EUROPEAN UNION AGENCY
FOR CYBERSECURITY

COMPENDIUM OF RISK MANAGEMENT FRAMEWORKS WITH POTENTIAL INTEROPERABILITY

Supplement to the Interoperable EU Risk Management Framework Report

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 978-92-9204-554-8 DOI:10.2824/75906 Catalogue number: TP-01-22-005-EN-N

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report presents the results of desktop research and the analysis of currently used cybersecurity Risk Management (RM) frameworks and methodologies with the potential for interoperability. The identification of the most prominent RM frameworks and methodologies was based on a systematic survey of related risk management approaches adopted in different contexts (including industry, business, government, academia, etc), at national, international and sectoral levels.

This collection of identified frameworks and methodologies includes well known and widely used RM standards that provide high level guidelines for risk management processes that can be applied in all types of organisations (e.g. ISO 27005; NIST SP 800-37, SP 800-30 & SP 800-39; BSI 100-3; OCTAVE S, Allegro & FORTE, Open FAIR etc.); frameworks applied in specific regions (e.g. COSO Enterprise Risk Management, the Australian ACSC Security Manual); frameworks applied in specific sectors (e.g. IMO MSC, Guidelines on Cyber Security Onboard Ships); industry-oriented standards (e.g. NIST 800-82, ANSI/ISA-62443-3-2-2020); and more structured methodologies that follow specific phases or steps to implement RM processes (e.g. ETSI TVRA, MONARC, MAGERIT, EBIOS, EU ITSRM, CORAS etc.)

This report also describes the main characteristics and features of each one of the RM frameworks and methodologies identified. Based on this analysis, a basic set of interoperability features is derived. These comprise features such as components of the risk management process (e.g. Risk Identification, Risk Assessment, Risk Treatment and Risk Monitoring); type of approach to risk identification (asset-based or scenario-based); type of approach to risk assessment (quantitative or qualitative); method of risk calculation; and others.

1. INTRODUCTION

1.1 PURPOSE AND SCOPE

This report has as main purpose to presents the results of a systematic search and analysis of currently used cybersecurity risk management (RM) frameworks and methodologies, at national, international and sectoral level. It complements the report "Compendium of Risk Management Frameworks"[1] and provides further analysis of the prominent risk management frameworks and methodologies with potential interoperability. Report "Compendium of Risk Management Frameworks" includes the basic features and characteristics of all RM frameworks and methodologies identified.

The collection of RM frameworks and methodologies which are described in this report is based on an extensive analysis of all appropriate sources, including repositories of relevant resources provided by organisations such as ENISA, NIST, ISACA, ISF etc; commercial and business sites and magazines; European Commission sites; and academic literature.

The frameworks and methodologies identified have been considered with regard to their main characteristics and in particular with those features that would enable them to interoperate or to be combined in the context of an interoperable EU RM framework.

1.2 REPORT STRUCTURE

This report includes four sections: **Section 1** defines its purpose and scope; **Section 2** presents the method followed to identify relevant RM frameworks and methodologies; **Section 3** describes the main characteristics of each identified framework or methodology; and **Section 4** proposes the main interoperability characteristics that can support an interoperable EU RM framework. This last section also summarises our conclusions.

[1] https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework

2. METHOD OF WORK

2.1 BASIC CONCEPTS AND TERMS

Information security risk management, henceforth risk management (RM), refers to coordinated activities to direct and control an organisation with regards to risks to the security of its information, according to the International Organization for Standardization (2018).

Information security risk management comprises a process to establish the external and internal context, assess the risks and treat the risks, using a risk treatment plan to implement decisions on how to manage the risk. Risk management examines what may happen and the possible consequences before deciding what should be done, and when, to reduce the risk to an acceptable level.

To compile a comprehensive list of approaches to the management of information risks, we considered both frameworks and methodologies. Risk management methodologies provide systematic guidance on how to identify, analyse, assess and manage risk, while risk management frameworks define a structure upon which organisations can build all processes related to identifying, analysing, assessing, and managing information security risks. Thus, risk management methodologies allow for the systematic identification, analysis, assessment and management of risk. They are typically concise and offer to solve a specific problem. Methodologies are less flexible than frameworks, due to their specificity.

Risk management frameworks offer a more generic approach, allowing diverse risk management processes to be included or combined within their context, so that they can be customized to the risk management needs of the specific organisational context. Typically, frameworks offer the foundation to further build a set of processes on and categorise risks by classifying them according to specific taxonomies. For the management of risk, frameworks may provide options for managing risks (modify, retain, avoid, share).

This report provides a comprehensive analysis of prominent risk management frameworks and methodologies that are currently in use, including high-level risk management frameworks and more structured risk management methodologies, in terms of their potential interoperability, so that all levels of abstraction are covered.

2.2 SURVEY METHODOLOGY

The identification of the most prominent RM frameworks and methodologies described in this report was done by means of a systematic survey of risk management approaches followed in different contexts (industrial, business, government, academic etc). This section presents the methodology which was followed to conduct the tabletop research that led to the identification of the risk management frameworks and methodologies (which have been included in D1) and the selection of the most prominent ones, according to their potential interoperability.

The systematic survey was performed following the guidelines in (Higgins, et al., 2019) and in (Weidt & Silva, 2016). The first stage was to determine the scope of the research and the criteria for inclusion and exclusion. The objective of the survey was to identify risk frameworks and methodologies that provide guidance for the assessment of information security risk or for the assessment and treatment of information security risk. The inclusion criteria were as follows:

- risk management frameworks and methodologies used as best practice in the industry, regardless of their scope, type and size of organisation, target audience, etc;

- risk management frameworks and methodologies proposed as standards and guidelines by international and national standardisation bodies;
- risk management methodologies and methods proposed by academia.

We excluded risk management frameworks and methodologies that were obsolete (i.e. those that had not been supported for more than ten years) and that did not support the fundamental risk management processes (i.e. those that provide guidance only for risk treatment, etc.). Further, we excluded risk management frameworks and methodologies that were proposed in academic sources but did not provide specific guidance for their implementation. Thus, the survey aimed to identify the state-of-the-art risk management frameworks and methodologies, rather than to provide an exhaustive list of all risk management frameworks and methodologies.

At the second stage, the team identified possible sources to search, including relevant resource repositories (e.g. the ENISA; NIST; BSI; CDCDOE; SANS; ISACA; ISF; European Commission portal; etc.); commercial and business sites and magazines; and academic literature. Significant sources were the existing Inventory of Risk Management / Risk Assessment Methods and Tools published by ENISA, as well as the project team members, who acted as information specialists (Higgins, et al., 2019), as they all have working experience in information security risk management in several risk management projects across Europe and internationally.

Each member of the project team conducted an independent search and reported the results, which were then synthesised and reviewed by all members of the team, i.e. a peer review (Higgins, et al., 2019). Several iterations of searching and reviewing were performed, and the elaboration was considered complete when all key frameworks and methodologies were included in the repository. Some of the frameworks that were originally included were eventually excluded because they were either outdated or they did not offer adequate guidance on the assessment and management of risk (i.e. they are high-level descriptions).

The description of the frameworks and methodologies as identified, which is presented in the next section, includes several features that support the purpose of this task and the upcoming tasks and deliverables, including the full name, vendor and origin of the frameworks and methodologies; their geographical scope of use (e.g. used in EU countries, USA, etc.); whether they support generic or sectorial risk management needs; whether they are freely available or not; whether they are supported by an automated tool or other material; supported languages etc.

At the final stage, drawing on the analysis of the risk management frameworks and methodologies, the project team initially identified a set of features that support their potential for interoperability. These features were further analysed as criteria for interoperability and the results of these analyses are documented in an upcoming report.

3. PROMINENT RISK MANAGEMENT FRAMEWORKS AND METHODOLOGIES

This section describes the most prominent risk management frameworks and methodologies that are currently in use as identified by the survey.

3.1 ISO/IEC 27005:2018

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

ISO/IEC 27005:2018 'Information technology — Security techniques — Information security risk management' is a risk management framework applicable to all types of organisations (e.g. commercial enterprises, government agencies, non-profit organisations) which intend to manage risks that could compromise the organisation's information security. It supports the general concepts specified in ISO/IEC 27001: 'Information Security Management' and it is designed to assist the implementation of information security based on a risk management approach.

ISO 27005:2018 describes an information security risk management process comprising the following sub-processes:

- the establishment of context;
- the assessment of risk, which includes risk analysis (risk identification and risk estimation) and risk evaluation;
- the treatment of risk;
- the acceptance of risk;
- the communication of risk and consultation;
- the monitoring and review of risk.

Context establishment includes the specification of risk evaluation and acceptance criteria, scope and boundaries for the assessment of risk and relevant responsibilities. Risk identification includes the identification of assets, threats, existing controls, vulnerabilities, and impacts. Taking these together, risk identification aims to determine what could happen to cause a potential loss, and to gain insight into how, where and why the loss might happen.

Risk estimation according to ISO 27005:2018 could be qualitative, quantitative or hybrid. During risk estimation, risk is estimated as a combination of assigned values of the likelihood of an incident and its consequences. Although ISO 27005:2018 does not provide a single method for calculating risk, it does offer guidelines and examples of scales and risk calculation matrices.

At the stage of risk evaluation, the list of risks and assigned value levels are compared against criteria for risk evaluation. Based on the results of risk evaluation, risk treatment decisions are made. Four options are proposed for risk treatment: risk modification, risk retention, risk avoidance, and risk sharing. Regarding risk modification and the application of security controls, the standard points to ISO 27001.

