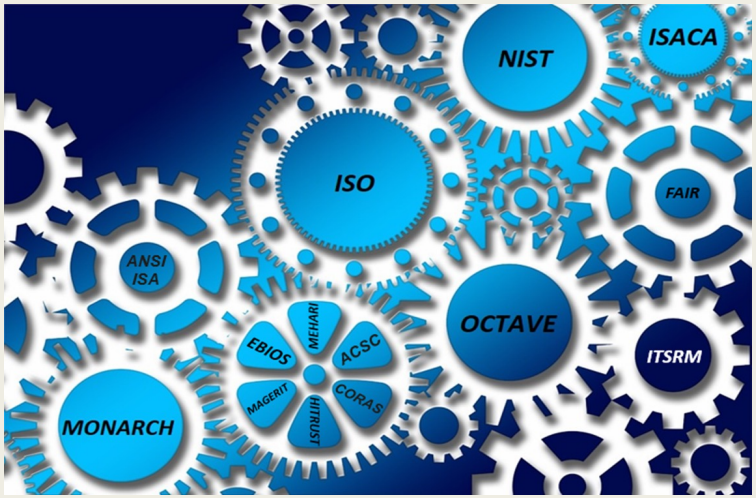
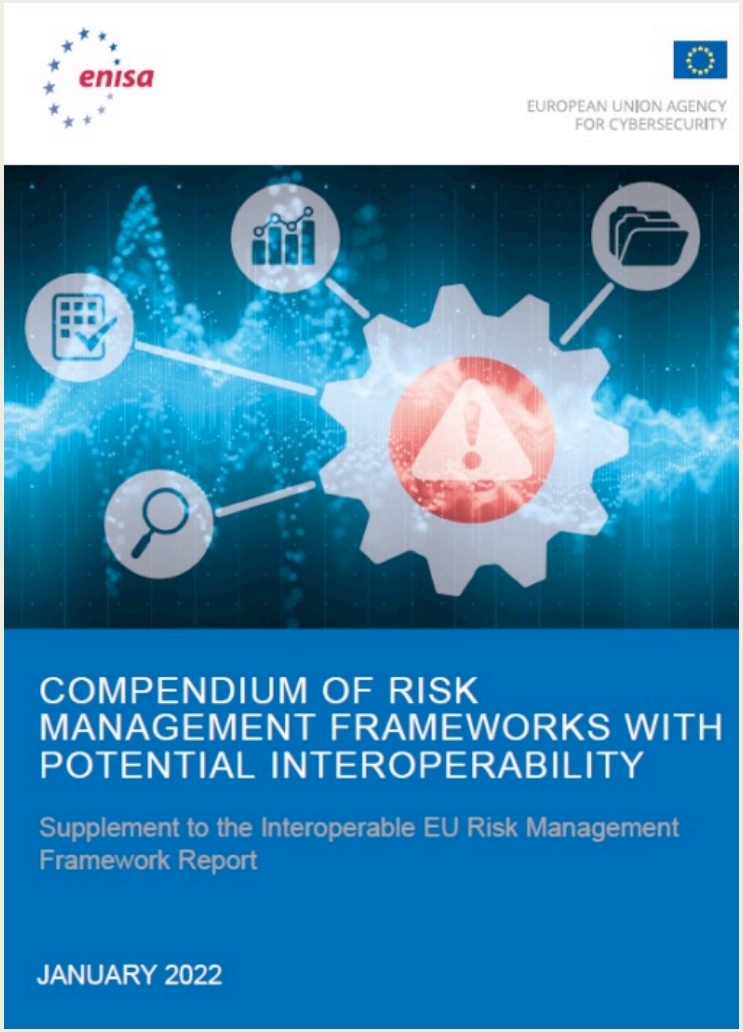
D-CBU-21-T25 / INTEROPERABLE EU RISK MANAGEMENT FRAMEWORK

PROJECT PRESENTATION




enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
INTEROPERABLE EU RISK MANAGEMENT FRAMEWORK
Methodology for and assessment of interoperability among risk management frameworks and methodologies
JANUARY 2022


enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
COMPENDIUM OF RISK MANAGEMENT FRAMEWORKS WITH POTENTIAL INTEROPERABILITY
Supplement to the Interoperable EU Risk Management Framework Report
JANUARY 2022

Agenda

- Project Objectives
- Project's Methodology
- Results
- Findings
- Next Steps
- Lessons Learnt
- Follow up project

Objectives

- Update ENISA's database regarding existing Risk Management frameworks/methodologies.
- Identify Risk Management frameworks/methodologies with interoperability potential.
- Engage key stakeholders in validating the proposed framework.
- Propose recommendations on possible follow-up work to the direction of an EU wide Interoperable Risk Management Framework with consistent methodology and risk assessment practices among Member States.

