




MEHARI 2010

Information risk management method ISO/IEC 27005 compliant

Exceeding the basic guidelines of the standard
allows for a real management of risk.

Summary

- 
- A red arrow pointing to the right, indicating the start of the summary list.
- Manage your risks using ISO 27005 and MEHARI 2010
 - The knowledge base of MEHARI 2010
 - Patterns and quantification functions
 - Synthesis of MEHARI 2010 new features
 - Open Source Distribution of MEHARI

Risk Management

- Risk management: why?
- Risk management: how?
 - ISO 27005 general concepts and open questions
 - A risk model is necessary beyond ISO 27005 concepts

Risk management: why?

ISO/IEC 27005 Section 1 Scope:

- This international standard ... is designed to assist the satisfactory implementation of information security based on a risk management approach.

Risk management: why?

ISO/IEC 27005 Section 7.1 General considerations:

- It is essential to determine the purpose of the information security risk management as this affects the overall process.
... This purpose can be:
 - Supporting an ISMS
 - Legal compliance and evidence of due diligence
 - Preparation of a business continuity plan
 - Preparation of an incident response plan
 - Description of the information security requirements for a product, a service or a mechanism

Risk management: why?

Reassessed purposes of MEHARI 2010:

Manage the risks faced by the enterprise or organisation, i.e.:

- Identify all the risks laying on the enterprise
- Quantify the seriousness level of each risk
- Apply, for each unacceptable risk, required controls such as to reduce this level to an acceptable value
- ...

Risk management: why?

Reassessed purposes of MEHARI 2010:

Manage the risks faced by the enterprise or organisation, i.e.:

- ...
- Establish a continual monitoring of the risks and their level
- Ensure that each individual risk is appropriately taken in charge, following a decision to accept, reduce, avoid or transfer it

Risk management: how?

The direct management of each risk adopted by MEHARI imposes additional specifications, beyond the standard, for:

- Risk identification
- Risk estimation
- Risk treatment

Risk identification

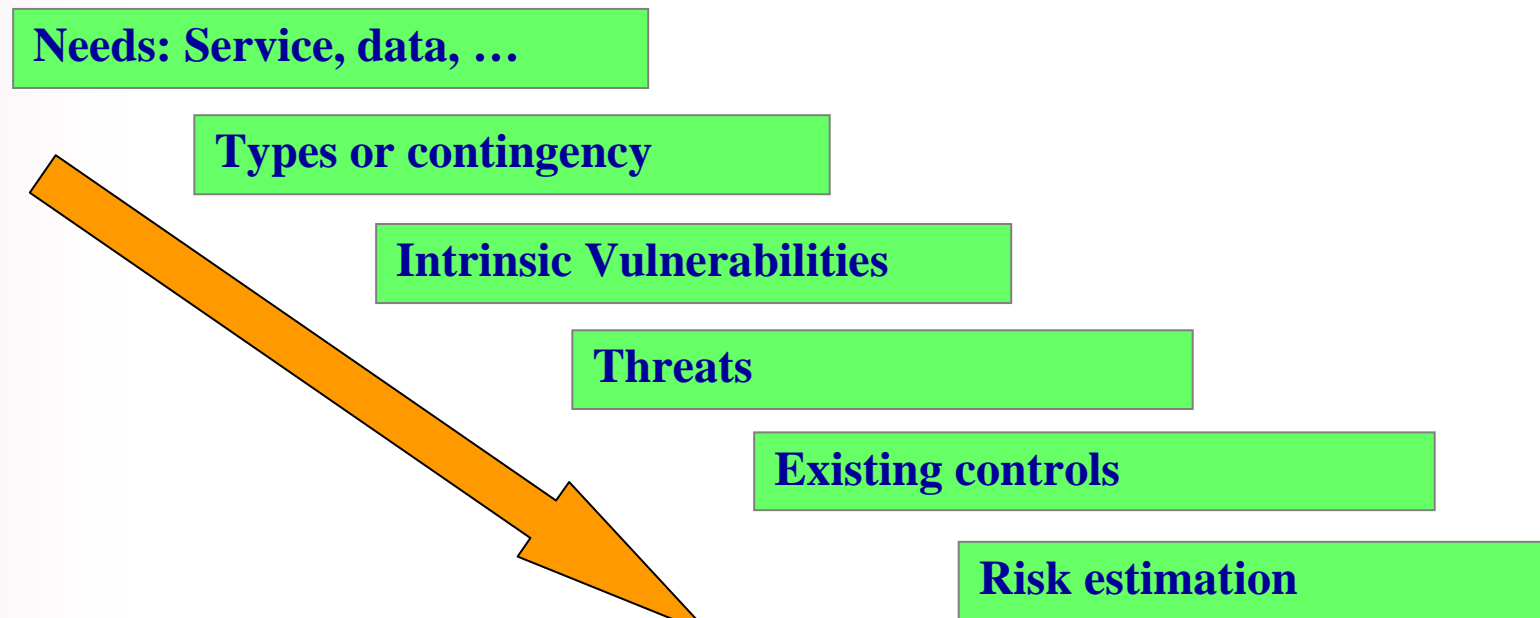
Compliance to ISO 27005 standard imposes identification of:

