cases.lu
Secure. Innovate. Lead.

OPTIMISED RISK ANALYSIS METHOD

cases MONARC

Customisable risk models

Simplified risk-based governance

Faster compliance with current norms and laws

Automatic generation of reports

EN

cases MONARC

SUMMARY

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie

SECURITY
MADEIN.LU

MONARC,
Optimised Risk Analysis Method

CASES[1] promotes information security through the use of behavioural, organizational and technical measures. Depending on its size and its security needs, organisations must react in the most appropriate manner. Adopting good practices, taking the necessary measures and adjusting them proportionally: all this is part of the process to ensure information security. Most of all, it depends on performing a risk analysis on a regular basis.

Although the profitability of the risk analysis approach is guaranteed, the investment represented by this approach in terms of the required cost and expertise is a barrier for many companies, especially SMEs.

To remedy this situation and allow all organisations, both large and small, to benefit from the advantages that a risk analysis offers, CASES has developed an optimised risk analysis method: MONARC (Method for an Optimised aNAlysis of Risks by CASES), allowing precise and repeatable risk management.

The advantage of MONARC lies in the capitalisation of risk analyses already performed in similar 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. therefore the vulnerabilities and threats are the same. It is therefore sufficient to generalise risk scenarios[2] for these assets[3] (also called objects) by context and/or business.

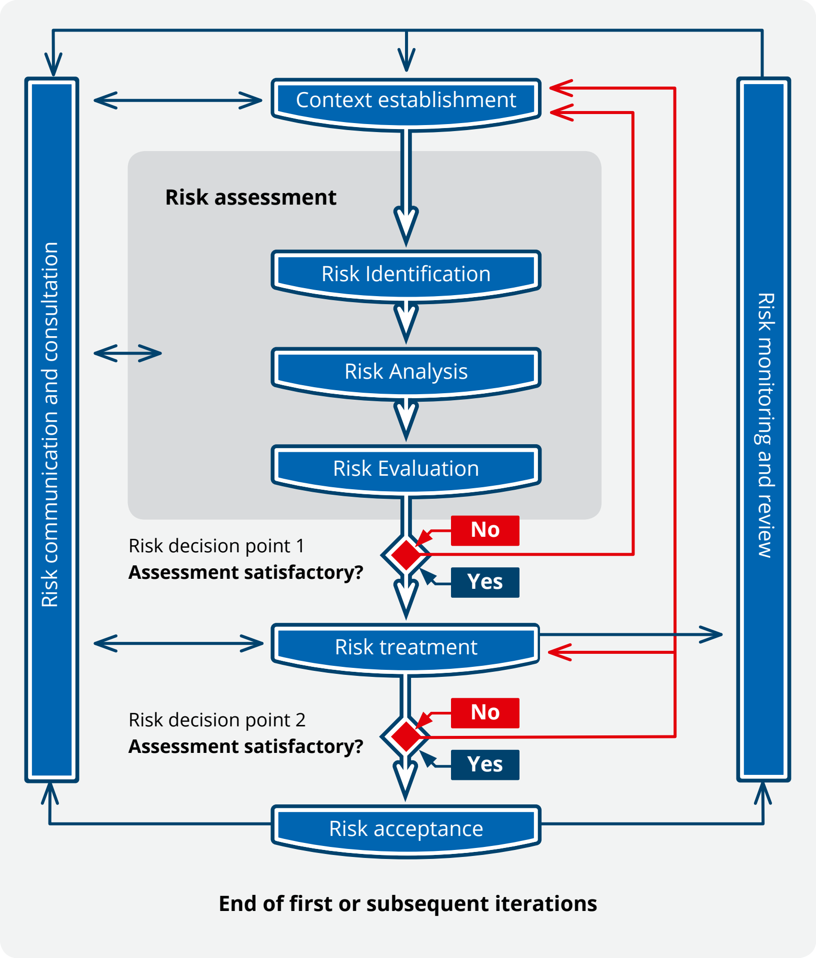
[1] CASES: Cyberworld Awareness and Security Enhancement Services: www.cases.lu

[2] A risk scenario is, more or less, a complete list of threats and vulnerabilities corresponding to an asset or group of assets.

