imported. *Interoperability Level: 3*	Risk is calculated by evaluating likelihood and impact on a scale from level 1 to level 4. It is mandatory that the efficiency of measures and the impact of threats be calculated. *Interoperability Level: 3*	There is a list of security services offered (Appendix G2). There are standard scales for impact, likelihood, reduction factors so RR calculation is not flexible. *Interoperability Level: 3*	FR, EN (Full set) SP, IT, DE, PL, RO, NL, PT (Overview) and others such as FA	ISO/IEC 27005:2011, ISO/IEC 27001:2013, ISO/IEC 27002:2013, ISO 31000

Frameworks and Methodologies	Generic Aspects		FUNCTIONAL						NON-FUNCTIONAL	
			Risk Identification				Risk Assessment	Risk Treatment		
	Asset based (AB)/ Scenario based (SB)	Quantitative (QT) / Qualitative approach (QL)	Asset Taxonomy	Asset valuation	Threat catalogues	Vulnerability catalogues	Risk Calculation method	Measure catalogues & Calculation of Residual Risk	Supported languages	Supports other risk-related frameworks
15.THE OPEN GROUP STANDARD, RISK ANALYSIS, V2.0	SB	QT	No asset taxonomy provided. *Interoperability Level: 3*	No asset valuation provided. New criteria can be imported. *Interoperability Level: 3*	No threat catalogues provided. Only generic categories. New threat catalogues can be imported. *Interoperability Level: 3*	No vulnerability catalogues provided. Only generic categories. New vulnerability catalogues can be imported. *Interoperability Level: 3*	Monte Carlo or other stochastic methods to calculate results. New risk calculation methods can be imported. *Interoperability Level: 3*	No safeguard catalogues provided. Only generic categories. RR calculation is flexible. *Interoperability Level: 3*	EN	ISO 27005
16.GUIDELINES ON CYBER SECURITY ONBOARD SHIPS	AB/SB	QT	Annex 1 provides a list of onboard systems, equipment and technologies with potential vulnerabilities. New asset categories can be imported. *Interoperability Level: 3*	It includes both the asset's total cost and the cost of maintaining it. Provides modifiable and expandable criteria. *Interoperability Level: 3*	Threat is the product of the threat actor's capability, opportunity and intent to cause harm. New threat catalogues can be imported. *Interoperability Level: 3*	Examples of potentially vulnerable onboard systems are provided. New vulnerability catalogues can be imported. *Interoperability Level: 3*	Risk is calculated by evaluating likelihood and impact. Criteria can be modified. *Interoperability Level: 3*	Sections 7 and 8 provide protection and detection measures. New safeguards can be imported. RR calculation is flexible. *Interoperability Level: 3*	EN	

3.2 ANALYSIS OF POTENTIAL INTEROPERABILITY OF RISK MANAGEMENT FRAMEWORKS

Having listed the interoperability features of each framework, together with the scoring of the respective levels of interoperability, we evaluated the potential interoperability as described in the methodology. We have summarised the results in the table below.

Table 3: Potential interoperability

Overall Evaluation of Frameworks and Methodologies / Interoperability Feature	Risk Identification				Residual Risk Calculation		Overall Potential Interoperability[2]
					Risk Assessment	Risk Treatment	
	Asset Taxonomy	Asset valuation	Threat catalogues	Vulnerability catalogues	Risk Calculation method	Measure catalogues & Calculation of Residual Risk	
1.ISO/IEC 27005:2018	Potential Interoperability: 2.7				Potential Interoperability: 3	Potential Interoperability: 3	**2,90**
2.NIST SP 800-37	Potential Interoperability: 3				Potential Interoperability: 3	Potential Interoperability: 3	**3,00**
3.NIST SP 800-30	Potential Interoperability: 1.6				Potential Interoperability: 2	Potential Interoperability: 3	**2,20**
4.NIST SP 800-39	Potential Interoperability: 2				Potential Interoperability: 3	Potential Interoperability: 3	**2,67**
5. BSI STANDARD 200-2	Potential Interoperability: 2				Potential Interoperability: 3	Potential Interoperability: 3	**2,67**
6.OCTAVE-S	Potential Interoperability: 3				Potential Interoperability: 3	Potential Interoperability: 3	**3,00**
7.OCTAVE ALLEGRO	Potential Interoperability: 3				Potential Interoperability: 3	Potential Interoperability: 3	**3,00**
8.OCTAVE FORTE	Potential Interoperability: 2,7				Potential Interoperability: 3	Potential Interoperability: 3	**2,90**
9.ETSI TS 102 165-1 (TVRA)	Potential Interoperability: 2,7				Potential Interoperability: 2	Potential Interoperability: 3	**2,57**
10.MONARC	Potential Interoperability: 2,7				Potential Interoperability: 3	Potential Interoperability: 3	**2,90**