- Assets § 8.2.1.2
- Threats § 8.2.1.3
- Existing controls § 8.2.1.4
- Vulnerabilities § 8.2.1.5
- Consequences § 8.2.1.6

Activities described ... may be conducted in a different order depending on the methodology applied § 8.2.1.1

Risk identification

MEHARI 2010 conducts the risk identification process as shown below :



Risk identification

Additional definitions are required at that stage:

Primary assets

In order to guarantee that all risks will be identified, MEHARI 2010 starts by considering the 3 types of "needs for each activity".

- Need of services
- Need of information (or data) required to complete the service
- Need for compliance (of processes and behaviour) to a referential (ethic, regulatory, legal, etc.)

The **primary assets** for the organisation or the enterprise will result from the exhaustive identification of these needs.

Risk identification

Secondary assets

MEHARI 2010 considers how the primary assets are embodied:

- materialisation or media
- Dependencies and contingencies

The thorough study of these incarnations allows to identify the **secondary assets** for each type of primary asset.

Risk identification

Vulnerabilities

ISO 27000 definition:

“weakness of an **asset or control** that can be exploited by a **threat**”

Note that this definition presents two totally different views.

Risk identification

Vulnerabilities

In order to identify all the risks, MEHARI 2010 differentiates these two views:

- **Intrinsic vulnerability:** Intrinsic character of an asset that may be acted by a threat
- **Contextual vulnerability:** weakness of a security control that may be exploited by a threat

The identification of risks must rest on the search of intrinsic vulnerabilities

Risk identification

Threats

In order to estimate the risks, the description of the threat needs to include all its specific elements.

MEHARI 2010 specifies this description including:

- **The initial event** and its character, either voluntary or accidental
- **The actor** triggering this event
- **The circumstances** attached to this event