Methodology (1/2)

- **Draft a list of existing RM frameworks/methodologies and identify prominent ones with interoperable features**
  - ***identify relevant fully developed*** *RM frameworks/methodologies and components of RM frameworks/methodologies (both national and sectorial);*
  - ***identify their characteristics / features*** *(indicatively: national/international scope of the framework/methodology; the target sector(s); the size of the target audience; its maturity; compliance with relevant standards; compatibility with EU regulation and legislation (e.g. NIS Directive, GDPR); availability of software support; openness; cost of acquisition; extent of use; open data sources; ability for dynamic risk assessment etc)*
  - ***develop a methodology*** *for* ***assessing the interoperability potential*** *of the identified RM frameworks/methodologies, based on a set of interoperability factors (i.e. risk identification, risk assessment, risk treatment)*
  - ***apply the methodology*** *for identifying the prominent RM frameworks/methodologies with interoperability potential*
- **Propose the new ENISA Inventory of RM Frameworks/Methodologies**

Methodology (2/2)

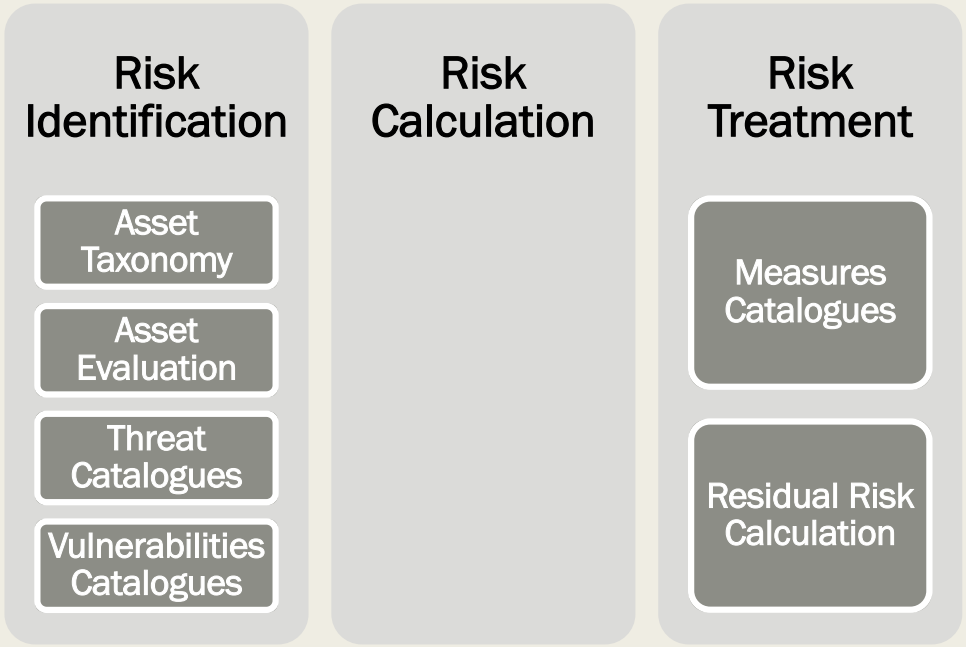
- Analyse the identified RM frameworks/methodologies with interoperability features with respect to their potential to form a coherent European RM framework
- Involve key stakeholders, including subject matter experts, and ENISA National Liaison Officers from EU MS and ENISA.
- Utilize stakeholders' comments and recommendations, to provide recommendations for the ENISA work program for 2022 and after, aiming
  - *to an EU wide Interoperable Risk Management Framework with consistent methodology and risk assessment practices among Member States*
  - *to identify new and emerging trends in RM,*
  - *to identify best practices to address new types of cyberthreats and/or vulnerabilities of systems, especially in the context of critical infrastructures support and*
  - *to identify further possibilities to support the cross-border and cross sectoral cooperation of organizations in different MS (e.g. by supporting knowledge sharing to collectively mitigate cyberthreats)*