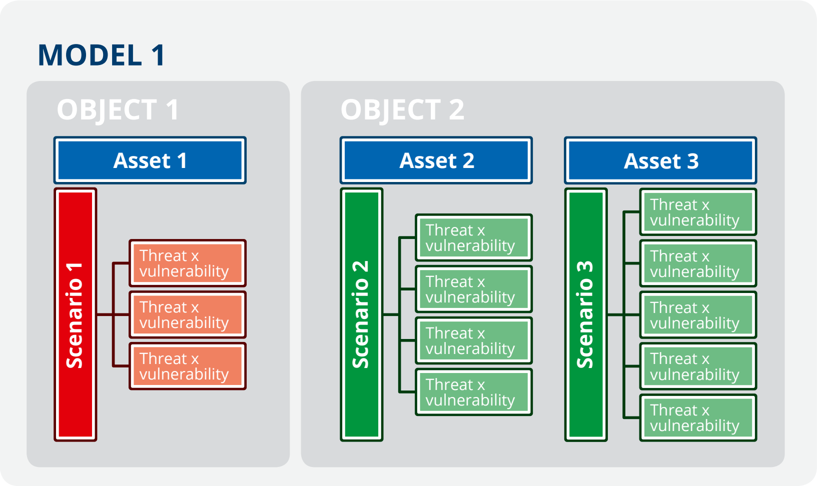
[3] Assets: all tangible and intangible elements that play a role in the activities of an organisation.

Introduction - Risk Modelling

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 in a short amount of time, while remaining compliant with the ISO/IEC 27005:2011 international standard.



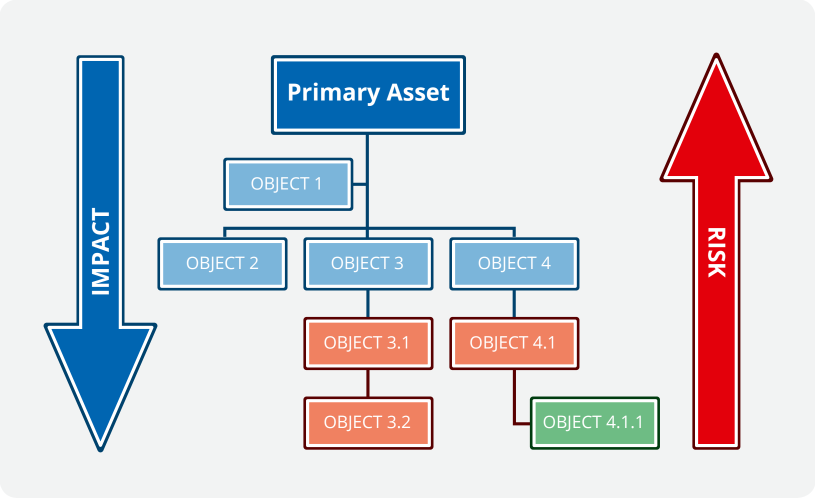
MONARC is based on a library of risk models offering objects made of risk scenarios by assets or groups of assets. This approach facilitates the management of the most common risks and allows for benefits in objectivity as well as efficiency. As MONARC is completely repeatable, these results can be intensified and adjusted to the maturity of each organisation by increasing the depth of risk scenarios.