3.2 NIST SP 800-37 REV. 2

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

The NIST SP 800 Series is a set of published documents that provide the US Federal Government with policies, procedures or guidelines for computer security. NIST compliance is mandatory for all federal agencies. Moreover, the NIST Series can be used either as a roadmap for security enforcement or as legal references in case of litigation involving security issues.

The National Institute of Standards and Technology (NIST) 'Risk Assessment Framework' (RMF) was first published as NIST SP 800-37 Rev. 1 (Joint Task Force Transformation Initiative, 2010) in 2010; it was superseded by NIST SP 800-37 rev. 2 (Joint Task Force, 2018), entitled 'Risk Management Framework for Information Systems and Organisations: A System Life Cycle Approach for Security and Privacy', in 2018. Its goal is to prepare organisations for appropriately managing risk.

NIST SP 800-37 is designed to address the requirements of Federal Information Systems and to satisfy, among others, the requirements set out in the Federal Information Security Modernization Act of 2014 (FISMA), the Privacy Act of 1974, OMB policies, and Federal Information Processing Standards. It can be applied to any type of organisation, including government bodies and private sector organisations.

NIST SP 800-37 Rev. 2 is an asset-based RMF which comprises 7 steps, namely Prepare, Categorise, Select, Implement, Assess, Authorise and Monitor. It does not adopt a specific risk assessment methodology, although the NIST 800-30 guide is extensively referenced. Each step comes with tasks, some of which are optional. Organisations are expected to complete all but the optional tasks for the implementation of the RMF.

- **Prepare** establishes context and priorities for security and privacy risk management, identifies and assigns roles to execute the RMF, sets organisational priorities, risk tolerances etc.
- **Categorise** assesses the impact of an adversary's action for operations, individuals and assets, including information processed by systems within scope (Risk identification).
- During subsequent steps the appropriate controls are **selected**, **implemented** and **assessed,** based on their effectiveness (Risk treatment).
- The **authorisation** step requires a senior management official to determine when the privacy and security risks are acceptable (Risk treatment).
- The goal of the **monitor** step is to continue performing risk assessments and impact analyses, and to document any system changes (Risk Monitoring).

Since the standard does not suggest the use of a specific risk assessment methodology, it does not provide details regarding assets and related taxonomies, threat and vulnerability catalogues, or risk calculation methods. However, it references other NIST related standards, including the NIST Cyber Security Framework (CSF) and the NIST Security and Privacy Controls (NIST SP 800-53).

3.3 NIST SP 800–30 REV.1

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

NIST (SP) 800-30 Rev. 1 (Joint Task Force Transformation Initiative, 2012), entitled 'Guide for Conducting Risk Assessments', is a standard developed by the National Institute of Standards and Technology (NIST) and published on the 12th of September 2012. The scope of SP 800-30

is to provide guidance for conducting risk assessments of federal information systems and organisations, describing the methodology and amplifying the guidance in SP 800-39. Its ultimate goal is to help organisations to better manage the risks of IT-related missions and it entails three functional components, namely Risk Assessment, Risk Treatment and Risk Monitoring. More specifically, the NIST SP 800-30 standard:

- describes as risk assessment the use of risk to determine the extent of a potential threat in order to identify appropriate controls for reducing or eliminating risk during the risk mitigation process, and this corresponds to risk assessment in the risk management framework;
- describes risk treatment as risk mitigation, which involves prioritising, evaluating, and implementing the appropriate risk-reducing controls as recommended by the assessment of risk;
- describes risk monitoring, which is the final functional component, as evaluation and assessment that continually updates and expands the systems and the software applications to assess the effectiveness of the security controls.

3.4 NIST SP 800–39

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf, USA

The final version of the NIST SP 800-39 (Joint Task Force Transformation Initiative, 2011), entitled ‘Managing information security risk’, was published by the National Institute of Standards and Technology (NIST) in March 2011.

The purpose of NIST SP 800-39 is to provide a structured, yet flexible approach for an integrated, enterprise-wide programme for managing the risk to information security of organisational operations (i.e. mission, functions, image, and reputation) and assets, individuals, other organisations etc. on an ongoing basis. It can be used together with other supporting NIST security standards and guidelines in order to ensure a specific and proper assessing, responding to and monitoring of enterprise risk.

Although it was specifically designed for companies considered to be part of US critical infrastructure, many other organisations in the private and public sectors (including federal agencies) are using it either as an Information Security Risk Management Framework or as part of a more comprehensive Enterprise Risk Management (ERM) programme. In the second case, they do not replace other, already implemented, risk-related activities, programmes, processes and/or approaches that cover risk management related to other laws, directives, policies, programmatic initiatives and/or strategic mission or business requirements. It should be implemented under the professional guidance of people who have expertise in both information security and risk management.

The NIST SP 800-39 suggests that risk management should be carried out as a holistic, organisation-wide activity that addresses risk from the strategic level to the tactical level, ensuring that risk-based decision making is integrated into every aspect of the organisation. In this context, it includes the following risk management components:

- Frame risk (i.e. establish the context for risk-based decisions); maps to Risk Identification;
- Assess risk; maps to Risk Assessment;
- Respond to risk once determined; maps to Risk Treatment;
- Monitor risk on an ongoing basis using effective organisational communications and a feedback loop for continuous improvement in the risk-related activities of organisations; maps to Risk Monitoring.

The risk management (RM) process is integrated throughout the organisation via a 3-tiered approach that addresses risk at the: (i) organisational level; (ii) mission or business process level; and (iii) information system level. The RM process is carried out seamlessly across the three tiers, with the overall objective of continuously improving the organisation's risk-related activities and effective inter-tier and intra-tier communications among all stakeholders having a shared interest in the mission or business success of the organisation.

3.5 NIST SP 800–82 REV. 2

https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final, USA

NIST SP 800-82 Rev. 2 (Stouffer, et al., 2015), entitled 'Guide to industrial control systems (ISC) security', is an Industrial Control Systems Security Guide. Its first revision was published in May 2013, while the second revision was published in May 2015. The second revision provides guidance on how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations, such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and safety requirements. The intended audience should be acquainted with general computer security concepts and communication protocols since the guide is technical in nature.

The Risk Management Process has four components: *framing, assessing, responding and monitoring*. These activities are interdependent and often occur simultaneously within an organisation. Risk Management is a continuous process where all components have on-going activities.

- The **framing** component consists of developing a framework for making decisions on the management of risk. This is a component that focuses on governance and aims to identify the relevant stakeholders for risk-related issues. As such, it does not constitute an interoperable characteristic, because it will vary from one organisation to another.
- **Assessing** risk identifies the threats and vulnerabilities, the harm that such threats and vulnerabilities may cause to the organisation, and the likelihood that adverse events arising from those threats and vulnerabilities may actually occur. The DHS National Cybersecurity & Communications Integration Center (NCCIC) serves as a centralised location where operational elements involved in cybersecurity are coordinated and integrated.
- The **response** component is based on the concept of a consistent organisation-wide response to the identification of risk. It includes the implementation of the chosen actions to address identified risk: *acceptance, avoidance, mitigation, sharing, transfer*, or any combination of those options. Risk responses are constrained by system requirements, potential adverse impacts on operations, or even regulatory compliance regimes.
- **Monitoring** risk is an on-going basic activity that keeps track of: the implementation of chosen risk management strategies; changes in the environment that may affect the calculation of risk; and the effectiveness and efficiency of activities to reduce risk. The activities in the monitoring component impact all the other components.

3.6 BSI STANDARD 200-2

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

The BSI-Standard 200-2 ('IT-Grundschutz Methodology') provides a methodology for the management of information security which can be adapted to the requirements of organisations of various types and sizes. It is based on the BSI-Standard 200-1 ('Management systems for information security (ISMS)') and thus also on ISO 27001. It includes guidelines and instructions for creating a comprehensive base for risk analysis, verification of the present level of security and implementation of an appropriate degree of information security.

BSI-Standard 200-2 includes three methodologies 'Standard Protection', 'Basic Protection' and 'Core Protection', which aim to achieve and maintain an appropriate level of information security in organisations. The 'Standard Protection' approach allows the attainment of a level of security for the business processes under consideration that is adequate for the requirements for normal protection and appropriate for protecting business-related information. The 'Basic Protection' approach provides a level of security that is significantly below Standard Protection, but offers a good basis for organisations to begin implementing an information security management process. Finally, the 'Core Protection' approach can be implemented in cases where information and business processes require particular protection.

3.7 OCTAVE-S

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

The OCTAVE Method (Operationally Critical Threat, Asset, and Vulnerability Evaluation) (Alberts, et al., 1999) was developed in 1999 at the Software Engineering Institute. Since then it has been updated and diverse versions have been published. It adopts an asset-based, strategic assessment of information security risk to be applied in large, hierarchic organisations.

The OCTAVE-S (Alberts, et al., 2005) is based on the OCTAVE approach and is a self-directed approach, meaning that people from an organisation assume responsibility for setting the organisation's security strategy. Octave-S is tailored to the limited means and constraints typically found in small organisations (less than 100 people) and can be led by a small, interdisciplinary team (three to five people) who gather and analyse information, producing a protection strategy and mitigation plans based on the organisation's unique operational security risks. To conduct OCTAVE-S effectively, the team must have a broad knowledge of the organisation's business and security processes, so as to be able to conduct all activities by themselves.

