Comparison between capabilities of samples of ISRM methods

Main resources for getting this information are:

- https://www.enisa.europa.eu/publications/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools?v2=1
- https://www.enisa.europa.eu/publications/inventory-of-risk-assessment-and-risk-management-methods?v2=1
- Risk Management - Principles and Inventories for Risk Management / Risk Assessment methods and tools — ENISA (europa.eu)
- https://coras.sourceforge.net/documents/tutorials/part1_securware_CORAS.pdf
- https://www.mdpi.com/2071-1050/15/12/9812
- https://kilthub.cmu.edu/articles/report/Introducing_OCTAVE_Allegro_Improving_the_Information_Security_Risk_Assessment_Process/6574790/1
- https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_ebios.html
- https://insights.sei.cmu.edu/documents/786/2007_005_001_14885.pdf
-

1 - CCTA Risk Analysis and Management Method

Abbreviation: CRAMM

Risk Analysis Type: Qualitative

Number of Steps: 3

Step	Objective
Risk identification	• Defining the boundary for the study for Risk Assessment • Identifying and valuing the physical assets that form part of the system; • Determining the 'value' of the data held by interviewing users about the potential business impacts that could arise from unavailability, destruction, disclosure or modification; • Identifying and valuing the software assets that form part of the system.
Risk analysis	• Identifying and assessing the type and level of threats that may affect the system; • Assessing the extent of the system's vulnerabilities to the identified threats; • Combining threat and vulnerability assessments with asset values to calculate measures of risks.
Risk evaluation	the process of assessing the identified risks to determine their significance and priority for treatment

Document Availability: Available

Tool Supported: Yes

CIA Compatibility: no

2- CORAS

Abbreviation: no abbreviation

Risk Analysis Type: Qualitative

Number of Steps: 8

Step	Objective
1 - Preparations for the Analysis	Gather basic information about the customer, the purpose and domain of the analysis, and the size of the analysis; ensure that the customer and other involved parties are prepared for their roles and responsibilities; appoint a contact person from the customer; agree on a tentative time schedule
2 - Customer Presentation of the Target	Achieve an initial understanding of what the parties wish to have analyzed and what they are most concerned about; decide on the focus, scope and assumptions of the analysis; establish a detailed plan for the analysis
3 - Refining the Target Description Using Asset Diagrams	Ensure a common and more precise understanding of the target of analysis, including its scope, focus and main assets
4 - Approval of the Target Description	Ensure that the background documentation for the rest of the analysis, including the target, focus and scope, is correct and complete as seen by the customer; decide a ranking of the assets according to importance in order to prioritize the time and resources during the analysis; establish scales for estimating risk and criteria for evaluating risks
5 - Risk Identification Using Threat Diagrams	Identify the risks that must be managed; determine where, when, why and how they may occur
6 - Risk Estimation Using Threat Diagrams	Determine the risk level of the identified risks
7 - Risk Evaluation Using Risk Diagrams	Decide which of the identified risks are acceptable and which of the risks that must be further evaluated for possible treatment
8 - Risk Treatment Using Treatment Diagrams	Identify cost effective treatments for the unacceptable risks

Document Availability: Available
Tool Supported: Yes
CIA Compatibility: Yes

3 - Operationally Critical Threat, Asset, and Vulnerability Evaluation Allegro

Abbreviation: OCTAVE allegro

Risk Analysis Type: Qualitative and Quantitative

Number of Steps: 8

Step	Objective
1 - Establish Risk Management Criteria	establishes the organizational drivers that will be used to evaluate the effects of a risk to an organization's mission and business objectives.
2 - Develop Information Asset Profile	begins the process of creating a profile for those assets. A profile is a representation of an information asset describing its unique features, qualities, characteristics, and value.
3 - Identify Information Asset Container	all of the containers in which an asset is stored, transported, and processed, whether internal or external, are identified.
4 - Identify Areas Of Concern	begins the risk identification process by brainstorming about possible conditions or situations that can threaten an organization's information asset.
5 - Identify Threat Scenarios	the areas of concern captured in the previous step are expanded into threat scenarios that further detail the properties of a threat,, a broad range of additional threats is considered by examining threat scenarios.
6 - Identify Risks	the consequences to an organization if a threat is realized are captured, completing the risk picture.
7 - Analyze Risks	a simple quantitative measure of the extent to which the organization is impacted by a threat is computed.
8 - Select Mitigation Approach	determine which of the risks they have identified require mitigation and develop a mitigation strategy for those risks.

Document Availability: Available

Tool Supported: no

CIA Compatibility: Yes

4 - Expression des Besoins et Identification des Objectifs de Sécurité

Abbreviation: EBIOS

Risk Analysis Type: Qualitative and Quantitative

Number of Steps: 5

Step	Objective
Scope and security baseline	- define the framework of the study, its business and technical scope, the associated feared events and the security baseline. --- - define the framework of the study; - define the business and technical perimeter of the studied object; - identify the feared events and assess their level of severity; - determine the security baseline
Risk origins	- The purpose of this step is to identify the risk origins (RO) and their target objectives (TO), linked with the particular context of the study. The Step aims to answer the following question: who or what can infringe upon the missions and business assets identified in Scope and security baseline, and for what purposes? - identify the risk origins and the target

	objectives; - assess the RO/TO pairs; - select the RO/TO pairs that are deemed as deserving priority in order to continue the analysis.
Strategic Scenarios	. - to obtain a clear view of the ecosystem, in order to identify the most vulnerable stakeholders in it. This will then entail building high-level scenarios, called strategic scenarios. These scenarios are attack paths that a risk origin can use to reach its target (i.e. one of the RO/ TO pairs selected during workshop 2). —--- - build the ecosystem digital threat mapping and select the critical stakeholders; - develop strategic scenarios; - define the security measures on the ecosystem.
Operational Scenarios	to build operational scenarios. They diagram the methods of attack that the risk origins could use to carry out the strategic scenarios. This step focuses on the supporting assets. The operational scenarios obtained are assessed in terms of likelihood. At the end of this workshop, you will create a summary of all of the risks of the study. —--- - develop the operational scenarios; - assess their likelihood.
Risk Treatment	- create a summary of the risk scenarios identified and to define a risk treatment strategy. This strategy results in the defining of security measures, listed in a security continuous improvement plan (SCIP). The residual risks are then identified as well as the framework for following these risks. —--- - create the summary of the risk scenarios; - define the risk treatment strategy and the security measures; - assess and document the residual risks; - set up the framework for monitoring risks.

Document Availability: Available

Tool Supported: No

CIA Compatibility: Yes