Risk assessment

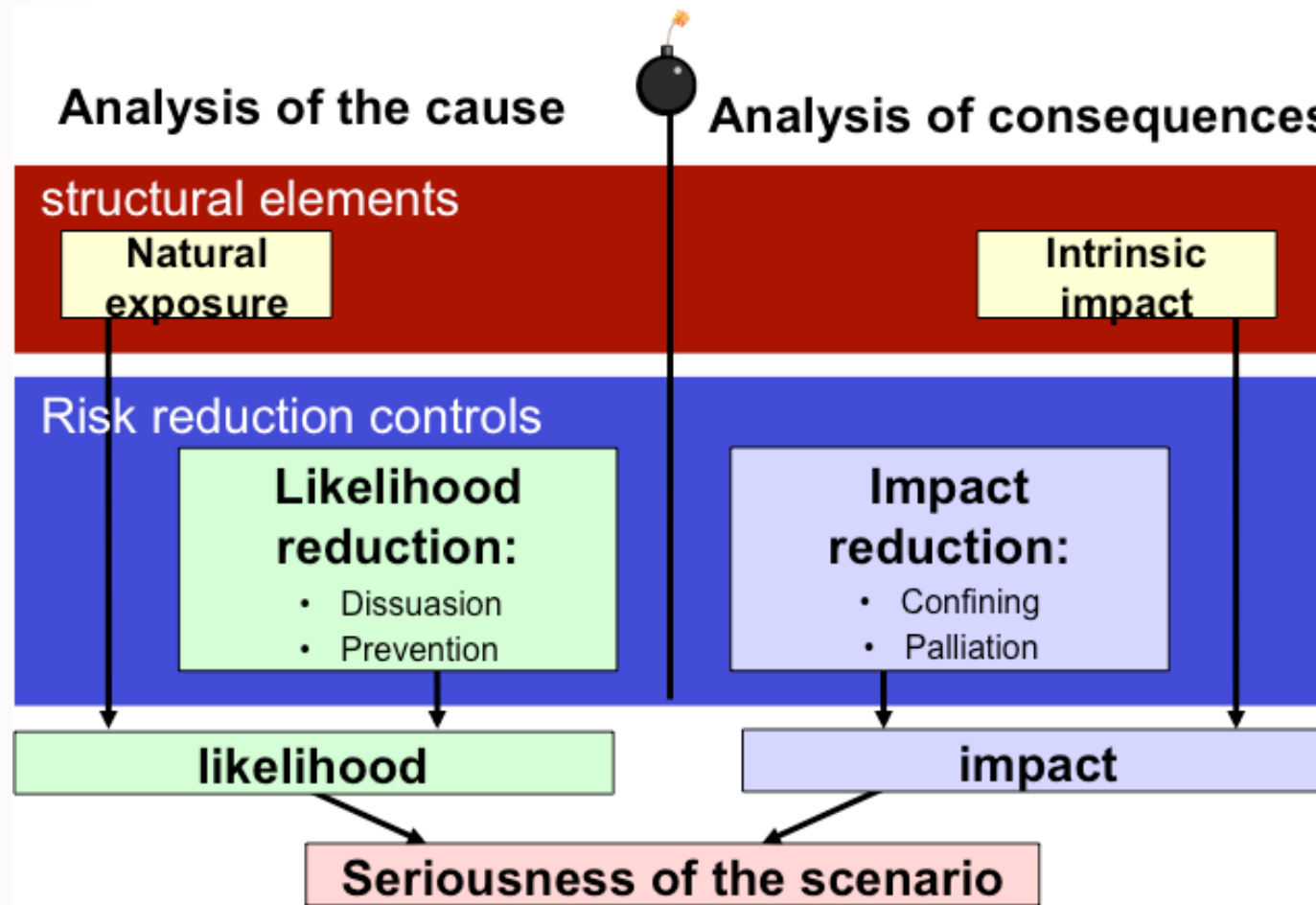
Risk assessment requires a risk model and this model must be suited to the objectives decided for the management of the risks.