OCTAVE-S follows three phases.

- Phase 1 aims at building asset-based threat profiles, by defining criteria for evaluating impacts, identifying important organisational assets and defining security requirements. In this phase, the team select three to five critical assets to analyse in depth, based on their relative importance to the organisation, and defines a threat profile for each critical asset.
- In Phase 2 infrastructure vulnerabilities are identified, by analysing how people use the computing infrastructure to access critical assets and by identifying who is responsible for configuring and maintaining critical components.

- During Phase 3, the team identify risks to the organisation's critical assets and creates a protection strategy for the organisation and mitigation plans to address the risks to the critical assets. The OCTAVE-S provides worksheets to support this phase.

3.8 OCTAVE ALLEGRO

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

The OCTAVE Allegro method (Caralli, et al., 2007) follows the OCTAVE approach and is also a self-directed risk assessment methodology. OCTAVE Allegro is designed to allow broad assessment of an organisation's operational risk environment, with the goal of producing robust results without the need for extensive knowledge of risk assessment. It differs from the previous OCTAVE approaches (OCTAVE and OCTAVE-S) by focusing primarily on information assets in the context of how they are used, where they are stored, transported and processed, and how they are exposed to threats, vulnerabilities and disruptions.

OCTAVE Allegro can also be performed in a workshop-style manner as, like the other versions, it is supported by guidance, worksheets and questionnaires. It is also well suited to perform risk assessment without extensive organisational involvement, expertise or input, and it can be applied by a small team of people belonging to the operational (or business) units and the IT department of the organisation.

OCTAVE Allegro consists of eight steps that are organised into four phases.

- In phase 1, the organisation develops criteria for risk measurement that are consistent with organisational drivers.
- In phase 2, information assets that are determined to be critical are profiled, so that clear boundaries for assets are established, including their locations (where the asset is stored, transported or processed), and security requirements are identified.
- In phase 3, threats to the information assets are identified in the context of the locations where each asset is stored, transported or processed. In the final phase, risks to information assets are identified and analysed, and the development of approaches to mitigation commences.

Octave Allegro is a flexible method that can be tailored for most organisations, it is driven by operational risk and security practices and it provides practical guidance, worksheets, and examples.

3.9 OCTAVE FORTE (OCTAVE FOR THE ENTERPRISE)

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

The OCTAVE FORTE method (Tucker, 2020) (CMU/SEI-2020-TN-002) was published in 2020 and is the newest version of the OCTAVE approach. The OCTAVE FORTE process model was developed to support organisations in evaluating their security risks. It applies Enterprise Risk Management (ERM) principles to bridge the gap between executives and practitioners acting as decision makers. To this end, OCTAVE FORTE identifies processes that support the achievement of strategic objectives, including ways to help executives and practitioners effectively communicate threats and opportunities across the organisation that relate to those objectives.

The OCTAVE Forte process model includes 10 steps:

- Step 1—Establish Risk Governance and Appetite
- Step 2—Scope Critical Services and Assets
- Step 3—Identify Resilience Requirements of Assets

- Step 4—Measure Current Capabilities
- Step 5—Identify Risks, Threats and Vulnerabilities to Assets
- Step 6—Analyse Risks Against Capabilities
- Step 7—Plan for Response
- Step 8—Implement the Response Plans
- Step 9—Monitor and Measure for Effectiveness
- Step 10—Review, Update and Repeat.

The OCTAVE FORTE process is partly based on standards published by the Committee of Sponsoring Organisations (COSO Framework), the International Organization for Standardization (ISO 31000), and the National Institute of Standards and Technology (NIST Cybersecurity Framework (CSF), NIST SP 800-39, NIST SP 800-37) while adhering to the fundamental principles of the CERT Resilience Management Model (CERT-RMM) and the Factor Analysis of Information Risk (FAIR) framework.

Compared to the OCTAVE ALLEGRO process, OCTAVE FORTE addresses all forms of risk, whereby cyber risks are analysed and managed in the same manner as all other risks within an enterprise risk portfolio. Baseline OCTAVE FORTE training also provides all executives, managers and practitioners with a common understanding of the risk management lexicon and practices.

3.10 ISACA RISK IT FRAMEWORK, 2ND EDITION

https://www.isaca.org/bookstore/bookstore-risk-digital/ritf2, Information Systems Audit and Control Association

The Risk IT Framework (ISACA, 2020) was originally developed in 2009 (1st edition) by the Information Systems Audit and Control Association (ISACA) to fill the gap between generic risk management concepts and detailed (primarily security-related) IT risk management frameworks.

As it works at the intersection of business and IT, it allows enterprises to manage and even capitalise on risk in the pursuit of their objectives. It extends COBIT, the globally recognised IT governance framework, and provides an end-to-end, comprehensive view of risks related to the use of IT and a similarly thorough treatment of risk management, from the tone and culture at the top to operational issues.

In summary, it fits all types of organisations or industries and enables enterprises to understand and manage exposure to danger, harm or loss that is related to the use of, or is dependent on, information and communications technology, electronic data and digital or electronic communications. It should be implemented under the professional guidance of people who have expertise in information security, governance and risk management.

The Risk IT Framework provides a set of guiding principles and supporting practices for enterprise management, combined to deliver a comprehensive process model for governing and managing IT risk. It helps enterprises achieve their goals, seize opportunities, and seek greater returns with less risk, as it provides them with a way to focus effectively on areas of IT-related business risk, including risks related to late project delivery, compliance, misalignment, obsolete IT architecture and IT service delivery problems. Guidance is provided on the key activities within each process, responsibilities for the process, information flows between processes and performance management of each process.

In brief, the Risk IT Framework offers a structured, systematic methodology that can enable enterprises to understand and manage all significant types of IT risk, building upon the existing risk related components. As it is not prescriptive regarding control frameworks, organisations can apply it alongside any control framework. It helps enterprises to **identify** current and emerging risks throughout the extended enterprise and to **develop** appropriate operational capabilities to ensure that business processes continue operating during adverse events.

The model is divided into three **domains** (Risk Governance, Risk Evaluation, Risk Response), each containing three **processes**, as follows:

1. **Risk Governance**
   1.1. establish and maintain a common risk view
   1.2. integrate with enterprise risk management
   1.3. make risk-aware business decisions
2. **Risk Evaluation** (maps to Risk Identification & Assessment)
   2.1. collect data
   2.2. analyse risk
   2.3. maintain risk profile
3. **Risk Response** (maps to Risk Treatment)
   3.1. articulate risk
   3.2. manage risk
   3.3. react to events.

The Risk Management Workflow consists of the following major phases, which do not necessarily need to be performed sequentially. Each enterprise should develop a workflow that supports the most efficient and effective means to accomplish necessary tasks. The workflow starts after determining the Example Types and the Categories of Risks (Strategic, Operational, IT Risk, Cybersecurity, Information Security):

- setting context
  - communication
- risk identification and assessment
- risk analysis and business impact evaluation
- risk response
- risk reporting and communication.

3.11 INFORMATION RISK ASSESSMENT METHODOLOGY 2 (IRAM2)

https://www.securityforum.org/solutions-and-insights/information-risk-assessment-methodology-iram2/, Information Security Forum

IRAM2 (Information Security Forum, 2021) was developed by the ISF (Information Security Forum); it supports risk assessment and treatment and entails a six-phase process, consisting of:

- scoping,
- business impact assessment,
- threat profiling,
- vulnerability assessment,
- risk evaluation,
- risk treatment.

IRAM2 is implemented by an automated toolset also developed by the ISF. The toolset is accessible exclusively to ISF members, with supplementary support documentation and consultancy being offered by ISF to assist with its use.

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

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

ETSI TS 102 165-1 (2017, version 5.2.3) (ETSI, 2017) offers methodology and pro-forma for threat, vulnerability and risk analysis (TVRA). According to ETSI TS 102 165-1, threat vulnerability and risk analysis (TVRA) is used to identify risk to an information system based upon the product of the likelihood of an attack and the impact that such an attack will have on the system.

The TVRA methodology provides a means of documenting the rationale for designing security countermeasures in a system by application of a systematic method, and by using part of the method to visualise the relationship of objectives, requirements, system design and system vulnerabilities. The methodology systematically quantifies the assets, vulnerabilities and threats associated to a system. The primary focus of the TVRA is on the assets of a system and it is required to ensure that they can perform their primary function when subjected to a malicious attack. The output of the TVRA is a quantified measure of the risks to the assets and a set of detailed security requirements that will minimise that risk.

The TVRA process consists of the following steps:

- Step 1: identification of the target of evaluation (TOE), resulting in a high-level description of the main assets of the TOE and the TOE environment and a specification of the goal, purpose, and scope of the TVRA;
- Step 2: identification of the objectives, resulting in a high-level statement of the security aims and issues to be resolved;
- Step 3: identification of the functional security requirements, derived from the objectives from step 2;
- Step 4: inventory of the assets as refinements of the high-level asset descriptions from step 1, and additional assets as a result of steps 2 and 3;
- Step 5: identification and classification of the vulnerabilities in the system, the threats that can exploit them, and the unwanted incidents that may result;
- Step 6: quantifying the likelihood of an occurrence and impact of the threats;
- Step 7: establishment of the risks;
- Step 8: identification of a framework of countermeasures (conceptual), resulting in a list of alternative security services and capabilities needed to reduce the risk;
- Step 9: cost-benefit analysis of countermeasures (including cost-benefit analysis of security requirements depending on the scope and purpose of the TVRA) to identify the best-fit security services and capabilities amongst alternatives from step 8;
- Step 10: specification of detailed requirements for the security services and capabilities from step 9.