[2] It is important to stress that most Scenario Based (SB) methods do not support the full set of functional characteristics evaluated (e.g. asset identification/evaluation), and thus the 'Overall Interoperability Potential' is not directly comparable to the non-SB methods.

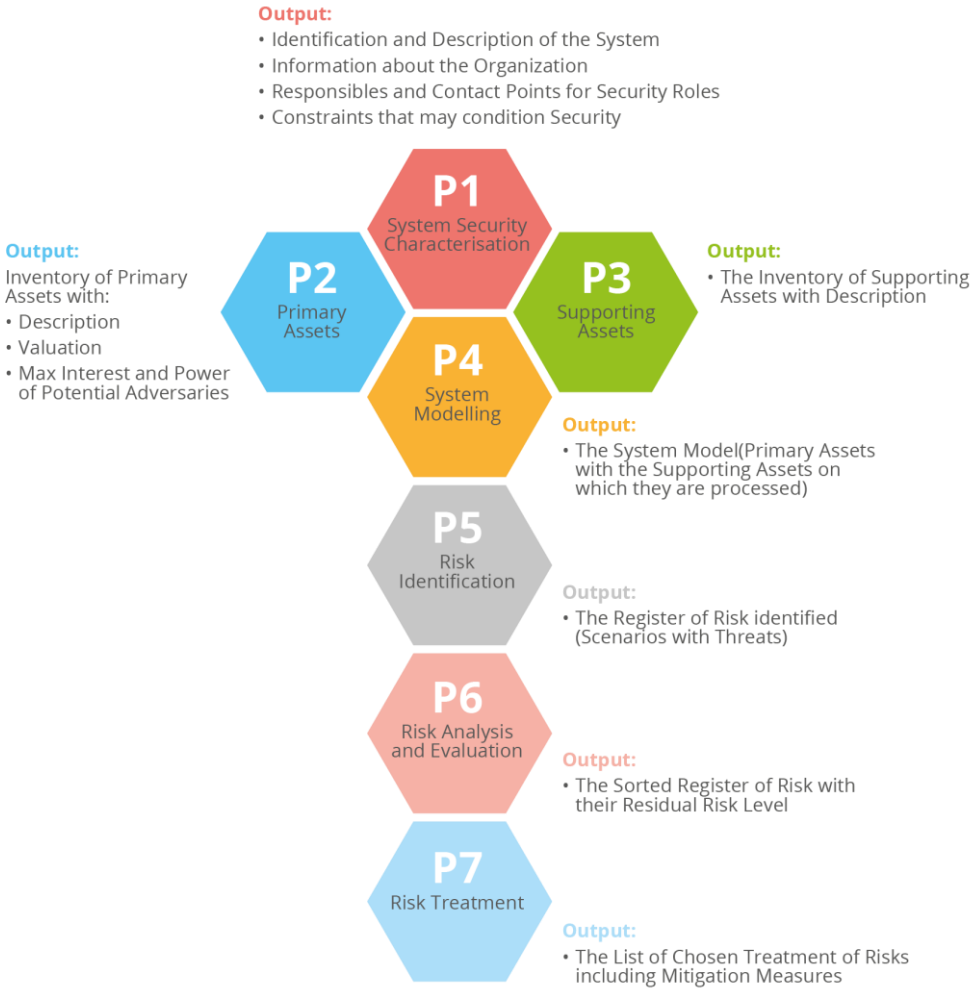
Overall Evaluation of Frameworks and Methodologies / Interoperability Feature	Risk Identification				Residual Risk Calculation		Overall Potential Interoperability[2]
					Risk Assessment	Risk Treatment	
	Asset Taxonomy	Asset valuation	Threat catalogues	Vulnerability catalogues	Risk Calculation method	Measure catalogues & Calculation of Residual Risk	
11.EBIOS RM	Potential Interoperability: 2,9				Potential Interoperability: 2	Potential Interoperability: 3	**2,63**
12.MAGERIT v.3	Potential Interoperability: 2,4				Potential Interoperability: 2	Potential Interoperability: 3	**2,47**
13.ITSRM[2]	Potential Interoperability: 1,9				Potential Interoperability: 2	Potential Interoperability: 3	**2,30**
14.MEHARI	Potential Interoperability: 2				Potential Interoperability: 1	Potential Interoperability: 3	**2,00**
15.THE OPEN GROUP STANDARD, RISK ANALYSIS, V2.0	Potential Interoperability: 2.1				Potential Interoperability: 3	Potential Interoperability: 3	**2,70**
16.GUIDELINES ON CYBER SECURITY ONBOARD SHIPS	Potential Interoperability: 3				Potential Interoperability: 2	Potential Interoperability: 3	**2,67**