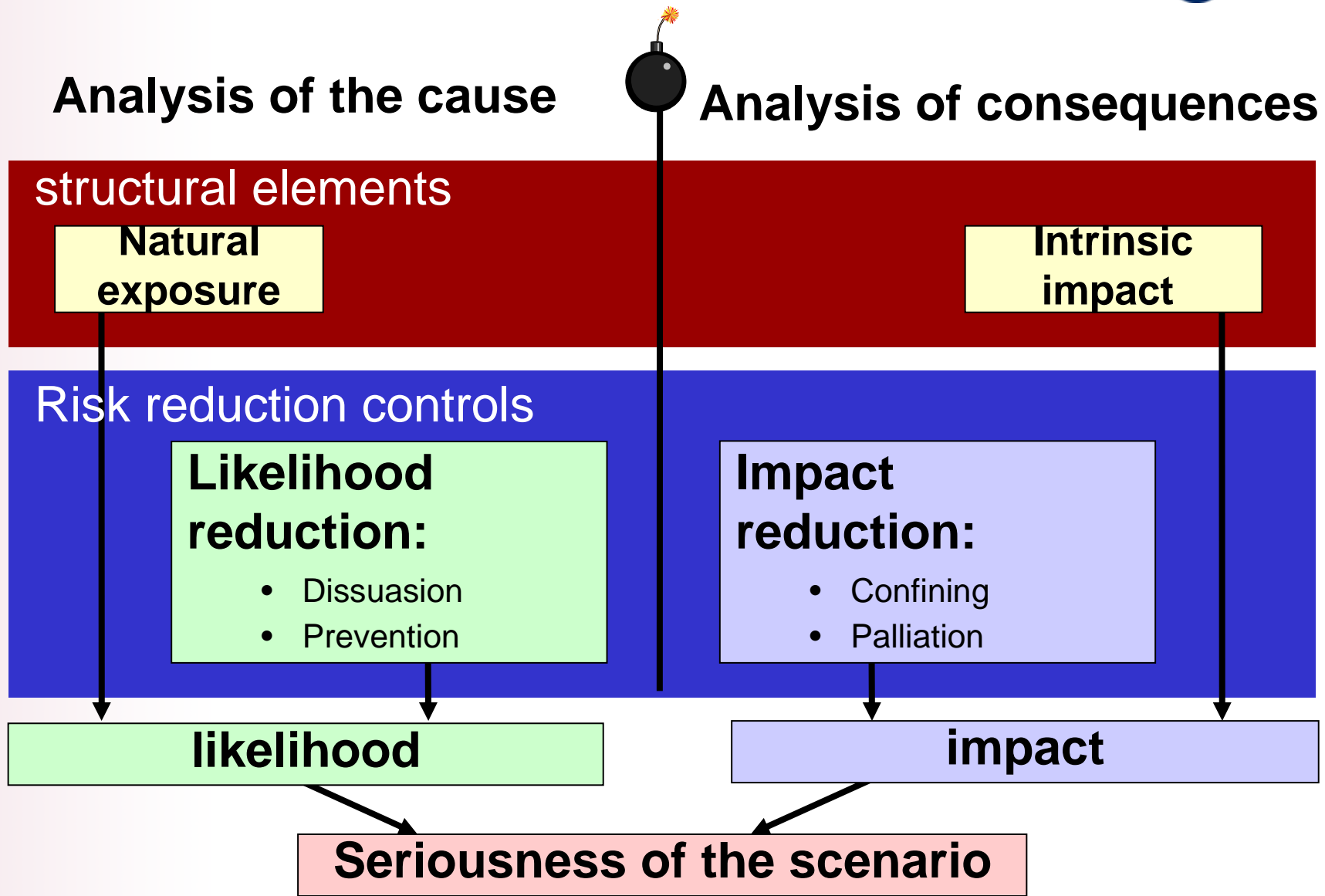
MEHARI, being a risk management method, imposes a model that considers:

- **Structural factors** attached to the type of activity and the context of the enterprise
- **The security controls implemented**
- **The quality of these controls**

Risk assessment

The risk model of MEHARI follows the schema below since its origin (the transfer of risk is now part of the treatment phase).





Risk management

The direct and individual management of risk imposes

- to use a model of risk
- the setting of objectives such as
 - security controls to improve
 - target levels of quality for the controls

and to be able to measure the achievement of these objectives.

This is hardly conceivable without a knowledge base comprising an audit base for the security

All the reflections developed by MEHARI for risk management, resulting from the decided additional objectives have led to the setting of fundamental principles and functional specifications.

MEHARI 2010 includes a document listing these principles and specifications.

Summary

- Manage your risks using ISO 27005 and MEHARI 2010
- ➔ ● The knowledge base of MEHARI 2010
- Patterns and quantification functions
- Synthesis of MEHARI 2010 new features
- Open Source Distribution of MEHARI