The application of countermeasures adds assets to the system and may create new vulnerabilities, indicating that the TVRA will need to be undertaken again, and the method should be repeated until all the risks have been reduced to an acceptable level.

3.13 MONARC

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

MONARC (Méthode Optimisée d'analyse des risques CASES – 'Method for an Optimised Analysis of Risks by CASES' (CASES, 2013) is a tool and a method allowing precise and

repeatable risk assessments to take place. It was created in 2013 by the Cyberworld Awareness Security Enhancement Services (CASES) department of the Cybersecurity Agency for the Luxembourg Economy and Municipalities in Luxembourg.

MONARC enables organisations, both large and small, to benefit from the advantages that risk analysis offers. It allows precise and repeatable risk management and works by risk analysis as applied in business contexts: the same vulnerabilities regularly appear in many businesses, as they face the same threats and generate similar risks. Most companies have servers, printers, a fleet of smartphones, Wi-Fi antennas, etc. so therefore the vulnerabilities and threats are the same. It is thus sufficient to generalise risk scenarios for these assets (also called objects) by context and/or business.

MONARC simplifies risk management by offering a risk management solution as well as information security governance, based on industry standards. It allows for analysis from existing and customisable models to be made, while remaining compliant with the ISO/IEC 27005:2011 international standard (CASES, 2013). Among the proposed risk models, it offers compliance with certain standards and laws, with a particular focus on European regulations for the protection of personal data (GDPR), ISO/IEC 27001 certification and the PCI-DSS standard.

The method deploys in four phases: Context Establishment, Risk Modelling, Risk Assessment and Treatment, Implementation and Monitoring (CASES, 2020). The four phases of MONARC fully respect the ISO/IEC 27005:2011 international standard, which contains the guidelines for risk management as related to information security. Each phase delivers a report of the decisions taken and the results obtained.

- In the Context Establishment phase, all the information related to the organisation is gathered in order to establish the scope and limits of the risk analysis, as well as to define the evaluation, acceptance and impact criteria. MONARC uses a qualitative evaluation method, while for vulnerabilities, threats and impacts it uses quantitative criteria.
- In the Risk Modelling phase, identification of threats and vulnerabilities is carried out and impacts are defined. The risk manager builds the risk tree by linking pre-determined MONARC objects to primary assets. To this end, she or he uses assets and associated risk scenarios determined by external experts, corresponding to the maturity level of the entity.
- In the Risk Assessment and Treatment phase, the level of risk is calculated and a risk treatment plan is formulated in order to reduce the risk down to an acceptable level. The assessment consists of quantifying the threats, vulnerabilities and impacts in order to calculate the risks. The treatment of risks follows the four types of treatment provided in ISO/IEC 27005:2011, namely *modification, rejection, acceptance* and *sharing*.

As described in the MONARC website for the Implementation and Monitoring phase (CASES, 2021): 'When the first treatment of risks has been carried out, an ongoing management phase with security monitoring and recurring control of security measures must be entered, in order to improve it in a sustainable manner'. It should be noted that the Monarch tool is frequently updated and enhanced with new features, thus the above description depicts its status at the time of review.

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

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

The EBIOS method for the analysis, evaluation and mitigation of risks relating to information systems was created in 1995. A new version of this method was created in 2018 under the name EBIOS Risk Manager and is now being maintained by the National Cybersecurity Agency of France (ANSSI) with the support of Club EBIOS.

EBIOS Risk Manager can be applied to public as well as private organisations, regardless of their size, their sector of activity and whether their information systems are being developed or already exist. The EBIOS Risk Manager methodology adopts an iterative approach to the management of risk, starting from the highest level (major missions of the studied object) to progressively reach the business and technical functions, by studying possible risk scenarios in five workshops. It aims to obtain a synthesis between 'conformity' and 'scenarios', by positioning these two complementary approaches where they provide the highest added value.

It provides a toolbox that can be adapted and whose use varies according to the objective of the project. EBIOS Risk Manager is compatible with the reference standards in effect, in terms of risk management (ISO 31000:2018) as well as in terms of cybersecurity standards in the ISO/IEC 27000 series (ISO27005 in particular).

EBIOS Risk Manager adopts a scenario-based approach (business strategic scenarios and operational scenarios) towards the stakeholders of the ecosystem (clients, partners, providers, supply chain). This methodology creates a link between decision-makers and operational teams: the strategic scenarios helps in clarifying the decision process at the highest level of the organisation while being based on the operational reality (operational scenarios).

EBIOS *Risk Manager* is supported by a complete ecosystem including an active community of experts from the public and the private sectors (Club EBIOS). Additionally a community of editors (from large editor companies to single players in risk management) develops tools compliant with the EBIOS *Risk* Manager method[2], of which some are available as freemium. Finally, EBIOS *Risk* Manager is supported by a large network of trainers and nine training organisations[3].

3.15 MAGERIT V.3: ANALYSIS AND RISK MANAGEMENT FOR INFORMATION SYSTEMS

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

MAGERIT version 1 was developed by the Spanish Ministry of Public Administration and it was first released in 1997. The MAGERIT v3 Spanish version was published in 2012 (Gobierno de Espana, n.d.). It is offered as a framework and guide for Public Administration. Given its open nature, it is also used outside the Administration. MAGERIT's focus is to offer a systematic method to analyse risk, make those responsible for the integrity of information systems understand the risks associated with these systems and the importance of treating them quickly. It also aims to help organisations select appropriate safeguards and prepare them for audits and certifications.

[2] https://www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager/label-ebios-risk-manager-des-outils-pour-faciliter-le-management-du-risque-numerique/
[3] https://www.ssi.gouv.fr/particulier/formations/secnumedu-fc-labellisation-de-formations-continues-en-cybersecurite/formations-continues-labellisees-secnumedu/

MAGERIT version 3 is structured into three books: 'Method', 'Catalogue of Elements' and 'Guide to Techniques'. The English version for the 1st book (Gobierno de Espana, 2014) was released in 2014. Book 1 covers a broad spectrum of risk management processes, from identifying assets, risks and impacts to defining roles and providing high level guidelines for secure software development by design. Book 2 contains the catalogue of elements, assets, threats, safeguards, and book 3 is the technical guide. It is an asset-based and qualitative RMF.

The main steps of MAGERIT are described in Book 1 and also in Book 2.

- The RM process first identifies the assets such as information, services, software, hardware etc. The dependencies of these assets are then organised in trees or graphs where the assets at the top depend on lower positioned assets and vice versa.
- In order to determine their importance, criteria for high level asset valuation are used in terms of confidentiality, integrity and availability. Chapter 4 of Book 2 (catalogue of elements) provides guidelines on the valuation of assets with a specific scale ranging from 0 - negligible to 10 - very high. There are several criteria to help security professionals determine the right value in the scale. Scales to determine the damage an impact can have on an asset and the likelihood that a threat occurs on a yearly basis are also provided as references. (Risk identification and assessment).
- After calculating impact and risk under the assumption that they are not protected, safeguards are selected. Chapter 5 of Book 2 includes an extensive list of potential threats which mention what types of assets they might affect and in what dimension - confidentiality, integrity, availability or more complex ones like accountability for access to data, and more. Chapter 6 of Book 2 enumerates a list of potential safeguards for each asset type. An extensive list of various types of protection is provided, including impact minimisation, elimination, recovery and more. (Risk assessment).
- MAGERIT also analyses the process of developing a security plan for risk monitoring. It first identifies the security projects, risk treatments actions, then plans how to implement them and finally implements and monitors their performance. It analyses in a descriptive way how such plans can be developed, so it can be used as a source for organisations implementing other ISOs and standards. (Risk treatment and monitoring).

A collection of tools, called Pilar (CCN-CERT, 2021), that implement MAGERIT, has been developed by the Centro Criptológico Nacional (CCN). It is widely used in the Spanish government. It comes with a standard library for assets, threats and countermeasures. A commercial license is required to undertake risk analysis projects (CCN-CERT, 2021). Appendix 3 of Book 1 suggests an XML format to exchange information such as identification of assets, code and name, classification of asset type, identification of asset dependencies and valuation of assets.

MAGERIT provides an in-depth analysis of risk management. It tackles all aspects of it, namely risk identification, assessment, treatment and monitoring. Its large catalogues of threats and safeguards as well as the description of how to create a security plan make it an excellent in-depth source for information on risk management. The downside is that it is in the Spanish language, but version 2, which is available in English, is still a good source of information.

3.16 EU ITSRM, IT SECURITY RISK MANAGEMENT METHODOLOGY V1.2

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

ITSRM² IT Security Risk Management Methodology (2018, version 1.0) (European Commission Directorate-General for Communication, Security standards applying to all European Commission information systems) is a methodology provided by DG DIGIT and the European Commission, as part of a set of standards for information security. The methodology comprises phases and steps that are mapped onto ISO 27005, including Context Establishment, Risk assessment and Risk Treatment.

ITSRM² provides practical guidelines for the implementation of the processes, including:

- a detailed formula to assess the level of risk and the level of residual risk;
- actionable tasks and methods for each risk management sub-process to achieve their respective outcomes, mainly building and assessing the different components of the risk;
- scales to be used throughout the corporation, with the aim of achieving comparable results;
- catalogues to facilitate the processes.

