METHODS

MEHARI 2010

Changes from previous versions

August 2010

Methods Commission

Please post your questions and comments on the forum:

http://mehari.info/

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11, rue de Mogador, 75009 PARIS

Tél.: +33 1 53 25 08 80 – Fax: +33 1 53 25 08 88 – e-mail: clusif@clusif.asso.fr

Web : http://www.clusif.asso.fr

Acknowledgments

The CLUSIF would like to thank specially Jean-Philippe Jouas for his outstanding contributions and the members of the Methods commission who participated to the realization of this document

The English translation has been managed by Jean-Louis Roule and Jean-Philippe Jouas.

This document describes the changes in MEHARI version 2010 compared with the previous version (MEHARI 2007).

The general direction of the changes was to bring MEHARI into conformity with the ISO/IEC 27005: 2008 standard, together with a desire to clarify the principles and the clear positioning of MEHARI as a method for managing risks.

1. Positioning MEHARI

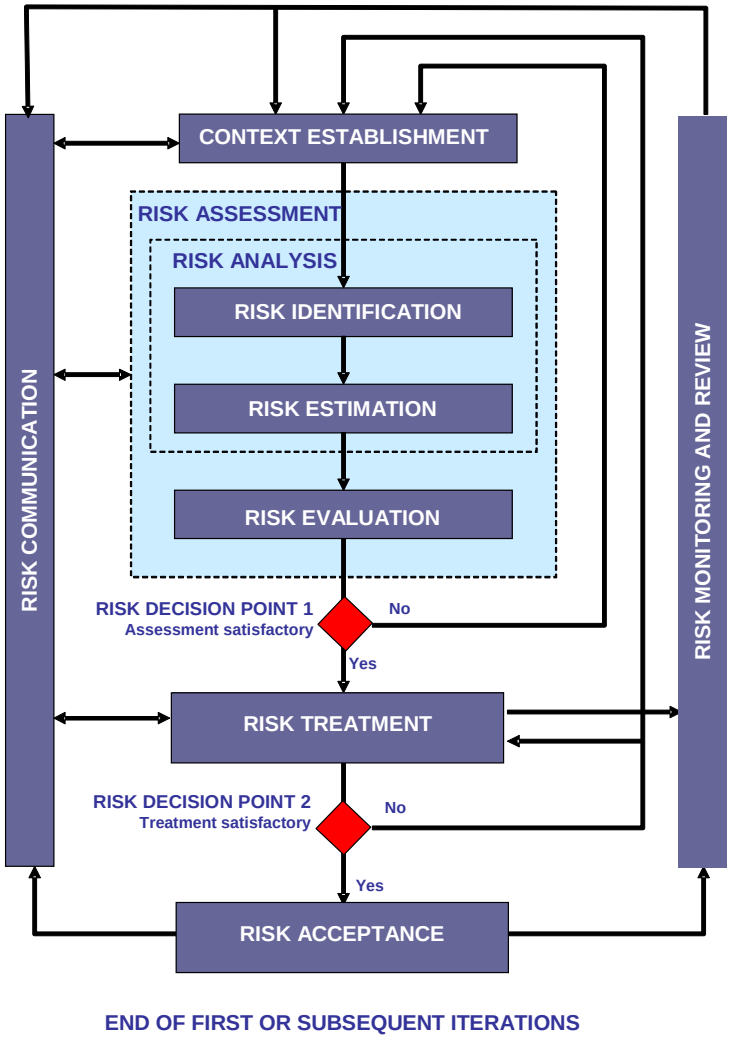
MEHARI has always been developed as a method of managing risks in a business or any other sort of organization, but also as a toolbox that can be used by Information Security Officers for managing information security.

While maintaining this specific objective, MEHARI 2010 is clearly positioned as a general method for the analysis and management of risks, with situations described by means of risk scenarios.

The ability to manage risks directly and individually has therefore become one of the basic principles of the method, and this has direct consequences, as described in this document.

2. Conformance with the ISO/IEC 27005 standard

The general diagram presented in the ISO/IEC 27005 standard and reproduced here is taken from the previous standard, ISO 13335, which was the original reference for MEHARI.



In addition to the standard, the description of the risk in terms of the assets, vulnerabilities and threats must be taken into account.

The points above have various consequences, which are integrated into MEHARI 2010 and described below.

2.1 Handling of recovery measures and transfer of risks

To comply completely with the standard, it was decided to move risk transfer into the risk treatment phase.

Recovery measures have therefore been entirely removed from the formulas for risk reduction.