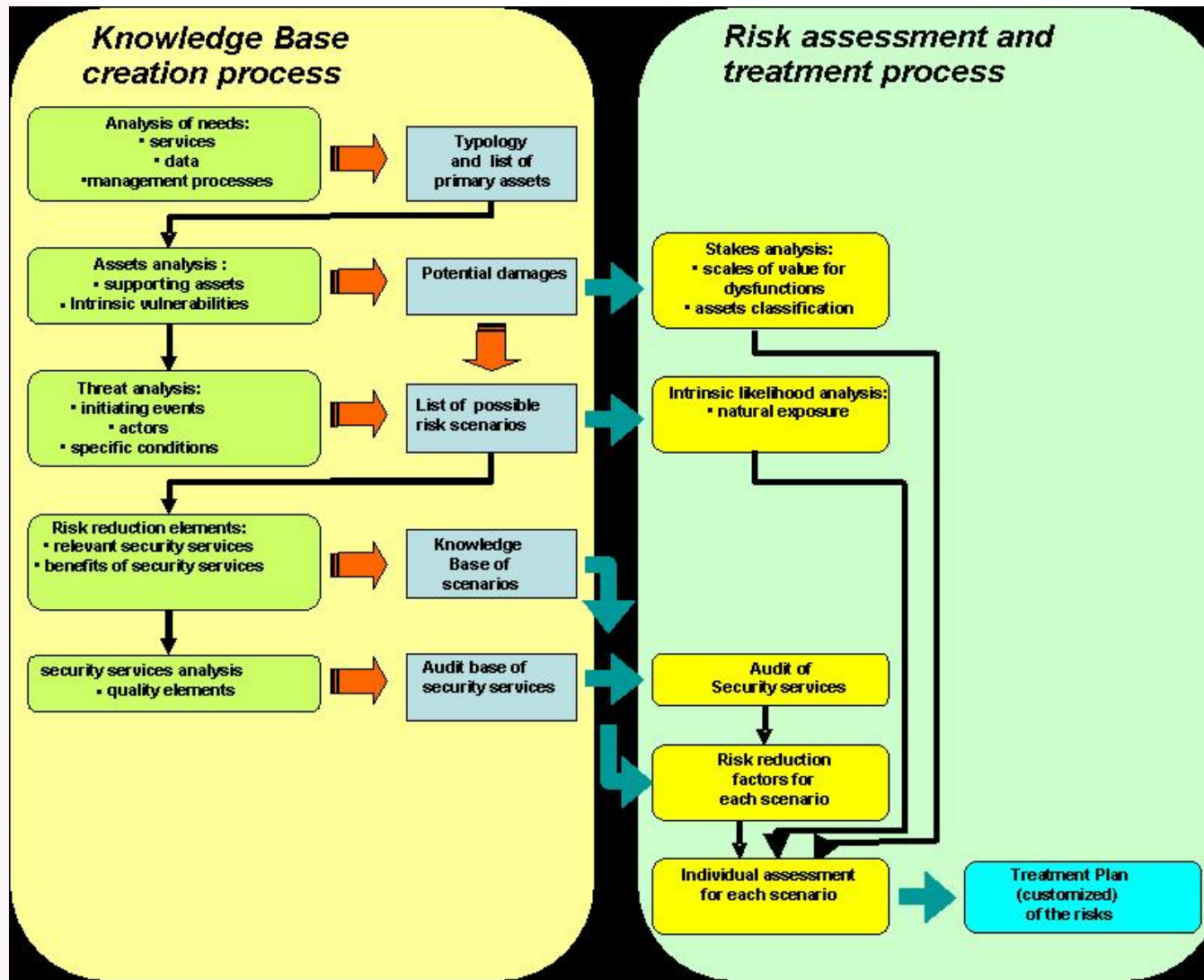
Mehari knowledge base

The inclusion of sub-bases for:

- Risk situations (or scenarios): is an opportunity
- security services (or controls): is a necessity
- the assessment of risk situations: is a necessity

Document the conditions for
creating and maintaining such a base: is a bonus

The risk management process



Development of a base for risk scenarios

The management of risk includes a risk identification step which is facilitated by the availability of a base of risk scenarios (or risk situations).

Thus the development of this comprehensive base within the method is a real opportunity.

Development of a knowledge base of security services

It is necessary to reference controls in the risk assessment phase and this leads to develop a base of security services associating homogeneous controls.

In order to assess the quality level of the security services, this knowledge base shall permit analysis capabilities according to several criteria.

A knowledge base for the assessment of risk scenarios

When the seriousness of a risk scenario may be reduced thanks to several security services, a risk model, even effective, is not sufficient:

- The mechanisms of risk assessment according to the quality level of several relevant security services cannot be guessed in midair.
- Sharing of expertises and further thought are guaranties of quality.
- Return of experience is efficient only with a shared base.

A knowledge base for the assessment of risk scenarios

The large number of risk situations and security services leads to the **necessity** to use a knowledge base of risk scenarios

This implies:

- Clarified constitution principles
- The capability to enrich and develop the base itself.

CLUSIF and the knowledge bases for risk management

CLUSIF has developed experience and competency in the development of a risk management knowledge base.

This experience has been confirmed with MEHARI 2010.

CLUSIF will provide a knowledge base development guide dealing with specific contexts or the management of risks other than related to information systems.

Such a guide answers to a necessity.