Risk Identification is divided into four sub-processes:

- identification of the primary assets,
- identification of the supporting assets,
- system modelling,
- identification of risks by performing a threat analysis based on the model.

Risk Analysis and Risk Evaluation compute levels of residual risk, prioritise them, and make decisions concerning treatment or acceptance to manage them.

Risk Identification is based on risk scenarios which result from combining assets, security requirements, threat, and supporting assets and existing measures. For assessing the level of risk, the methodology combines the asset value, the likelihood of an event, its frequency and how easily it can materialise, the attractiveness of the asset, the power and interest of adversaries and the strength of existing measures. The methodology uses catalogues for constraint types, asset types, adversary types, threats, and security measures.

3.17 MEHARI

http://meharipedia.x10host.com/wp/home/, CLUSIF, France

MEHARI (CLUSIF, 2012) was developed and has been updated since 1996 by CLUSIF and CLUSIQ and it is distributed free under a Creative Commons license. MEHARI is compliant with the guidelines set by the ISO 27005:2011 standard, and ISO 31000, and allows the seamless integration of risk into an ISO 27001 ISMS development process.

MEHARI is available for free. It includes a risk identification process, based on asset identification and evaluation, a risk assessment process which is guided by a threat directory, and it supports risk management by providing a catalogue of security measures. Mehari 2010 has been updated and is currently available as of now as Mehari Expert, having been revised to comply with updates to ISO/IEC 27005:2011, ISO 2700,1 and ISO 27002 2013.

Three variants of Mehari knowledge bases are currently available in French: Mehari Expert for medium to very large organisations, Mehari Standard for small to medium and large organisations and Mehari Pro for very small entities. The Mehari Expert knowledge base has also been translated to English.

3.18 ENTERPRISE RISK MANAGEMENT – INTEGRATED FRAMEWORK

https://www.coso.org/Documents/COSO-Deloitte-Managing-Cyber-Risk-in-a-Digital-Age.pdf, COSO - Committee of Sponsoring Organizations of the Treadway Commission, USA

Developed by the COSO (Committee of Sponsoring Organisations of the Treadway Commission) in the USA, this framework (COSO, 2021) defines the essential components of enterprise risk management. It is based on a set of principles and concepts for the enterprise and has as its objective to offer a common language for enterprise risk. COSO established an

advisory council composed of representatives from the five COSO organisations, in order to help derive this framework. The council included PricewaterhouseCoopers and Deloitte.

The strategy for the framework was based on taking the mission, vision and core values of an organisation and achieving an enhanced performance. The way this enhancement was achieved was by understanding the implications of the chosen strategy, the possibility of the strategy not aligning the risk to the strategy and its performance for the organisation.

The Integrated Framework for Enterprise Risk Management focuses on Governance and Culture, Strategy and Objective-Setting, Performance, Review and Revision, and Information, Communication and Reporting. This framework assumes that Core traits of companies that have already reached the highest maturity level as defined by the National Institute of Standards and Technology (NIST) include securing the involvement of senior leadership; raising the profile for cybersecurity across the organisation and beyond Information Technology (IT); and aligning cybersecurity efforts more closely with the business's strategy.

The key characteristics of this framework are seen in the strategy and objective setting, where the following four principles are set.

- Analyses Business Context - The organisation considers the potential effects of business context on its risk profile.
- Defines Risk Appetite - The organisation defines risk appetite in the context of creating, preserving and realising value.
- Evaluates Alternative Strategies - The organisation evaluates alternative strategies and their potential impact on risk profile.
- Formulates Business Objectives - The organisation considers risk while establishing the business objectives at various levels that align with and support the strategy.

As change occurs, the organisation needs to consider new cyber risks that did not exist previously and account for the protection of its consumers in the context of the changing operating environment. The application stages are the following.

- Identify Risk - The organisation identifies a risk that has an impact on the execution of its strategy and the achievement of its business objectives.
- Assess Severity of Risk - The organisation assesses the severity of risk.
- Prioritise Risk - The organisation prioritises risks as a basis for selecting responses to risks.
- Implement Risk Responses - The organisation identifies and selects risk responses.
- Develop Portfolio View - The organisation develops and evaluates a portfolio view of risk.

This guidance within the framework shows how an organisation can leverage the five components for effective risk management. Having as its objective to improve the capabilities of an organisation is key in the context of being able to apply an enterprise framework.

3.19 AUSTRALIAN ACSC SECURITY MANUAL

https://www.cyber.gov.au/sites/default/files/2021-06/01.%20ISM%20-%20Using%20the%20Australian%20Government%20Information%20Security%20Manual%20%28June%202021%29.pdf, Australian Cyber Security Centre

The Australian Cyber Security Centre (ACSC) published, in June 2021, the Australian Government Information Security Manual (ISM) (ACSC, 2021), which adopts the use of a risk management framework that draws from NIST 800-37, and includes six steps: define the

system, select security controls, implement security controls, assess security controls, authorise the system and monitor the system. As such, the ISM has similar properties to the NIST 800-37 framework.

The ACSC ISM provides an extensive list containing a plethora of controls and guidelines aimed at various aspects of computer systems, ranging from how to write security documentation to preserving physical security and data transfer. However, it does not provide details with regards to the way that these controls contribute to risk treatment, as it does not adopt a specific risk assessment method. Being a generic risk management framework, the ACSC ISM does not provide any recommendations regarding asset taxonomy and valuation, nor does it use a specific threat or vulnerability catalogue.

3.20 ANSI/ISA-62443-3-2-2020

https://www.isa.org/products/ansi-isa-62443-3-2-2020-security-for-industrial-a, ISA-International Society of Automation

Targeting Security and IT professionals, the ANSI/ISA-62443-3-2-2020 standard, entitled 'Security for industrial automation and control systems, Part 3-2: Security risk assessment for system design' (International Society of Automation, 2021), from the International Society of Automation (ISA), dedicates an entire part to the assessment of security risk for system design. Part 3-2 of the document details the requirements for the effective assessment of risk at the design stage even though the risk has not yet materialised. A key feature of this publication is the processes of assessing risk for zones individually. The requirements set out describe the steps set out in the standard; these are:

- defining a system under consideration (SUC) for an industrial automation and control system (IACS);
- partitioning the SUC into zones and conduits;
- assessing risk for each zone and conduit;
- establishing the target security level (SL-T) for each zone and conduit;
- documenting the security requirements.

Thus, focus is on the requirements to identify and, where required, further compartmentalise the risks at the design phase. What is interesting is that controls for the specific design are derived from security requirements. Risks are assessed at the system design level and definitions such as likelihood, impact and analysis of process hazards are included.

The idea of comparing unmitigated risk with tolerable risk is interesting. This is stated as a requirement and effectively drives the process by which each identified threat is compared to what the organisation sees as tolerable risk. If the unmitigated risk exceeds the tolerable risk, the organisation will determine whether to accept, transfer or mitigate the risk. Thus, the phases of treatment and identification of ownership of risk are present even at the design phase for the system in question.

3.21 THE OPEN GROUP STANDARD FOR RISK ANALYSIS (O-RA), VERSION 2.0

https://publications.opengroup.org/c20a, The Open Group

The Open Group Standard for Risk Analysis (The Open Group, 2021) provides a set of standards for various aspects of information security risk analysis that is based on the Open FAIR™ framework (FAIR Institute, 2021) and can be applied to any risk scenario. It can be used as a foundation for normalising the results of risk analyses across various risk domains. A Risk

Analysis Tool (Beta version), in the form of an Excel spreadsheet, is also provided to perform a quantitative risk analysis.

The Open FAIR risk analysis uses ranges and/or distributions for measurements and estimates of risk factors to reflect the uncertainty about data completeness. For the calculation of risk two main components are used, the Loss Event Frequency and the Loss Magnitude. To quantitatively estimate the risk, the analyst performs a Monte Carlo analysis of the risk.

The methodology provides an approach to quantify risk regardless of the cybersecurity framework used. It focuses on risk analysis only as opposed to a holistic approach regarding risk management, and defines a scenario-based (aka Loss Scenario) process which comprises five stages:

- Stage 1: identify the loss scenario (scope the analysis)
- Stage 2: evaluate the frequency of the loss event
- Stage 3: evaluate the loss magnitude (LM)
- Stage 4: derive and articulate risk
- Stage 5: model the effect of controls.

Although generic threat categories are provided, also called Threat Events, there is no catalogue of threats that a practitioner can use for this purpose. The same applies to vulnerabilities, while for the measures, the methodology provides only categories of controls which affect the risks.

- **Avoidance controls** affect the frequency and/or probability of threat agents establishing contact with assets.
- **Deterrent controls** affect the probability that a contact event becomes a threat event.
- **Vulnerability controls** affect the probability that a threat event will result in a loss event (the probability that threat capability will overcome resistance strength), usually by changing the asset's resistance strength.
- **Responsive controls** affect the loss magnitude, either by limiting primary losses, limiting the frequency of secondary loss events, or limiting the magnitude of secondary loss events.

3.22 CORAS

http://coras.sourceforge.net/, SourceForge https://publications.opengroup.org/c20a, The Open Group

The CORAS method (SourceForge, 2015) was developed and is supported by SourceForge. It is a method for conducting the analysis and management of security risk. It provides a customised language for modelling threats and risks as well as detailed guidelines explaining how the language should be used to capture and model relevant information during the various stages of the security analysis. It is model-based, using the Unified Modelling Language (UML) to model the target of the analysis. It also supports special CORAS diagrams which are inspired by UML.

