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	identify and document potential risks that could affect the confidentiality, integrity, or availability of the system and its data.
Risk analysis	systematically assess the identified risks to determine their significance and prioritize them for mitigation.
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

Study of the context	- Identify the risk sources that are relevant for the studied object - . Identify and describe the studied object - Identify the reference bases to be complied with - . Identify the components of the ecosystem
Identification of risks relating to the risk sources	- Assess the relevance of the risks relating to risk sources - Determine the final states that they may lead to - Identify the risk sources that are relevant for the studied object
Analysis of the risks at the primary assets' level	. - Identify the primary assets - Analyze the "functional" scenario of risk sources - Assess the severity of each risk at the primary assets' level
Analysis of the risks at the supporting assets' level	. - Identify the supporting assets - Analyze the "practical" scenario of risk sources - Assess the likelihood of each risk at the supporting assets' level
Evaluation, treatment and risks acceptance	- Evaluating the risks - Identify the objectives - Demonstrate the satisfaction of the reference bases to be complied with - . Determine the additional controls to be implemented - Accept the residual risks - Monitoring risks and continuous improvement

Document Availability: Available

Tool Supported: Yes

CIA Compatibility: Yes