Summary

- Manage your risks using ISO 27005 and MEHARI 2010
- The knowledge base of MEHARI 2010
- ➔ ● Patterns and quantification functions
- Synthesis of MEHARI 2010 new features
- Open Source Distribution of MEHARI

Calculation functions are necessary

The risk model imposes calculation functions for the quantification of the level of risks, such as:

- Quality level of the security services
- Factors influencing risk reduction
- Combination of the effects of several services or influencing factors.
- Assessment of the risk's parameters
- Assessment of the risk's seriousness

A reasoned confidence

The calculation capacities of the method may give a false impression of good precision:

- Several parameters, necessary for the calculations, are estimates and not scientific elements
- The formulas themselves are reasonable and rational but no 100% accuracy is guaranteed.

Anyway, as for any analysis process, the calculation models allow to split up a complex problem into simpler elementary problems.

The models aid to the reasoning and the decision processes.

A reasoned confidence

The confidence about the models which adopt a cautious approach in the build-up of the knowledge base is reinforced by:

- Consideration of the hardiness and the permanent checking of the quality level of each security service.
- Consideration of only those security services whose effect on risk reduction is guaranteed.
- Cautiousness in the decision grids used.

Implementation advice

The calculation automatism remain essential, even mandatory, helpers, for:

- Preselecting risk reduction action plans
- Underscoring the remaining risks, once corrective actions have been decided or installed.
- Simulating the effect of the controls decided concerning the resulting level of risk.
- Piloting the security of information through risk management.

The automatism are integrated in the Excel and Open Office knowledge bases

Examples of Mehari worksheet result

Results for the quality of the security **services** (with mention of the audit schema variants)

| SECURITY SERVICES & SUB-SERVICES | | | | | | | | | | | | |
|---------------------------------------------|------------------------------------------------------------------------------------------------------|--|----------------------------------------|-----|-----|----|----|-----|-----|-----|--|--|
| DOMAINS | | | Objective values to be handled (if 1): | | | | | | | 1 | | |
| SERVICES | | | | | | | | | | | | |
| SUB-SERVICES | | | Theme | | | | | Min | Obj | Fin | | |
| 01 Organization of security | | | | V1 | V2 | V3 | V4 | | | | | |
| 02 Sites security | | | | V1 | V2 | V3 | V4 | | | | | |
| 02A | Physical access control to the site and the building | | | | | | | | | | | |
| 02A01 | Management of access rights to the site or building | | B1 | 2,0 | 2,0 | | | 2,0 | | 2,0 | | |
| 02A02 | Management of access authorizations granted to the site or the building | | B1 | 2,8 | 2,8 | | | 3,0 | | 3,0 | | |
| 02A03 | Access control to the site or the building | | B1 | 2,0 | 1,0 | | | 1,0 | | 1,0 | | |
| 02A04 | Intrusion detection to the site or the building | | B1 | | | | | 1,0 | | 1,0 | | |
| 02A05 | Access to the loading and unloading areas (goods receipt and consignment) or to areas open to public | | B1 | X | 1,3 | | | 1,0 | | 1,0 | | |

Examples of Mehari worksheet result

Panorama of the risks per asset type and seriousness (Risk%asset)