New/Up-to-date ENISA Inventory of RM Frameworks / Methodologies

1. ISO/IEC 27005:2018
2. NIST SP 800-37, REVISION 2ORGANISATION
3. NIST SP 800 – 30 REV.1
4. NIST SP 800 – 39 REV.1
5. NIST SP 800 – 82 REV. 2
6. BSI STANDARD 200-2
7. OCTAVE-S
8. OCTAVE ALLEGRO
9. OCTAVE FORTE (OCTAVE FOR THE ENTERPRISE)
10. ISACA RISK IT FRAMEWORK, 2ND EDITION
11. INFORMATION RISK ASSESSMENT METHODOLOGY 2 (IRAM2)
12. ETSI TS 102 165-1, THREAT VULNERABILITY AND RISK ANALYSIS (TVRA)
13. MONARC
14. EBIOS RISK MANAGER (EXPRESSION DES BESOINS ET IDENTIFICATION DES OBJECTIFS DE SÉCURITÉ - EXPRESSION OF NEEDS AND IDENTIFICATION OF SECURITY OBJECTIVES)
15. MAGERIT V.3: ANALYSIS AND RISK MANAGEMENT INFORMATION SYSTEMS
16. EU ITSRM, IT SECURITY RISK MANAGEMENT METHODOLOGY V1.2
17. MEHARI
18. ENTERPRISE RISK MANAGEMENT – INTEGRATED FRAMEWORK
19. AUSTRALIAN ACSC SECURITY MANUAL
1. ANSI/ISA-62443-3-2-2020, Security for industrial automation and control systems
16. THE OPEN GROUP STANDARD, RISK ANALYSIS (O-RA), VERSION 2.0
17. CORAS
18. IS RISK ANALYSIS BASED ON A BUSINESS MODEL
19. IMO MSC-FAL.1/CIRC.3 GUIDELINES ON MARITIME CYBER RISK MANAGEMENT
20. GUIDELINES ON CYBER SECURITY ONBOARD SHIPS
21. HITRUST
22. ISRAM - INFORMATION SECURITY RISK ANALYSIS METHOD
23. FAIR - FACTOR ANALYSIS OF INFORMATION RISK
24. GUIDE TO CONDUCTING CYBERSECURITY RISK ASSESSMENT FOR CRITICAL INFORMATION INFRASTRUCTURE
25. RISK MANAGEMENT TOOLS (Risk Management Studio, SimpleRisk, Verinice, Practical Threat Analysis - PTA , vsRisk,

RM Components

- *A risk management framework 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*** *(Security controls selection and implementation, and residual risk calculation),*
  - ***Risk Monitoring*** *(Assess measures effectiveness and monitor risks) --- although essential for efficient risk management, it is independent to the rest of the phases and can be typically conducted using any assessment methodology, process, or tool; as such, it is considered to be out of this project's scope*



INTEROPERABILITY

- *“the ability of a risk management component or methods to reuse information provided by risk management components or methods of other frameworks with equal ease and with the same interfaces, towards the same goals”*

INTEROPERABILITY CRITERIA (1/4)

- *Functional Components – Interoperability Criteria*
  - *Generic aspects:*
    - *Asset based and/or Scenario based*
    - *Quantitative and/or Qualitative*
  - ***Risk Identification:*** *risk management frameworks/methodologies 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*
    - *Asset Valuation*
    - *Threats catalogues*
    - *Vulnerabilities catalogues*

INTEROPERABILITY CRITERIA (2/4)

- ***Functional Components – Interoperability Criteria***

  - ***Risk Assessment:*** *risk management frameworks/methodologies are considered interoperable if they use the same Risk Assessment methodology, or their corresponding methods can provide results that can be easily mapped to the other's results. At this level we consider the following features:*
    - *Risk Calculation method*
  - ***Risk Treatment:*** *risk management frameworks/methodologies are considered interoperable if they result in the same set of measures or a set of measures with equal contribution in risk levels reduction. At this level we consider the following features:*
    - *Measures catalogue*
    - *Residual Risk Calculation*