In the CORAS method a security risk analysis is conducted in eight steps:

- preparations for the risk analysis,
- introductory meeting – customer presentation of the target,
- refinement of target description using asset diagrams,
- approval of target description,
- risk identification using threat diagrams,
- risk estimation using threat diagrams,
- risk treatment using treatment diagrams,
- risk evaluation using risk diagrams.

The CORAS method provides an automated tool (The CORAS Tool) (SourceFroge, 2012) that supports documenting, maintaining and reporting analysis results through risk modelling. The CORAS tool is a diagram editor that can be freely downloaded and can support modelling using all kinds of CORAS diagrams.

3.23 IS RISK ANALYSIS BASED ON A BUSINESS MODEL

https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.99.9619&rep=rep1&type=pdf&usg=AOvVaw3C77Cao-a74uX34l6JeycN, Korea Advanced Institute of Science and Technology, Korea

The IS risk analysis based on a business model was published in 2003 by Dr Bomil Suh and Dr Ingoo Han from the Korea Advanced Institute of Science and Technology (Suh & Han, 2003). The paper is available in English. They pointed out a lack of systematic methods to measure the value of the assets of an information system in terms of operational continuity. Their report proposes an IS risk analysis method based on a business model using a quantitative approach. The values of IS assets come from their importance towards operational continuity, as well as from their replacement costs. Its target audience is medium to large organisations.

Through this method, risk identification, assessment and treatment are performed, but the method does not reference other standards as sources of threats or catalogues of assets or safeguards. However, this method can help implement other methods and vice versa. Firstly, the nature and mission of the organisation should be defined, then the organisation's objectives to achieve its mission, and lastly the relative importance of each business function must be determined, ranging from 0 to 1.

It is vital for risk analysts to fully understand the organisation's innerworkings, since they have to analyse each business function down to its sub-functions, if necessary, until the actual IS assets responsible for these functions are clearly defined. Then, the intended objectives of each function are identified by line managers.

- In stage 1, due to its hierarchic structure, a technique called Analytic Hierarchy Process (AHP) (Forman & Gass, 2001) can be used. AHP compares the effects of a business function on its sub-functions without considering the effect of other objectives or business functions. The relative importance of its value, calculated by means of the AHP, represents the percentage of business objectives which are accomplished by each business function. Examples include the abstract personnel business function and the employee administration sub-function. It is important to note that there is no specific set of functions and sub-functions or a threshold of importance regarding these functions. The method is supposed to be quantitative but abstract, to help quantify the risks in most business environments.
- Stage 2 includes asset identification and evaluation. In this stage the assets are identified and assigned to business functions and, based on their cost and their importance for operational continuity, their value is calculated. Asset categorisation is made in 7 groups. Hardware, software, data/database, personnel, documentation, and various facilities. A specific formula is used to calculate asset values. This is a weighted sum – weighed by the relative importance of business functions associated to the asset in question.
- Stage 3 assesses threats and vulnerabilities. Risk has two components: injury and probability. In this step the risk probability is determined by the risk analyst and the injury level is determined based on the relative importance of the assets in stage 2. Threats can be categorised based on source and adversarial intent. Some examples, such as accidental and internal threats, human errors, intentional and internal threats, disclosure of a system by dishonest employees etc., are provided.
- Stage 4 performs the calculation of the annual loss expected. In this step the injury component mentioned in stage 3 is calculated as the resulting loss if a threat is successful. The annual loss expectancy of each asset is based on the income loss, the replacement cost, and the probability of the threat occurrence.

IS Risk analysis, being a business model-based method, does not provide extensive catalogues of assets, threats or safeguards as other methods do but it does provide mathematical formulas that can quantify asset importance and annual loss expectancies. These formulas can prove useful during the risk management process, especially if the risk analysts want to quantify the importance of certain assets or business functions to help upper management understand and engage with the risk management process.

3.24 IMO MSC-FAL.1/CIRC.3 GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx, International Maritime Organization, UN

These official International Maritime Organization guidelines (IMO, 2017) provide a high-level approach to the management pf maritime cyber risk which refers to the extent a technology asset is exposed to risks during an event that could result in shipping-related operational failure. The guidelines are recommendatory and were presented by IMO in 2017 in order to encourage cybersecurity management practices in the maritime domain. In the context of these guidelines, cyber risk management means the process of identifying, analysing, assessing and communicating a cyber-related risk and accepting, avoiding, transferring or mitigating it to an acceptable level, considering the costs and benefits to stakeholders of the actions undertaken.

These guidelines present the functional components that support effective management of cyber risk. They are not sequential, as all should be concurrent and continuous in practice, and they should be incorporated appropriately in a risk management framework.

- Identify: define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to a ship's operations.
- Protect: implement risk control processes and measures, and contingency planning to protect against a cyber event and ensure continuity of shipping operations.
- Detect: develop and implement the activities necessary to detect a cyber event in a timely manner.
- Respond: develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber event.
- Recover: identify measures to back up and restore cyber systems necessary for shipping operations impacted by a cyber event.

These functional elements follow the NIST framework and encompass the activities and desired outcomes of effective cyber risk management across critical systems affecting maritime operations and information exchange. They constitute an ongoing process with effective feedback mechanisms. IMO suggests that organisations follow best practices included in standards like ISO 27001, NIST framework etc.

3.25 GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

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

The Guidelines on Cyber Security Onboard Ships version 4 (BIMCO, Chamber of Shipping of America, Digital Containership Association, INTERCARGO, InterManager, INTERTANKO, ICS, IUMI, OCIMF, Sybass, WSC, n.d.) were issued by a group of maritime organisations. The

guidelines explain why and how cyber risks should be managed in a shipping context. They outline the risk assessment process with an explanation of the part played by each component of cyber risk and offer advice on how to respond to and recover from cyber incidents.

Cyber risk management is implemented in accordance with the objectives and functional requirements of the International Safety Management (ISM) Code. The guidelines propose a six-step approach in managing cyber risks.

- Identify threats: understand the external cybersecurity threats to the ship and the internal cybersecurity threat posed by inappropriate use and poor cybersecurity practices.
- Identify vulnerabilities: develop inventories of onboard systems with direct and indirect communication links and understand the consequences of a cybersecurity threat on these systems, as well as the capabilities and limitations of existing protective measures.
- Assess risk exposure: determine the likelihood of vulnerabilities being exploited by external threats, the likelihood of vulnerabilities being exposed by inappropriate use, and the security and safety impact of any individual or combination of vulnerabilities being exploited.
- Develop protection and detection measures: reduce the likelihood and the potential impact of vulnerabilities being exploited through protective measures.
- Establish response plans: develop contingency plans to effectively respond to identified cyber risks.
- Respond to and recover from cybersecurity incidents: respond to and recover from cybersecurity incidents using the contingency plan and assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.

The management of cyber risk involves the senior management level of a company on an ongoing basis and not just the ship security officer or IT manager.

3.26 HITRUST

https://hitrustalliance.net/product-tool/hitrust-csf/, HITRUST CSF, USA

The HITRUST CSF (HITRUST Alliance, 2021) is a framework created by security industry experts. The HITRUST Alliance, Inc., founded in 2007, is a not-for-profit organisation, whose mission is to champion programmes that safeguard sensitive information and manage information risk for organisations across all industries and throughout the third-party supply chain. In collaboration with leaders in privacy, information security and risk management from both the public and private sectors, HITRUST develops, maintains and provides broad access to its widely adopted common security, privacy risk and compliance management and de-identification frameworks[4], related assessment and assurance methodologies and initiatives advancing the sharing, analysis, and resilience of data protection.

The HITRUST CSF can be used by all organisations that create, access, store or exchange sensitive information. It can be used across all sectors and throughout the third-party supply chain. It is made to be scalable for organisations based on the type of entity and the volume of data or transactions. However, it proves to be one of the most widely adapted frameworks in the healthcare industry. Since its formation in 2007, 81% of US hospitals and healthcare systems, and 83% of health plans leverage HITRUST. It has been the most widely adopted control framework in the healthcare sector, according to a 2018 HIMSS survey. Moreover,

[4] De-identification is the process used to prevent someone's personal identity from being revealed.

HITRUST compliance is required by all major healthcare payers in the US. No matter what a business does in the healthcare realm, HITRUST CSF certification is often required.

It should be implemented under the professional guidance of people who have expertise in compliance, privacy, information security and risk management. It is designed to streamline regulatory compliance through a common set of security controls mapped to the various standards. It provides scalable security and privacy requirements based on the differing risks and exposures of each unique organisation.

The HITRUST CSF normalises security and privacy requirements for organisations, including federal legislation (e.g. HIPAA), federal agency rules and guidance (e.g. NIST), state legislation (e.g. California Consumer Privacy Act), international regulation (e.g. GDPR), and industry frameworks (e.g. PCI, COBIT). In this context, it simplifies the myriad of requirements by providing a single-source solution, tailored to the needs of any organisation, in order to enable the organisation to achieve and maintain compliance with, among others, HIPAA.