The risk analysis is made by describing the primary assets (business or information process according to ISO/IEC 27005:2011) and by associating objects modelling the predefined risks in a cascade, that is to say, by building a tree of objects. The impact is defined at the highest level and inherited downwards to all the risk objects in order to calculate risk:

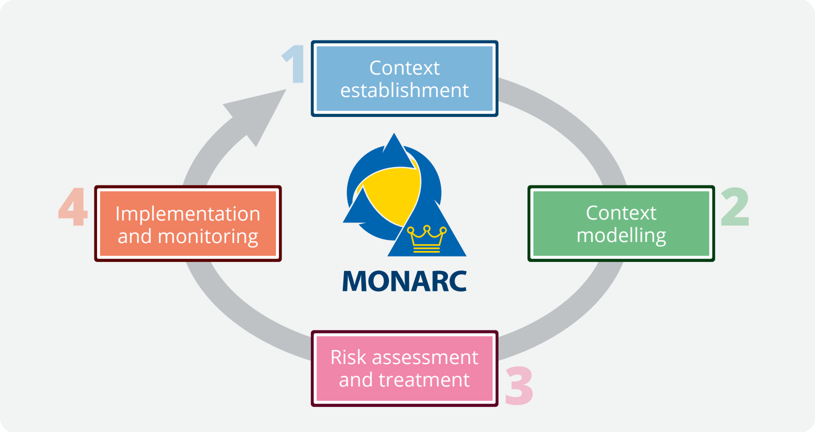
Risk = Threat x Vulnerability x Impact.

Other aspects (threats and vulnerabilities) of risks are calculated at the level of each object, which moves upwards towards the primary asset and groups all of the risks identified with their estimates together.

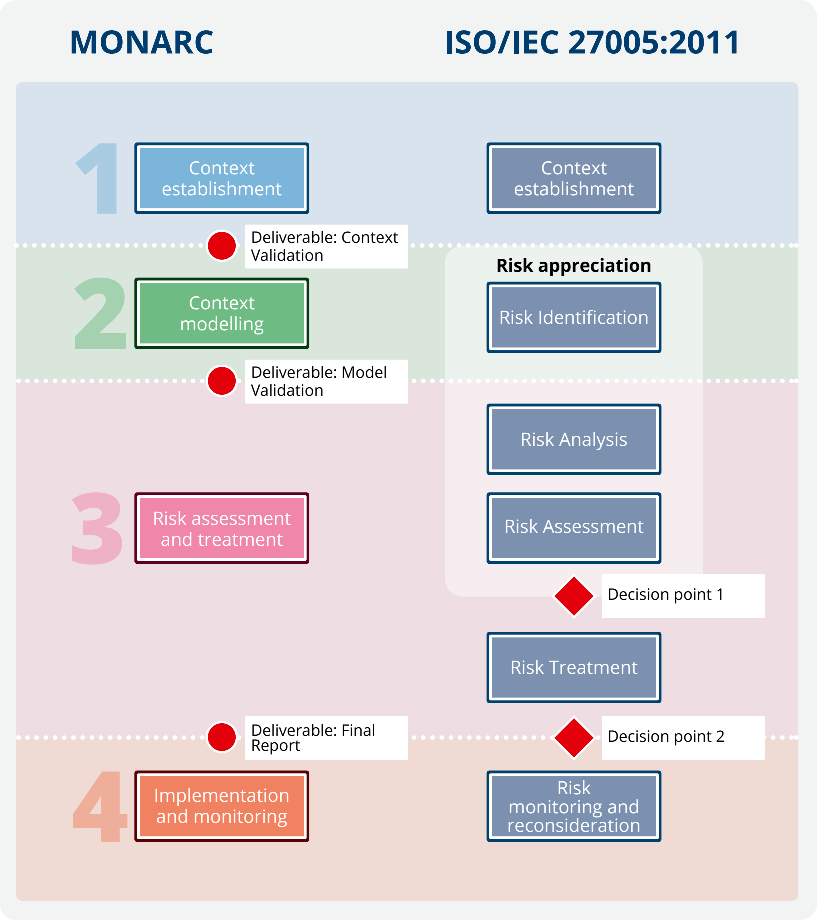


Among the proposed risk models, we find support for compliance with certain standards and laws, with a particular focus on European regulations for the protection of personal data (GDPR), ISO/IEC 27001 certification and the PCI-DSS standard. These models are shareable at will, and each user in the MONARC community can develop, improve and share their own experiences to more effectively address risks.