INTEROPERABILITY CRITERIA (3/4)

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

INTEROPERABILITY CRITERIA (4/4)

Generic Aspects		FUNCTIONAL						NON-FUNCTIONAL	
		Risk Identification				Risk Assessment	Risk Treatment		
Asset based (AB)/ Scenario based (SB)	Quantitative (QT) / Qualitative (QL)	Asset Taxonomy	Asset valuation	Threats catalogues	Vulnerabilities catalogues	Risk Calculation method	Measures catalogue & Residual Risk Calculation	Supported languages	Supports other risk-related frameworks

INTEROPERABILITY LEVEL EVALUATION MODEL (1/2)

- ***Indicative*** parameters that are evaluated per functional characteristic of the risk management framework/methodology ……

Functional Characteristics	Parameters to Check
Asset Taxonomy	Does the framework/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/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/criteria modifiable?
	Can the analyst introduce new scales/criteria?
Threat Catalogues	Does the framework/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 from other sources?

INTEROPERABILITY LEVEL EVALUATION MODEL (2/2)

- To reflect the **inherent interoperability level of the RM framework/methodology,** per functional feature (risk identification, calculation and treatment), a four-level scale was used:

Non Applicable:	The framework/methodology does not use or support this feature.
Low Interoperability Level:	The framework/methodology requires a proprietary solution for this feature, provided by the framework itself
Medium interoperability Level:	The framework/methodology supports this feature/provides guidelines but not compulsory, the proposed solution is modifiable.
High interoperability Level	The framework/methodology uses this feature, but it either does not provide any guidelines, or it can adopt similar features by other frameworks/methodologies, e.g., standardised, or a proprietary solution.

Prominent RM frameworks/methodologies with interoperability potential

1. ISO/IEC 27005:2018
2. NIST SP 800-37, REVISION 2ORGANISATION
3. NIST SP 800 – 30 REV.1
4. NIST SP 800 – 39 REV.1
5. BSI STANDARD 200-2
6. OCTAVE-S
7. OCTAVE ALLEGRO
8. OCTAVE FORTE (OCTAVE FOR THE ENTERPRISE)
9. ETSI TS 102 165-1, THREAT VULNERABILITY AND RISK ANALYSIS (TVRA)
10. MONARC
11. EBIOS RISK MANAGER (EXPRESSION DES BESOINS ET IDENTIFICATION DES OBJECTIFS DE SÉCURITÉ - EXPRESSION OF NEEDS AND IDENTIFICATION OF SECURITY OBJECTIVES)
12. MAGERIT V.3: ANALYSIS AND RISK MANAGEMENT INFORMATION SYSTEMS
13. EU ITSRM, IT SECURITY RISK MANAGEMENT METHODOLOGY V1.2
14. MEHARI
15. THE OPEN GROUP STANDARD, RISK ANALYSIS (O-RA), VERSION 2.0
16. GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

NLOs' views on interoperability potential

- The objective of interoperability is the joined understanding of risk levels
- The four interoperability levels per functional feature (i.e., low, medium, high, non-applicable), were considered appropriate and clear
- Asset-based and scenario-based methodologies are not mutually exclusive – the interoperability evaluation tem from the application of RM framework on different sectors.
- RM methodologies should be able to "translate" IT-level RM results into management-level results
  - *RM output/report should be quantified, measurable or tangible*
- Interoperable definitions of terms in EU RM frameworks and regulatory frameworks
- Use of templates facilitate more standardised implementations - help share knowledge - make the community more interactive.

NLOs' views on Interoperable RM Framework (1/2)

- Adoption of baseline controls – facilitates achieving a minimum level of security.
  - *Subsequent risk assessment to identify further risks and appropriate controls is possible.*
- Use a standardised risk reporting format
  - *same rations and scales*
- Use threat taxonomies that look the threats in equal level of detail
  - *Common at EU level – sector-specific*
- Consider Supply chain /SLA management
- Facilitate comparison of the security exposure (sectoral benchmarking) to other type of companies or organisations in the same NIS sector, or size of company, or even region to distribute across Europe
- Use of common terminology
  - *same rations and scales*

NLOs views – Interoperable RM Frameworks (2/2)

- EBIOS Risk Manager: is considered interoperable and can integrate parts from other methodologies, including the connection between management and technical level.
- Monarc: is considered interoperable, includes dashboarding features, supports template sharing, common configuration setups, or even entire completed analyses for reuse between departments or even different enterprises.