| Panorama of scenarios' seriousness level | | Availability | | | | Integrity | | | | Confidentiality | | | | | |
|------------------------------------------|---------------------------------------------------------------------------------|--------------|------|------|------|-----------|------|------|------|-----------------|------|------|------|----|---|
| | | S. 1 | S. 2 | S. 3 | S. 4 | S. 1 | S. 2 | S. 3 | S. 4 | S. 1 | S. 2 | S. 3 | S. 4 | | |
| Data and information assets | | | | | | | | | | | | | | | |
| <i>Data and information</i> | | | | | | | | | | | | | | | |
| D01 | Data files and data bases accessed by applications | 0 | 38 | 1 | 1 | > | 1 | 0 | 15 | 0 | > | 20 | 0 | 0 | 0 |
| D02 | Shared office files and data | 0 | 22 | 1 | 0 | > | 0 | 9 | 0 | 0 | > | 0 | 0 | 18 | 0 |
| D03 | Personal office files (on user work stations and equipments) | 0 | 25 | 1 | 0 | > | 0 | 7 | 0 | 0 | > | 0 | 0 | 17 | 0 |
| D04 | Written or printed information and data kept by users and personal archives | 0 | 0 | 10 | 0 | > | | | | | | 0 | 0 | 12 | 0 |
| D05 | Listings or printed documents | | | | | | | | | | | 7 | 0 | 0 | 0 |
| D06 | Exchanged messages, screen views, data individually sensitive | 6 | 0 | 0 | 0 | > | 0 | 14 | 0 | 0 | > | 14 | 0 | 0 | 0 |
| D07 | electronic mailing | 9 | 0 | 0 | 0 | > | 3 | 0 | 0 | 0 | > | 0 | 0 | 4 | 0 |
| D08 | (Post) Mails and faxes | 14 | 0 | 0 | 0 | > | 0 | 1 | 0 | 0 | > | 0 | 0 | 7 | 0 |
| D09 | Patrimonial archives or documents used as proofs | 10 | 0 | 0 | 0 | > | | | | | | 4 | 0 | 0 | 0 |
| D10 | IT related Archives | 18 | 0 | 0 | 0 | > | 5 | 0 | 0 | 0 | > | 3 | 0 | 0 | 0 |
| D11 | Data and information published on public or internal sites | 23 | 0 | 0 | 0 | > | 9 | 0 | 0 | 0 | > | | | | |
| Service assets | | | | | | | | | | | | | | | |
| <i>General Services</i> | | | | | | | | | | | | | | | |
| G01 | User workspace and environment | 0 | 0 | 2 | 2 | > | | | | | | | | | |
| G02 | Telecommunication Services (voice, fax, audio & videoconferencing, etc.) | 0 | 18 | 0 | 0 | > | 6 | 0 | 0 | 0 | > | | | | |
| <i>IT and networking Services</i> | | | | | | | | | | | | | | | |
| R01 | Extended Network Service | 27 | 0 | 0 | 0 | > | 5 | 0 | 0 | 0 | > | | | | |
| R02 | Local Area Network Service | 0 | 0 | 17 | 10 | > | 5 | 0 | 0 | 0 | > | | | | |
| S01 | Services provided by applications | 0 | 0 | 33 | 31 | > | 0 | 18 | 0 | 0 | > | 16 | 0 | 0 | 0 |
| S02 | Shared Office Services (servers, document management, printers, etc.) | 61 | 0 | 0 | 0 | > | 0 | 0 | 9 | 0 | > | | | | |
| S03 | Users' disposal of Equipments (workstations, local printers, peripherals, etc.) | 11 | 1 | 0 | 0 | > | | | | | | | | | |
| S04 | Common Services, working environment: messaging, archiving, print, editing | 62 | 0 | 0 | 0 | > | 9 | 0 | 0 | 0 | > | | | | |
| S05 | Web editing Service (internal or public) | 0 | 0 | 0 | 0 | > | 0 | 0 | 0 | 0 | > | | | | |

Examples of Mehari worksheet result

Selection of action plans for risk treatment (partial display)

| | | | | | | | | | | | | | | |
|---------------------|---------------------------------------------------------|-----|-----|-----|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|----------|---------------------|---------------|--------------|---------------------|---------------|--------------|
| Action plans | | | | | | <p style="color: red;">If 0 in the opposite cell, the intrinsic seriousness of the scenarios will be considered → 1</p> <p style="color: red;">If 1 in the opposite cell, the current seriousness of the scenarios will be considered → 1</p> | | | | | | | | |
| Family of scenarios | Number of scenarios | | | | | <p style="color: red;">If 1 in the opposite cell, the reduced seriousness from the completion of projects (Obj_projects) or selected plans (1 in the "Decision" row below) will be considered → 1</p> | | | | | | | | |
| | S 1 | S 2 | S 3 | S 4 | Tot | Measures needing improvement | Type of plan | Decision | Services to improve | Current level | Target level | Services to improve | Current level | Target level |
| R02-A | Unavailability of the local area network service | | | | | | | | | | | | | |
| | 0 | 0 | 17 | 10 | 27 | Deterrence : Plan of type A | | | 03B06 | 1 | 3 | 06C02 | 1 | 3 |
| | | | | | | Prevention : Plan of type A | | | 02A01 | 2 | 4 | 02A02 | 3 | 4 |
| | | | | | | Prevention : Plan of type A | | | 03A01 | 1 | 4 | 03A02 | 1 | 4 |
| | | | | | | Prevention : Plan of type A | | | 05D01 | 1 | 4 | 06A02 | 1 | 4 |
| | | | | | | Confining : Plan of type A | | | 02A04 | 1 | 4 | 03B04 | 1 | 4 |
| | | | | | | Palliation : Plan of type E | | | 01C02 | 1 | 3 | 01E01 | 1 | 3 |
| | | | | | | Palliation : Plan of type A | | | 03A02 | 1 | 3 | 03A06 | 1 | 3 |