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 ITSRM2.

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



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

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 ITSRM[2].

4.1 PROCESS P1 SYSTEM SECURITY CHARACTERISATION

4.1.1 Description of process

The purpose of the System Security Characterisation process is to gather initial information concerning the system and its context, which will be used for the rest of the RM processes. The output of this process includes a high-level description of the system and the organisation, the contact points for security roles, any constraints for security requirements and any mandatory security measures that result from these requirements. This process is mapped with the ISO 27005 step Context Establishment.

For the purposes of identifying interoperability opportunities and features, this process is considered outside the scope of our analysis, as described in accompanying "Compendium of Risk Management Frameworks"[4].

4.2 PROCESSES P2 PRIMARY ASSETS AND P3 SUPPORTING ASSETS

4.2.1 Description of processes

The objective of the P2 Primary Assets process is to identify the Data and Functions (considered as Primary Assets) that are crucial for the organisation to achieve its business objectives, determine their *value* (from a business perspective) as well as their attractiveness for potential adversaries (combination of the *power* and *interest* of potential adversaries that can be motivated by threatening the Primary Asset). For this process the methodology offers a business impact scale, a catalogue of potential adversaries and a scale of levels of interest for potential adversaries.

Finally, the objective of P3 Supporting Assets is to identify and register the Supporting Assets employed (inventory of hardware and software, a high-level design, an architectural diagram etc.) for the management of the primary assets (Data and Functions provided by the target system).

This process is part of the Risk Identification step of ISO 27005.

4.2.2 Recommendations and integration of interoperability features

To achieve interoperability among different RM frameworks, we need to enable the use of each other's asset taxonomy and valuation algorithm with equivalent results and without negatively affecting subsequent steps. Therefore, we need to ensure that:

- the asset taxonomy used by an RM framework is modifiable;
- the analyst can introduce new categories of assets or import taxonomies from other sources;

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

- the RM framework uses or describes specific guidelines for the evaluation of assets (i.e. scale and criteria for assessment of asset value and impact) which are modifiable or the analyst can introduce new scales or criteria.

4.3 PROCESS P4 SYSTEM MODELLING

4.3.1 Description of process

The purpose of P4 System Modelling is to develop a model of a system in terms of associations between primary and supporting assets, data flows, and system architecture.

This process is part of the Risk Identification step of ISO 27005.

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 ITSRM[2] 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. A combination of the frameworks and methodologies studied is achievable, as depicted by the tables in Chapter 3.

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.

Based on the results of the aforementioned analysis and on the comments, recommendations, and insights provided by key stakeholders and other reviewers (see Appendix), Chapter 4 provides recommendations for interoperable EU Risk Management that ENISA could consider for the 2022 Work Programme.

6. BIBLIOGRAPHY

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-european-commission-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, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906330 (Accessed August 5, 2021)

ENISA (2016) *Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies*, https://www.enisa.europa.eu/publications/pets (Accessed August 5, 2021)

7. APPENDIX – INTERVIEWS WITH NLOS

The risk management methods analysed and the assessment of their potential interoperability were shared with ENISA's National Liaison Officers from various Member States to receive their comments, suggestions and recommendations. Interviews were conducted using a semi-structured questionnaire and synchronous online sessions that allowed the engaged parties to share their views and directly discuss their concerns on the initial results.