Lessons learned

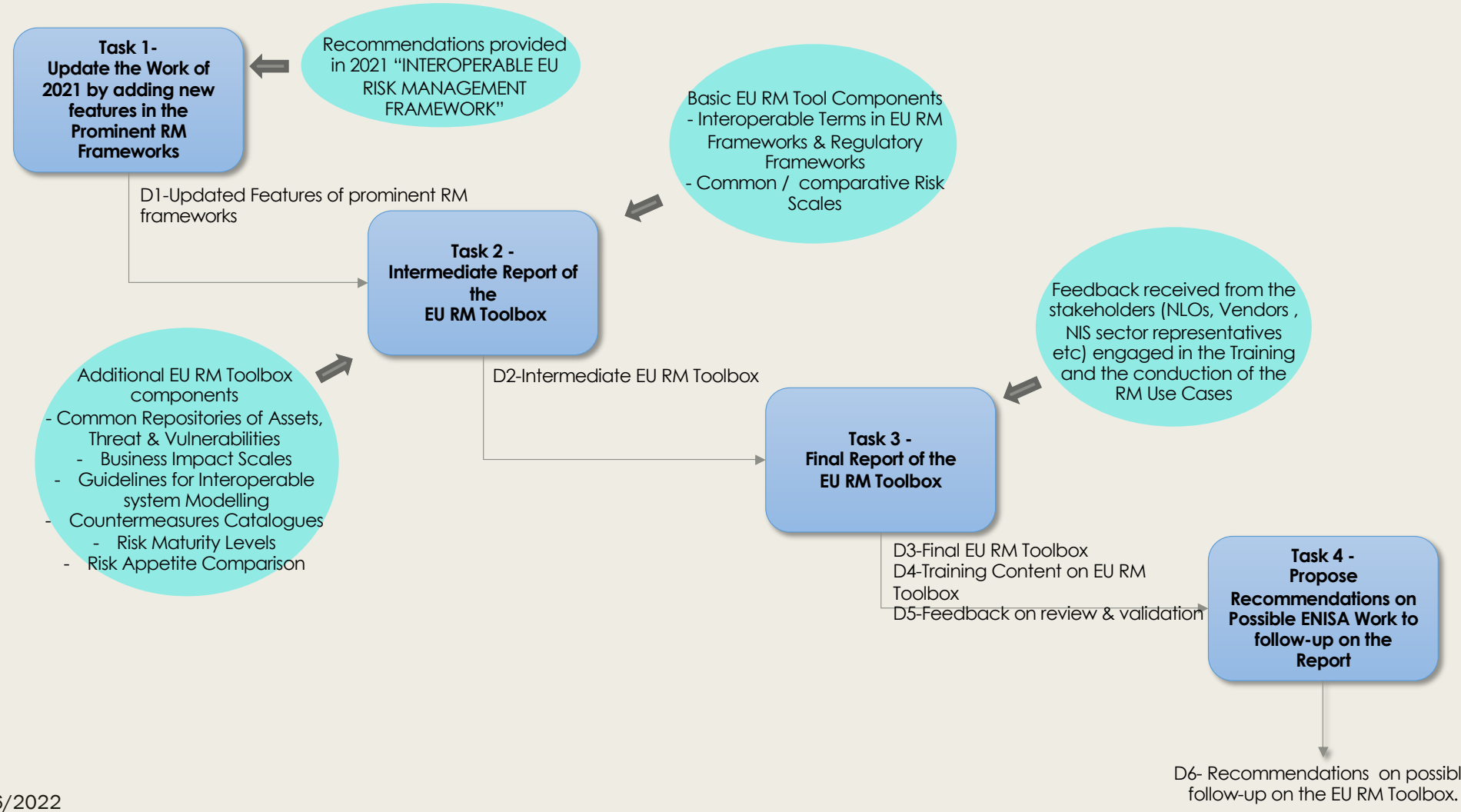
- Evaluation Methodology –
  - *a number of scenario-based methods do not support all the characteristics, e.g. asset identification/evaluation*
  - *overall score is not directly comparable to the others' scores.*
- Different scope and objectives of the RM frameworks - direct comparison of their interoperability score/potential 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/processes to follow during RM.
- Well – structured methodologies (e.g. EBIOS RM, Magerit, and Monarc) prescribe in a higher level of detail the steps to be followed and support all phases of a RM process.