Examples of Mehari worksheet result

Analysis and decision process for each scenario (partial display)

| DESCRIPTION | Consideration of Security services if 1 : | | | | | | | | | | | | | 1 | | Accept (A) or transfer (T) | | |
|----------------------------------------------------------------------------------------------------------------------|-------------------------------------------|----------|-----------|------------------|----------|-------------|-------------------|------------|-----------|------------|----------------|--------|-------------------|--------|------------|----------------------------|-------------|---|
| | Direct Selection | Type AEM | Type AICE | Intrinsic values | | | security measures | | | | decided values | | calculated values | | | | | |
| | | | | Impact | Exposure | seriousness | Dissuasion | Prevention | Confining | Palliation | Confinability | Impact | Likelihood | Impact | Likelihood | | seriousness | |
| | | | | | | | | | | | | | | | | | | |
| Accidental erasure of files of data, due to a production incident | 1 | A | A | 2 | 3 | 2 | 1 | 1 | 1 | 3 | 1 | 4 | | 2 | 3 | 4 | | T |
| Erasure, due to an error, of files of data, by a user authorized legitimately, connected from the internal network | 1 | E | A | 2 | 3 | 2 | 1 | 1 | 1 | 3 | 0 | | 4 | 2 | 3 | 3 | | A |
| Erasure, due to an error, of files of data, by a user authorized illegitimately, connected from the internal network | 1 | E | A | 2 | 3 | 2 | 1 | 1 | 1 | 3 | 0 | | | 2 | 3 | 2 | | |

Summary

- Manage your risks using ISO 27005 and MEHARI 2010
- The knowledge base of MEHARI 2010
- Patterns and quantification functions
- ➔ ● Synthesis of MEHARI 2010 new features
- Open Source Distribution of MEHARI

Evolution of the risk scenarios

Description of the primary assets:

Data, services, processes

Asset classification process revised for Mehari 2010

Structuring and description of the scenarios

asset + damage: vulnerability,

event, circumstances, actor: threat

groupings by family: asset and type damage

Use of tools for the selection of scenarios

Evolution of the “security services” base

Domains of security:

New: Working environment, Archives, ISMS, Telecom

Visualisation of audit variants

Classification of the controls: efficiency, robustness, permanence

➔ adaptation to the maturity level of the organisation

Evolution of the risk model

Risk assessment

recovery controls (e.g. insurance) handled as “transfer of risk” (like for ISO 27005)

➔ simplification of risk assessment

Assistance for risk management

Synthesis of risks ordered by seriousness levels

for each family of assets

for each type of threat

Treatment plans

plans proposed based on their efficiency level

assistance for the choice of planned projects (including termination date)

Summary

- Manage your risks using ISO 27005 and MEHARI 2010
- The knowledge base of MEHARI 2010
- Patterns and quantification functions
- Synthesis of MEHARI 2010 new features
- ➔ ● Open Source Distribution of MEHARI

Benefits of Open source distribution?

1 + CLUSIF = not for profit association!

2 + lighter distribution mechanism

Consequences for the image of Mehari ?

3 + Mehari is now a recognised method

30.000 downloads in 4 years,

international image: 150+ countries

4 + many voluntary translations: Spanish, German, Italian, ...

5 + added capacity to exchange on **mehari.info**

6 + enhanced international image of CLUSIF

Benefits from the free distribution

Downloads are 100 times more often than for previous versions.

Creation of new CLUSI (Burkina, Quebec, Ivory coast)

English bases downloads represent 15% of total

Mehari training (Quebec, Ivory coast)

Improved worldwide image of CLUSIF.

Multinational contacts and translations



Thank you