The main outcomes of this engagement are provided in the following sections.

7.1 EVALUATING POTENTIAL INTEROPERABILITY

The methodology that was developed and applied for evaluating the potential interoperability of Risk Management (RM) frameworks and methodologies based on the identification of their functional and non-functional features was reviewed by the participants, who highlighted the following issues.

- When considering the functional features, it is not the existence of catalogues that should be considered, but guidelines in the main. Likewise, it is not the threats, but how to identify threats.
- Scenario Based frameworks are more appropriate for the definition of strategy while Asset Based are more appropriate for low level analysis (e.g. system assessment). The evaluation of interoperability might include a combination of both since an organisation might have to implement both approaches. Asset-based and scenario-based are not mutually exclusive. Other approaches also exist, such as event-based or based on conformity.
- It is important for the RM methodologies to be able to 'translate' IT-level RM results into management-level results. As such, it would be great to include the feature 'to report to management', as management dashboarding is a key feature of a risk management framework or tool to support funding and management sponsoring and feedback. Therefore, the RM framework output or report should be quantified, measurable or tangible.
- A functional feature that depicts the specific sector where each specific RM framework is designed to be applied could also be considered.
- The objective of interoperability is the joined understanding of risk levels.
- It is important to consider how each RM methodology can assist compliance with regulatory frameworks (e.g. GDPR, NIS).
- Different standards and tools use different language – a cross-table of definitions might prove helpful (terms, definitions and semantics interoperability). To this end, it is important to define interoperable definitions of terms in EU RM frameworks, and regulatory frameworks (e.g. the definition of 'incident' in Risk Management frameworks versus the definition in regulations, such as NIS)
- The four interoperability levels for each functional feature (i.e. low, medium, high, non-applicable), were considered appropriate and clear.
- Versioning should also be added as a feature as some RM methodologies have frequent updates.
- The use of templates helps compare the results of RM methodologies. Templates facilitate more standardised implementations – can also help share knowledge – make the community more interactive – facilitate interoperability not only between companies

but also between departments. These basic default setups help stakeholders to start their implementations and facilitate reusability. As such, importing and exporting templates is an important feature.

- One important feature to consider would be the maturity level required to start applying the framework or methodology. 'Can you start with low maturity' or 'how quickly can you get started' are some questions that might need to be answered.
- It is important to consider if different RM frameworks are designed to cover sector-specific requirements (e.g. financial sector, essential services operator).
- It is important to consider the landscape of tools covering specific frameworks. For example, how many tools are supporting each RM framework?

7.2 SUGGESTIONS FOR AN INTEROPERABLE EU RM FRAMEWORK

Another set of questions targeted an identified set of functional and non-functional features that can be used for developing the proposed interoperable risk management framework. The NLOs' concerns on the topic are summarised next.

Activities or processes that could enable synergies among risk management methodologies and available resources could focus on the following issues.

- The methodologies must use a standardised risk reporting format (e.g. the same ratios and scales), otherwise it would be extremely difficult to compare the results.
- Regarding threat catalogues and taxonomies, some methodologies use high level (e.g. espionage) while others go into much more detail. To compare the frameworks there should be a taxonomy that examines the threats in an equal level of detail, because a threat or vulnerability catalogue is open to interpretation.
- A specific methodology for Supply Chain or SLA management might be very useful.
- Publishing or exporting a Top X (top 3 , top 5, or top 10) of risks that companies face (anonymised, or statistical reports without detail).
- Comparing the security exposure (sectoral benchmarking) to other types of companies or organisations in the same NIS sector, or size of company, or even region to be distributed across Europe and even beyond that, would also help a lot.

Among the features that an EU wide Interoperable Risk Management Framework should have are the following.