Next steps

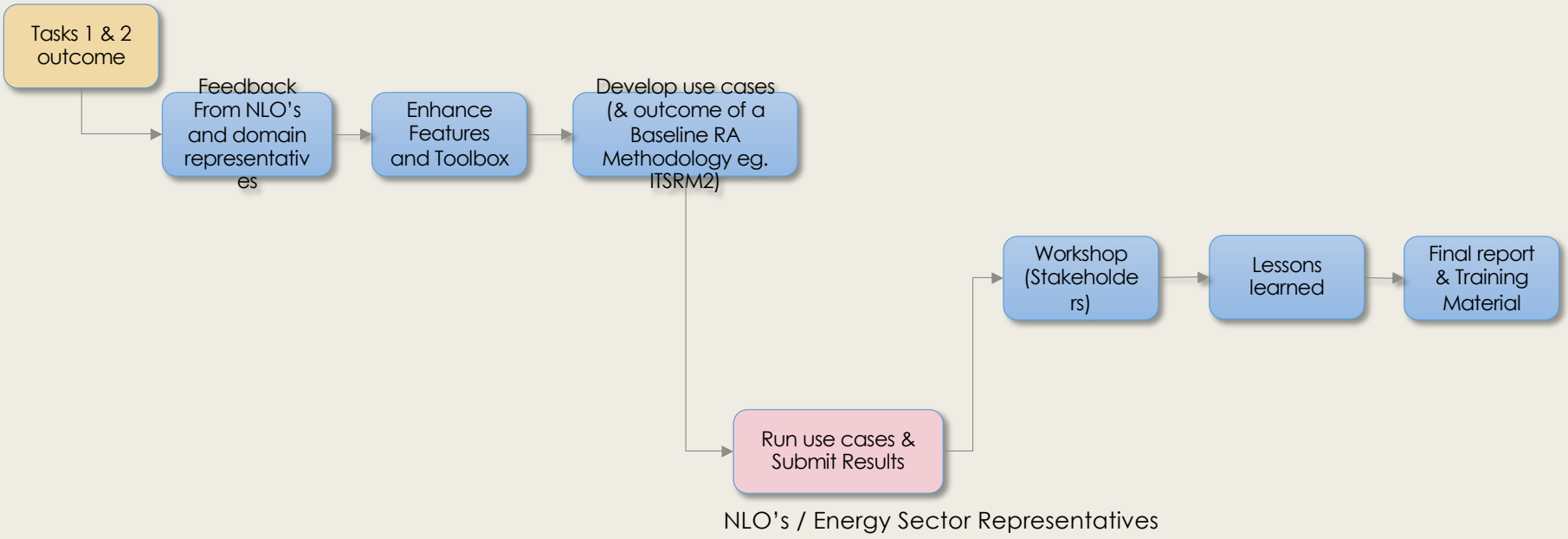
- Introduce the interoperability concept and guidelines for interoperability among QT and QL approaches
  - *Develop use cases with the three approaches: QT, QL and conformity.*
- The introduction of new concepts in ISO 27005, regarding interoperability should be considered.
- Develop a methodology backed up by an interoperable framework so that
  - *reports can be easily exchanged,*
  - *it is highly possible to re-use data, analysis and evaluations,*
  - *results are interpretable by others.*
- A shared import/export protocol or a share integration or interface.
- A common framework or common assets pluggable to existing tools.
- A tool that supports both detailed and management level RM.