The method deploys in four phases

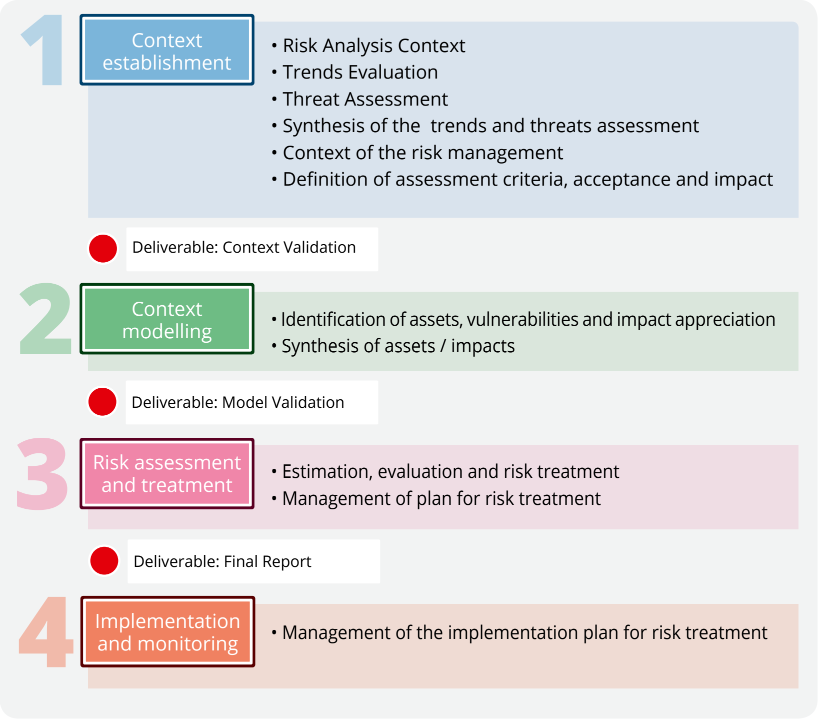


Upon each complete iteration, the analysis may be refined with an increased level of detail and need. The four phases of MONARC fully respect the ISO/IEC 27005:2011 international standard, which contains the guidelines for risk management as related to information security. A comparison with MONARC is displayed on Figure 2.



Each phase delivers a report of the decisions taken and the results obtained.

Method summary



1 Context establishment

- Risk Analysis Context
- Trends Evaluation
- Threat Assessment
- Synthesis of the trends and threats assessment
- Context of the risk management
- Definition of assessment criteria, acceptance and impact

● Deliverable: Context Validation

2 Context modelling

- Identification of assets, vulnerabilities and impact appreciation
- Synthesis of assets / impacts

● Deliverable: Model Validation

3 Risk assessment and treatment

- Estimation, evaluation and risk treatment
- Management of plan for risk treatment

● Deliverable: Final Report

4 Implementation and monitoring

- Management of the implementation plan for risk treatment

The ability to choose the level of completeness (scope, detail, attack scenarios/risk scenarios) depending on the maturity of the organisation, is also an important element of optimising the MONARC approach. Although at first sight this approach may appear to eliminate certain aspects, we must not forget that it is designed as a pragmatic and repeatable solution to meet the needs of any type of organisation. In this way, companies with little experience in information security or with limited financial or human resources have the opportunity to choose a level of initial security that is less high while suited to their expertise and financial means. The security level can then be gradually improved.

Thanks to its flexibility, MONARC can not only integrate different levels of detail, but also reduce the number of risks to be addressed in the first performance. This approach significantly improves the speed, efficiency, accessibility and acceptance of risk analysis.