The HITRUST CSF is a proprietary risk and control framework that is updated on an annual basis. Its core structure is based on ISO/IEC 27001 & 27002 and incorporates more than 40 other security and privacy related regulations, standards, and frameworks providing comprehensive and prescriptive coverage. Extensive work is carried out to harmonise with each of the current authoritative sources, while continually evaluating new sources for inclusion. Through the lifecycle of each release, relevant requirements and best practices are integrated and normalised, as needed, while better aligning and eliminating redundant requirements within the framework.

3.27 ISRAM - INFORMATION SECURITY RISK ANALYSIS METHOD

https://fuse.franklin.edu/facstaff-pub/32/, Institute of Electronics and Cryptology, Gebze Institute of Technology, Franklin University

The Information Security Risk Analysis Method (ISRAM) (Karabacak & Sogukpinar, 2005) was published in 2005. It is a survey-based quantitative approach which proposes to analyse the security risks of information technologies by taking current necessities into consideration.

ISRAM is a quantitative, paper-based risk analysis method that is designed to allow effective participation of managers and staff in the process. It is a survey preparation and conduction process to assess the security risk in an organisation. ISRAM does not make single loss expectancy (SLE) or ALE calculations during the calculation of ‘risk’. The unit of ‘risk’ is a single numerical value between 1 and 25, which will be defined according to a specific table that the method has.

ISRAM is performed using public opinion obtained by conducting a survey. It consists of seven main, well-defined steps. The first four steps belong to the survey preparation phase, the fifth step is the conduct of the survey, and the last two steps comprise the phase in which results are obtained and assessed.

- Step-1: awareness of the problem,
- Step-2: listing and weighing the factors,
- Step-3: converting factors into questions, designating answer choices from which interviewees will select answers and assigning numerical values to answer choices,
- Step-4: preparation of risk tables,
- Step-5: conduction of the survey,
- Step-6: application of formula and obtaining a single risk value,
- Step-7: assessment of the results.

ISRAM does not have rigid frames as the number of questions and answer choices, risk tables, weight values and other values may be changed from one analysis to another. ISRAM can be used for a wide range of problems, from technical complications to procedural and political issues.

3.28 FAIR - FACTOR ANALYSIS OF INFORMATION RISK

https://www.fairinstitute.org/what-is-fair, FAIR Institute, USA

The FAIR (Factor Analysis of Information Risk) (Jones, n.d.) cyber risk framework has emerged as the premier Value at Risk (VaR) framework for cybersecurity and operational risk. Compliant with international standards, the FAIR model was developed in 2005 by Jack Jones, who is currently the Chairman of The FAIR Institute.

The FAIR model is universally accepted and can be applied to any and all companies that contend with both perceived and tactile risks. The purpose of the FAIR model is to help organisations understand, analyse, and measure information risk. The model provides an approach to quantify risk and defines the necessary building blocks for implementing effective cyber risk management programmes. Being able to quantify cyber risk is at the core of any such programme. The basic form of the Factor Analysis of Information Risk model is composed of four stages:

- Stage 1. identification of inherent components of the risk scenario(s)
- Stage 2. evaluation of loss event frequency
- Stage 3. evaluating probable loss magnitude (PLM)
- Stage 4. deriving and articulating risk.

The FAIR model works well with other methodologies, such as the ISO/IEC 27002:2005, ITIL, OCTAVE, COBIT, and COSO among others, serving as an analytical and computational engine that complements other available risk assessment models.

3.29 GUIDE TO CONDUCTING CYBERSECURITY RISK ASSESSMENT FOR CRITICAL INFORMATION INFRASTRUCTURE

https://www.csa.gov.sg/legislation/supplementary-references, Cyber Security Agency of Singapore

The Guide to Conducting Cybersecurity Risk Assessment for Critical Information Infrastructure (CSA Singapore, 2019) was first published in 2019 by the Cyber Security Agency of Singapore (CSA). It is available in English. It is a supplementary reference to the Cybersecurity act of 2018. That act established a legal framework for the oversight and maintenance of national cybersecurity in Singapore. Critical Information Infrastructure (CII) sectors are Energy, Water, Banking and Finance, Healthcare, Transport including Land, Maritime and Aviation, Infocom, Media, Security and Emergency Services and Government.

The CSA, in collaboration with each sector lead, the lead government agency in charge of each CII sector, identified their essential services based on criteria such as the impact on Singapore's economy. The target audience includes any organisation, not only CII organisations. The scope of the guide focuses on risk identification, assessment and treatment. Risk monitoring and reporting are outside the scope.

The guide defines commonly used terms such as threat event, vulnerability, likelihood, impact and risk, roles, and responsibilities, in addition to a range for risk levels, ranging from low to very high with different level of risk tolerance. These terms can be mapped onto other ISOs and standards since a high-level description for each one is provided.

The guide contains three steps for risk assessment: identification, analysis, and evaluation. It is a scenario-based guide.

- First, assets are categorised into two subsets. Crown Jewels refer to assets playing a critical role in achieving business objectives. This means that adversaries are most likely to target them. Examples include a distributed control system (DCS) of a power plant. Stepping stones are defined as resources that adversaries would like to compromise and control in order to reach Crown Jewels via lateral movements; for example, an active directory (AD) server. Threats are subsequently identified and risk scenarios are constructed to perform risk analysis.
- The next step (risk analysis) includes a sample assessment table to determine how likely a cybersecurity risk is to occur based on discoverability, exploitability and reproducibility. Likely ratings range from rare (1) to highly likely (5); explanations for each of the above-mentioned parameters are provided. The impact rating ranges from negligible (1) to very severe (5), with each rating accompanied by a description of how it affects confidentiality, integrity, and availability.
- Lastly, a risk matrix is used for risk evaluation. The columns represent the likelihood of risk and the rows represent the impact ratings. The guide mentions risk treatment as a requirement for complete risk management, but it does not provide any control catalogue, as this is considered outside its scope. However, the fact that earlier parts of the guide reference other sources of threat catalogues indicates that it can be used in conjunction with other standards.

The Cyber Kill Chain by Lockheed Martin (Lockheed Martin, 2021), MITRE ATT&CK Knowledge Base (MITRE, 2015-2021) and NIST SP800-30 (Joint Task Force Transformation Initiative, 2012) are directly referenced as sources for threat libraries. The guide can be easily used in conjunction with popular frameworks and standards to perform risk identification, analysis and evaluation.

3.30 RISK MANAGEMENT TOOLS

https://www.riskmanagementstudio.com/download/, Klappir Green Solutions, Ireland

Our survey has also identified several software **tools** and **applications** that implement risk management methodologies or support the implementation of parts or steps of them, including the following: Risk Management Studio, SimpleRisk, Practical Threat Analysis - PTA, Verinice, Cyber Security Evaluation Tool (CSET®), and vsRisk One Trust, which have been included in deliverable D1.

Often used in risk management activities for projects, these tools offer the ability to explicitly prioritise and develop responses towards risk treatment. More generally, risk management tools offer a good way to avoid conflict in the workplace, when in the process of assigning risk ownership and also documenting official responses in the remit of risk treatment activities.

Selecting the right tool for an organisation performing risk management activities is important because this effectively forms part of the definition of how the organisation performs risk analysis and manages processes of, for example, risk acceptance and also risk treatment. Even though the selection of a tool should be made after processes for risk management activities have been defined, this is not always the case. This is the main reason as to why some of the risk management tools are referenced in this work, as these tools align with risk management objectives, while attempting to support organisations in the process of implementing risk management processes.

However, as most RM tools are proprietary, entail cost, and implement specific methodologies or parts of such methodologies, and have limited flexibility and potential for interoperability, they have not been further analysed in this deliverable.

3.31 SYNOPSIS

In this report we presented the most important features and characteristics of a large set of RM frameworks and methodologies that were identified through a systematic-desktop review process.

This collection includes well known and widely used RM standards that provide high level guidelines for risk management processes that can be applied in all types of organisations (e.g. ISO 27005; NIST SP 800-37, SP 800-30 & SP 800-39; BSI 200-2; OCTAVE S, Allegro & FORTE, Open FAIR etc.).

The collection also includes frameworks that are mostly applied in specific regions (e.g. COSO Enterprise Risk Management, the Australian ACSC Security Manual) or specific sectors (e.g. IMO MSC, guidelines on cybersecurity on board ships), and industry-oriented standards (e.g. NIST 800-82, ANSI/ISA-62443-3-2-2020) as well as structured methodologies that include specific phases or steps to implement RM processes (e.g. ETSI TVRA, MONARC, MAGERIT, EBIOS, EU ITSRM, CORAS etc.)

4. CONCLUSIONS

4.1 INTEROPERABILITY FEATURES

Although 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 and therefore strongly depends on the context, paraphrasing the definition provided by Lazarinis et al, (2011), interoperability can be considered to be 'the ability of two or more systems or components, to exchange information and to make mutual use of the information that has been exchanged'.

Based on this definition, the interoperability of risk management frameworks and methodologies can be defined as *'*the ability of a risk management component or method 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.