- Use of common terminology, with the same interpretations of terms. ISO 27005 terminology could be used for this purpose.
- Common, at EU-level, threat catalogues as well as sector-specific vulnerability catalogues.
- A risk assessment scale could facilitate comparison of results, especially for each sector, although difficult to enforce.
- Adoption of baseline controls that could be applied to the different categories of risk maturity so that all organisations could have a minimum level of security. Subsequently they could carry out risk assessment to identify further risks and appropriate controls.
- A high-level framework in combination with any detailed risk assessment framework.
- Integrate an organisation's risk management with its IT risk management. The organisations' objective is to provide services or products. This should be somehow related to its IT risk management.

Some efforts towards interoperable RM frameworks are ongoing. These include the connection of EBIOS with Magerit, or that of BSI and Estonian approaches which tie together business risk scenarios related to information security and asset-based risk management using the results of scenario-based assessments (only six scenarios to assess).

Another national authority is also trying to create best practices where, for each phase, they are trying to identify some minimum steps and persuade organisations to use them. They encourage organisations to use the proposed evaluation method and get some data that will be comparable, but this is just in the beginning. The same approach was also stressed by another NLO who recognised the need to adopt ISO13335 RM methods: detailed RM, baseline RM and a combination of them.

Baseline security is a growing trend – some security steps are optimised for typical assets and security measures are implemented without thinking about vulnerabilities or threats. For the parts of the organisation which are not so typical or where the security requirements are higher (CIA context), detailed risk management is conducted. The importance of templates and how these can contribute to the successful deployment of RM methodologies across sectors has also been highlighted.

Another national authority developed a Risk Assessment framework based on the location of each organisation by considering physical risks (e.g. nuclear radiation is a threat that cannot be removed from the threat catalogue for entities located close to a nuclear facility). Furthermore, the probability of occurrence is pre-defined for certain threats, based on quantitative data collected on previous incidents at regional or national level.

With regards to the synergies that could come about by enabling interoperability among risk management activities with an EU wide risk management framework, the participants stressed that if the EU came up with its own framework then it would be easier for a national authority to get its clients to look at the issue holistically and use all the elements of risk identification, as opposed to focusing only on parts of the issue (e.g. vulnerabilities).

For several organisations risk management now is more of a compliance exercise rather than a way to control risks and, therefore, their approach is fragmented. Moreover, use of a common framework can contribute towards assessing service level agreements between organisations (vendors, suppliers, clients, etc.), comparing certifications for different standards and using a common threat catalogue. Interoperability can also facilitate better interpretation of results, knowledge sharing and allow analysts to have reference values of companies of the same size, sector, or region.

7.3 NEXT STEPS TOWARDS AN INTEROPERABLE FRAMEWORK

Participants were also asked to identify the synergies among existing frameworks already used or developed by EU member states and to contribute to the next steps that should be taken to facilitate the uptake and use of the proposed framework. The comments or information received on this, are summarised below.

Participants claimed that they are already running an interoperable framework, such as:

- EBIOS risk manager, which is considered interoperable and can integrate parts from other methodologies, including the connection between management and the technical level;
- Monarc, which has some dashboarding features, supports template sharing, common configuration setups or even entire completed analyses for reuse between departments or even different enterprises;
- Estonia's upcoming framework, which is compliant with ISO 27001 and the revised NIS Directive;
- ILR, the NIS regulator, conducted the implementation of Serima, which supports the Risk Management framework, with LIST.lu (Luxembourg Institute of Science and Technology).

Regarding the next steps that participants consider important for the use of the proposed methodology, and the need for an automated tool to facilitate the adoption of an EU RM framework, they noted the following.

- Use cases with the three approaches, QT, QL and conformity, are needed.
- The introduction of new concepts in ISO 27005, regarding interoperability should be considered.
- The interoperability concept and guidelines for interoperability among QT and QL approaches should be introduced.
- It would be great to have a methodology backed up by an interoperable framework so that reports can be exchanged easily, that would be highly visible so work can be re-used, and would have results that could be interpreted by others.
- A shared import/export protocol or a share integration or interface would be great. If a common framework or common assets would be pluggable to existing tools, that would be nice.
- A tool would be useful if it supports both detailed and management level RM. A tool focusing only on IT risk assessment will not be useful. If a risk management tool were integrated into workflow management then organisations would probably use it. If it has one interoperability module then maybe somebody would use it also but first we need to define the root need – why we need it, who will use it, when and how often?

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