Based on the ISO/IEC 27005:2011 standard and drawing on the basics of EBIOS and the experience offered by CASES, the MONARC approach takes advantage of proven methods and adapts them to the real needs of businesses and other organisations in order to reduce the complexity and cost of risk analysis.

MONARC modelling includes the following concepts:

- **The extent of the risk analysis** – what should be taken into consideration?
    - The list of primary assets as well as the impacts caused by loss of confidentiality, integrity or availability.
- **The detail of risk analysis** – what level of detail should be required?
    - The list of secondary assets.
    - The list of threats that must be associated with secondary assets as well as the likelihood of said threats.
    - The list of vulnerabilities that must be associated with secondary assets as well as the likelihood of exploiting said vulnerabilities.
- **Risk treatments authorised** and their maximum efficiency.
- **The threshold of acceptable risk** (risk acceptance grid).

PHASE 1 - Context Definition

The first step is to take stock of the context, challenges and priorities of the company or organization that wishes to analyse its risks. This particularly serves to identify key activities and critical processes of the business in order to guide the risk analysis towards the most important elements. To do this, a kick-off meeting is organized with the members of the management and key individuals. The goal is to know what makes the company «live» and what could destroy it, to identify the key processes, the internal and external threats as well as organisational, technical and human vulnerabilities.

1) **Risk analysis context**: gathering all the information related to the organisation in order to establish the scope and limits of the risk analysis. In this phase, certain objects may be excluded from the risk analysis (with justification).

   The market environment and its likely impact on the development of the organisation will be considered in order to outline the scenarios in terms of the development of vulnerabilities and potential attacks.

2) **Definition of evaluation, acceptance and impact criteria**: MONARC uses a qualitative evaluation method. Vulnerabilities, threats and impacts are estimated on a scale of 0 to 4. A risk acceptance grid must then be defined, or rather, a maximum value of risk (R = T x V x I) must be set, from which risks can no longer be accepted and must be treated.

   For example, if R> or = 18, the risk must be treated.

3) MONARC provides predefined and estimated scales of threats, vulnerabilities and impacts, which can be adapted to business needs. This involves the adaptation of the probability of the occurrence of threats compared to increased or reduced exposure, or the adjustment of the qualification of vulnerabilities based on the security measures in place. The level of direct impact in terms of confidentiality, integrity and availability and their consequent impacts on the business can be defined by primary assets (costs for the organisation, damage to the reputation, harm to the private life, legal consequences, etc.)

Advantage :

The reuse of pre-determined objects gives a greater objectivity to the risk analysis, since the list of assets, threats and vulnerabilities to consider was selected by experts, who are external to the entity. This approach also promotes the exchange of experience and the implementation of contextual benchmarks in the development of inter-laboratory tests.

PHASE 2 - Risk Modelling

This phase includes the modelling of objects and trees, and is finalised by a report that must be approved by the management.

1) Identification of assets

The assets were identified in the previous phase. They must now be detailed and formalised in a diagram that displays their interdependencies.

A primary asset means either a service, or an information.

A secondary asset is a supporting element to a primary asset (such as the file server).

Identifying the assets of an organisation is an essential step, and everything that has value to the company should be taken into consideration. However, it is not appropriate to begin the first risk analysis with a comprehensive list of primary and secondary assets in consideration to every possible risk scenario. The choice of details must be made according to the number and importance of the primary and secondary assets as well as the number of analysis already performed (there will be more details in the third analysis than the first).

Note that it is not necessary to have a complete list of all assets. The principles of proportionality and necessity should be kept in mind.

2) Vulnerability Assessment

The identification of threats and vulnerabilities is carried out by means of “MONARC objects”. Here we can once again decide on the desired level of granularity, either opting for risks affecting the organization and exploiting common vulnerabilities, or through going deeper into the technical expertise.

3) Impact Assessment

Impacts are defined at the level of the primary assets (processes or information), following the information gathered in the context establishment phase. The secondary assets inherit the impact of the primary asset to which they are attached (object tree). The impact level of the secondary assets can be modified manually.