Through the analysis of a wide collection of RM frameworks and methodologies (presented in the previous section) we identified several features that enable (or limit) the potential for interoperability of RM frameworks and methodologies. These include the following:

- **Compliance** with or support of risk management standards (e.g. by ISO, NIST) and other frameworks or methodologies;
- **The risk management components it supports** which typically include at least Risk Identification (usually based on identification of Assets, Threats and Vulnerabilities), Risk Assessment (including Risk Calculation and Evaluation), Risk Treatment (including security controls selection and implementation), and Risk Monitoring (Assess measures effectiveness and monitor risks);
- **Approach used**, whether it's an asset based approach to risk management or a scenario based approach;
- Use of quantitative or qualitative (or semi-quantitative) **methods for assessing risk**;
- Use of specific, extendable or reusable **catalogues or libraries** (e.g. to support asset evaluation, identification of risks or vulnerabilities, selection of security controls etc);
- Method of **risk calculation** (e.g. most methodologies use one of the Risk = Impact x Likelihood, Risk = Impact x Threat Likelihood x Vulnerability Level or a similar formula);
- Supported **languages** (with the existence of an English version of the methodology considered an advantage);
- ***Licensing costs***.

The potential for interoperability of different frameworks and methodologies relates to the features identified above. For example, if conducting risk assessment following a methodology depends on a specific threat or vulnerability catalogue, the methodology's ability to adopt an alternative catalogue in the context of an interoperable framework will be limited.

Overall, the extensive review and analysis of a large set of RM frameworks and methodologies conducted within Task 1 has allowed us to identify many features which could be used as the basis for designing and implementing an interoperable EU RM framework. These features of interoperability are further analysed in Task 2 and are used to evaluate the interoperability potential of the prominent risk management frameworks. The results of this evaluation are presented in deliverable D3, and they can support the design of an interoperable European RM Framework which can be extended or customised by EU Member States in their effort to mitigate large scale and cross-border cyberattacks and maintain a robust cybersecurity posture.

REFERENCES

ACSC, 2021. *Australian Government Information Security Manual (ISM).* [Online]
Available at: https://www.cyber.gov.au/acsc/view-all-content/ism
[Accessed 27 July 2021].

Alberts, C., Behrens, S., Pethia, R. & Wilson, W., 1999. *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0.* [Online]
Available at: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=13473
[Accessed 27 July 2021].

Alberts, C., Dorofee, A., Stevens, J. & Woody, C., 2005. *OCTAVE-S Implementation Guide, Version 1.* [Online]
Available at: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6795
[Accessed 27 July 2021].

ANSSI, 2021. *EBIOS RISK MANAGER – THE METHOD.* [Online]
Available at: https://www.ssi.gouv.fr/guide/ebios-risk-manager-the-method/
[Accessed 27 July 2021].

BIMCO, Chamber of Shipping of America, Digital Containership Association, INTERCARGO, InterManager, INTERTANKO, ICS, IUMI, OCIMF, Sybass, WSC, n.d. *The Guidelines on Cyber Security Onboard Ships.* [Online]
Available at:
https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/ANNEX%20Guidelines%20on%20Cyber%20Security%20Onboard%20Ships%20v.4.pdf
[Accessed 27 July 2021].

Bundesamt für Sicherheit in der Informationstechnik (BSI), 2008. *BSI Standard 100-3 - Risk analysis based on IT-Grundschutz.* [Online]
Available at:
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-3_e_pdf.pdf?__blob=publicationFile
[Accessed 27 July 2021].

Caralli, R., Stevens, J., Young, L. & Wilson, W., 2007. *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.* [Online]
Available at: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419
[Accessed 27 July 2021].

CASES, 2013. *MONARC, Optimised Risk Analysis Method.* [Online]
Available at: https://www.cases.lu/assets/docs/CASES_Monarc2016EN-web.pdf
[Accessed 27 July 2021].

CASES, 2020. *Method Guide.* [Online]
Available at: https://www.monarc.lu/documentation/method-guide/
[Accessed 27 July 2021].

CASES, 2021. *What is MONARC?.* [Online]
Available at: https://www.monarc.lu/
[Accessed 27 July 2021].

CCN-CERT, 2021. *</Pilar>.* [Online]
Available at: https://pilar.ccn-cert.cni.es/
[Accessed 27 July 2021].

CLUSIF, 2012. *MEHARI_PEDIA.* [Online]
Available at: http://meharipedia.x10host.com/wp/mehari-method/
[Accessed 27 July 2021].

COSO, 2021. *Enterprise Risk Management — Integrated Framework.* [Online]
Available at: https://www.coso.org/pages/erm-integratedframework.aspx
[Accessed 27 July 2021].

CSA Singapore, 2019. *Guide to Conducting Cybersecurity Risk Assessment for Critical Information Infrastructure.* [Online]
Available at:
file:///C:/Users/sokratik/Downloads/Guide_to_Conducting_Cybersecurity_Risk_Assessment_for_CII.pdf
[Accessed 27 July 2021].

ETSI, 2017. *CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA).* [Online]
Available at:
https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/05.02.03_60/ts_10216501v050203p.pdf
[Accessed 27 July 2021].

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
[Accessed 27 July 2021].

FAIR Institute, 2021. *From a Compliance-based to a Risk-based Approach to Cyber Risk Quantification.* [Online]
Available at: https://www.fairinstitute.org/what-is-fair
[Accessed 27 July 2021].

Forman, E. H. & Gass, S., 2001. *The analytical hierarchy process—an exposition*. *Operations Research,* 49(4), p. 469–487.

Gobierno de Espana, 2014. *MAGERIT – version 3.0 Methodology for Information Systems Risk Analysis and Management. Book I - The Method.* [Online]
Available at:
file:///C:/Users/sokratik/Downloads/MAGERIT_v_3_book_1_method_PDF_NIPO_630-14-162-0.pdf
[Accessed 27 July 2021].

Gobierno de Espana, n.d. *MAGERIT v.3: Analysis and risk Management information systems.* [Online]
Available at:

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en
[Accessed 27 July 2021].

Higgins, J. et al., 2019. *Cochrane Handbook for Systematic Reviews of Interventions.* 2nd Edition ed. Chichester (UK): John Wiley & Sons.

HITRUST Alliance, 2021. *HITRUST CSF - Our Framework.* [Online]
Available at: https://hitrustalliance.net/product-tool/hitrust-csf/
[Accessed 27 July 2021].

IMO, 2017. *GUIDELINES ON MARITIME CYBER RISK MANAGEMENT.* [Online]
Available at: https://www.gard.no/Content/23896593/MSC-FAL.1-Circ.3.pdf
[Accessed 27 July 2021].

Information Security Forum, 2021. *INFORMATION RISK ASSESSMENT METHODOLOGY 2 (IRAM2).* [Online]
Available at: https://www.securityforum.org/solutions-and-insights/information-risk-assessment-methodology-iram2/
[Accessed 27 July 2021].

International Society of Automation, 2021. *ANSI/ISA-62443-3-2-2020, Security for industrial automation and control systems, Part 3-2: Security risk assessment for system design.* [Online]
Available at: https://www.isa.org/products/ansi-isa-62443-3-2-2020-security-for-industrial-a
[Accessed 27 July 2021].

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

ISACA, 2020. *Risk IT Framework, 2nd Edition.* 2nd edition ed. s.l.:ISACA.

Joint Task Force Transformation Initiative, 2010. *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.* [Online]
Available at: https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/archive/2014-06-05
[Accessed 27 July 2021].

Joint Task Force Transformation Initiative, 2011. *Managing Information Security Risk: Organization, Mission, and Information System View.* [Online]
Available at: https://csrc.nist.gov/publications/detail/sp/800-39/final
[Accessed 27 July 2021].

Joint Task Force Transformation Initiative, 2012. *Guide for Conducting Risk Assessments.* [Online]
Available at: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
[Accessed 27 July 2021].

Joint Task Force, 2018. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.* [Online]
Available at: https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
[Accessed 27 July 2021].

Jones, J., n.d. *An Introduction to Factor Analysis of Information Risk (FAIR).* [Online]
Available at: http://www.riskmanagementinsight.com/media/docs/FAIR_introduction.pdf
[Accessed 27 July 2021].

Karabacak, B. & Sogukpinar, I., 2005. ISRAM: information security risk analysis method. *Computers & Security,* 24(2), pp. 147-159.

Lockheed Martin, 2021. *The Cyber Kill Chain.* [Online]
Available at: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
[Accessed 27 July 2021].

MITRE, 2015-2021. *MITRE ATT&CK.* [Online]
Available at: https://attack.mitre.org/
[Accessed 27 July 2021].

SourceForge, 2015. *The CORAS Method.* [Online]
Available at: http://coras.sourceforge.net/
[Accessed 27 July 2021].

SourceFroge, 2012. *The CORAS Tool.* [Online]
Available at: http://coras.sourceforge.net/coras_tool.html
[Accessed 27 July 2021].

Stouffer, K. et al., 2015. *Guide to Industrial Control Systems (ICS) Security.* [Online]
Available at: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
[Accessed 27 July 2021].

Suh, B. & Han, I., 2003. The IS risk analysis based on a business model. *Information & Management,* Volume 41, p. 149–158.

The Open Group, 2021. *Risk Analysis (O-RA), Version 2.0.* [Online]
Available at: https://publications.opengroup.org/c20a
[Accessed 27 July 2021].

Tucker, B. A., 2020. *Advancing Risk Management Capability Using the OCTAVE FORTE Process.* [Online]
Available at:
https://resources.sei.cmu.edu/asset_files/TechnicalNote/2020_004_001_644641.pdf
[Accessed 27 July 2021].

Weidt, F. & Silva, R., 2016. Systematic Literature Review in Computer Science-A Practical Guide. *Relatórios Técnicos do DCC/UFJF,* 1(0), pp. 1-7.

TP-01-22-005-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 978-92-9204-554-8
DOI:10.2824/75906