Recommendations for developing an ineroperable RM framework

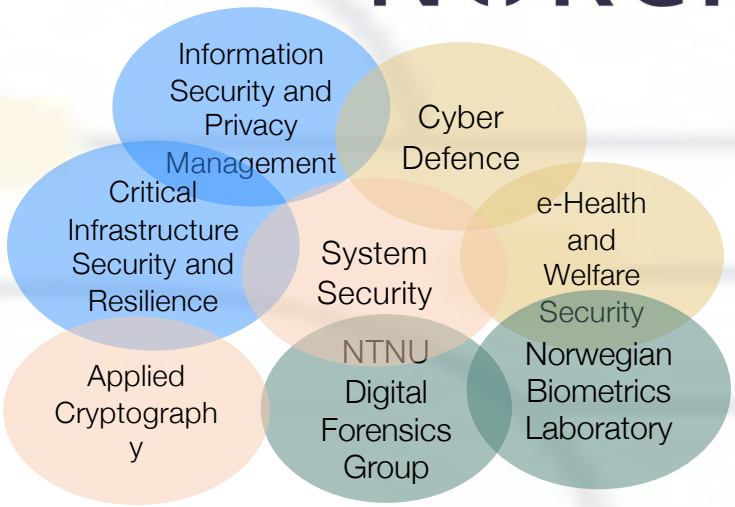
- ITSRM2 can be used as a reference framework for the RM framework, adopting the following points:
  - Employs a modifiable asset taxonomy, provides specific guidelines for the evaluation of assets and allows the introduction of new scales/criteria.
  - **standard representation techniques** for modeling the system facilitate interoperablity
  - Develop **Common Threat Repositories**
  - Develop **Common Vulnerability repositories**
  - Develop **Common/Comparative Risk Scales**
  - Develop **Baseline security measures and Risk maturity levels** associated with the different categories of risk and levels of risk maturity
  - Provide **Guidelines for comparing risk appetite**


Task 1- Update the Work of 2021 by adding new features in the Prominent RM Frameworks
Recommendations provided in 2021 "INTEROPERABLE EU RISK MANAGEMENT FRAMEWORK"
D1-Updated Features of prominent RM frameworks
Basic EU RM Tool Components
- Interoperable Terms in EU RM Frameworks & Regulatory Frameworks
- Common / comparative Risk Scales
Task 2 - Intermediate Report of the EU RM Toolbox
Additional EU RM Toolbox components
- Common Repositories of Assets, Threat & Vulnerabilities
- Business Impact Scales
- Guidelines for Interoperable system Modelling
- Countermeasures Catalogues
- Risk Maturity Levels
- Risk Appetite Comparison
D2-Intermediate EU RM Toolbox
Feedback received from the stakeholders (NLOs, Vendors , NIS sector representatives etc) engaged in the Training and the conduction of the RM Use Cases
Task 3 - Final Report of the EU RM Toolbox
D3-Final EU RM Toolbox
D4-Training Content on EU RM Toolbox
D5-Feedback on review & validation
Task 4 - Propose Recommendations on Possible ENISA Work to follow-up on the Report
D6- Recommendations on possible follow-up on the EU RM Toolbox.

09/06/2022


Tasks 1 & 2 outcome
Feedback From NLO's and domain representativ es
Enhance Features and Toolbox
Develop use cases (& outcome of a Baseline RA Methodology eg. ITSRM2)
Workshop (Stakeholde rs)
Lessons learned
Final report & Training Material
Run use cases & Submit Results
NLO's / Energy Sector Representatives

Norwegian Centre for Cybersecurity in Critical Sectors - NORCICS



SIEMENS

HELGELAND KRAFT

YARA

Lyse

POLITIET OSLO POLITIDISTRIKT

NTNU

equinor

Elvia

NorSIS Norsk senter for informasjonssikring

mnemonic Securing your business.

Michigan Tech

UF IoT

UNIVERSITY of GUELPH

POLYTECHNIQUE MONTRÉAL UNIVERSITÉ D'INGÉNIERIE

UiA Universitetet i Agder

Sykehuset Innlandet HF

TUHH Technische Universität Hamburg

Technical University of Munich

TELECOM SudParis

IP PARIS

ma

NYU ABU DHABI

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

UNIVERSITÄT PASSAU

DTU Technical University of Denmark

Hydro

NC-SPECTRUM

SINTEF

NR Norsk Regnesentral NORWEGIAN COMPUTING CENTER

KONGSBERG

THANK YOU!