The risk manager builds the risk tree by linking pre-determined MONARC objects to primary assets. As such, it uses assets and associated risk scenarios determined by external experts, corresponding to the maturity level of the entity.

The risk manager does not need to seek out all relevant risk scenarios, but can rely on scenarios already offered by the experts.

Advantage :
The security officer may propose objects (lists of predefined risk scenarios) and ensure that each department uses the same objects and conforms to a single taxonomy. Thus, the various analyses performed will be able to be compared in the department and even linked to a “corporate” analysis. A detail can therefore be increased by adding additional assets and corresponding scenarios. For example, upon the emergence of new threats.

PHASE 3 - Risk Assessment and Treatment

Risk calculation / threshold

		T x V								
		0	1	2	3	4	6	8	9	12
IMPACT	0	0	0	0	0	0	0	0	0	0
	1	0	1	2	3	4	6	8	9	12
	2	0	2	4	6	8	12	16	18	24
	3	0	3	6	9	12	18	24	27	36
	4	0	4	8	12	16	24	32	36	48

$$\sum R = T \times V \times I$$

R = Risque · **T** = Threat · **V** = Vulnerability · **I** = Impact

The assessment consists of quantifying the threats, vulnerabilities and impacts in order to calculate the risks.

To do this, it is necessary to have quality information about the exact likelihood of the threats, the ease of exploitation of vulnerabilities and potential impacts; hence the need to rely on metrics that have been validated by experts.

When the risk assessment identifies a risk that is higher than the acceptable level (risk acceptance grid), risk treatment measures should be implemented in order to reduce the risk down to an acceptable level.

1) **Risk estimation, assessment and treatment**: qualitative assessment of the probability of threats and qualification of vulnerabilities as regards to the modelled assets. The calculation of the level of risk is always made on the basis of the following formula:

Risk = **T**hreat x **V**ulnerability x **I**mpact

The method ranks the risks in ascending or descending order based on multiple criteria, such as the level of risk, impact, probability of threats, etc. This allows the comparison of risk levels with regards to the acceptance threshold.
The treatment of risks may follow the four types of treatment provided in ISO/IEC 27005:2011: modification, rejection, acceptance and sharing.

2) **Management of the risk treatment plan**: prioritisation of recommendations following the level of importance and organisational priorities. An interactive table is made available to support the management of the treatment plan.

3) **Final report:** generation of the final deliverable presenting the results and all information related to the risk analysis.

PHASE 4 - Monitoring and Control

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.

This fourth phase also allows to continuously optimise security by increasing the detail of objects used and by expanding the scope of the risk analysis.

Advantage :
The security officer will be able to set minimum and maximum probabilities for certain threats. He may also determine the ease of exploitation of certain vulnerabilities.

Governance

MONARC offers a number of governance possibilities:

- Adaptation of impacts for the loss of confidentiality, integrity or availability for certain areas of activity in relation to the primary assets.
- Adaptation of risk acceptance grids.
- Adaptation of target profiles by adding or removing business areas.
- Adaptation of target profiles requiring different levels of maturity (detail).
- Adaptation of needs' matrices by changing the required standards (endogenous factors such as assets, threats, vulnerabilities and measures).

New libraries of models can be added along the way as needed.

Lastly, MONARC has a community of users that can enhance the performance of risk analysis through the exchange of experiences.

Club MONARC

Club MONARC brings users of the MONARC method together. It allows them to meet regularly in order to exchange experiences and help the tool evolve. They can also work together on shared libraries of objects.

Club MONARC also gives them privileged access to events organised by SECURITYMADEIN.LU, and allows them to appear in the cybersecurity "ecosystem", in order to emphasize their qualitative approach.

www.cases.lu

services@cases.lu

cases.lu
cyberworld awareness and
security enhancement services
LUXEMBOURG

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie

SECURITY
MADEIN.LU