Auditing questions relating to insurance are however retained, and handled as general measures.

In consequence, the decision tables have been modified: the residual impact is deducted directly from the intrinsic impact and from the effectiveness of containment (or confinement) and palliation measures (the STATUS-RI indicator is therefore removed).

2.2 Describing assets

The definition of assets given by ISO/IEC 27005 (section 8.2.1.2) is as follows:

"An asset is anything that has value to the organization and which therefore requires protection. For the identification of assets it should be borne in mind that an information system consists of more than hardware and software".

Annex B of the standard gives more detail:

"To perform asset valuation, an organization first needs to identify its assets (at an appropriate level of detail). Two kinds of assets can be distinguished:

- *The primary assets:*
    - *Business processes & activities*
    - *Information*
- *The supporting assets (on which the primary elements of the scope rely) of all types:*
    - *Hardware*
    - *Software*
    - *Network*
    - *Personnel*
    - *Site*
    - *Organization's structure"*

MEHARI distinguishes the following **primary assets**:

- Services (also cited as types of asset in ISO 27000)
- Data
- Management Processes

These items clearly meet the main idea of the standard to give priority to the fundamentals of the organization, and they better match the idea of **needs** that must be protected.

Each business activity is an entry point but not a need in itself. Conversely, the services required to engage in the business activity are clearly needs, as is the data (including its history) that is required for service implementation.

The addition of management processes at this level is necessary to handle non-conformity to regulations, laws, and frameworks imposed.

It is of course necessary to describe the materialization of these primary assets, in order to address their vulnerabilities.

MEHARI 2010 introduces the concept of **secondary** or **supporting assets.**

It is necessary to describe all contingencies that could affect the primary assets (particularly services) and all the forms that these assets can take (particularly for data).

Note, in particular, that the idea of contingency reveals aspects that would otherwise remain hidden, such as access means to services (user accounts), methods of accessing data (decryption keys), external suppliers, etc.

Note also that these options allow highlighting the differences between, say, live data, archived data, or data published on websites.

Given these definitions, the tables describing assets and their classification have therefore been modified in MEHARI 2010.

2.3 Describing vulnerabilities

The notion of vulnerability is described in the ISO/IEC 27000 standard as follows:

"*Weakness of an **asset** or a security **measure** (control) that can be exploited by a **threat**.*"

This definition contains two clearly different aspects:

- Inherent characteristics of an asset that could be exploited by a threat,
- Weaknesses in security measures.

Therefore, when seeking to identify new risks (or simply all the risks that confront an organization), which is an important step in the analysis and management of risks, starting from the weaknesses in the security measures assumes that these measures are well defined, which is not the case for new or emergent risks.

In contrast, the notion of vulnerability, taking its most basic meaning, is useful if not indispensable, and was already used without being obvious in MEHARI previous versions to develop and describe risk scenarios.

To avoid ambiguity, MEHARI 2010 introduces two different definitions of vulnerability:

- An **inherent vulnerability** is an inherent characteristic of an asset that can be exploited by a threat.
- A **contextual vulnerability** is a weakness in a security measure that can be exploited by a threat.

Identification of risks is based exclusively on inherent vulnerability, whereas contextual vulnerabilities have a role in risk assessment.

MEHARI 2010 knowledge base has been created based on these definitions and the set of scenarios precisely describe the inherent vulnerability exploited in each scenario.

2.4 Describing threats

The concept of a threat required also further clarification.

MEHARI 2010 introduces a formal definition of a threat, containing the following elements:

- A trigger event
- The circumstances of occurrence, including various aspects:
  - Location of occurrence,
  - Time or time period of occurrence,
  - Phase or step in a process,
- The type of actor.

These elements have always been present in MEHARI risk scenarios, but they were not formalized and they were only mentioned in the title of the scenario. They are now clearly indicated in the specific columns of the scenarios tab.

Note that these various aspects are often the key points for evaluating the likelihood of a risk scenario, and that their presence in the definitions supports the objective of individual analysis of each risk situation and its risk level.

Note: The table of natural exposure has been moved to the "Expo" tab of the knowledge base, and is called "Table of events: types and natural exposure".

2.5 Identifying and describing risk scenarios

The description of a risk scenario in MEHARI 2010 is highly structured, and contains:

- The type of primary asset (which corresponds to an entry in the table of intrinsic impacts), specified by the criterion attained:
- An **intrinsic vulnerability**, described by:
  - The type of secondary asset
  - The type of damage
- A threat type, described by:
  - A trigger event
  - The circumstances of location, time, or process
  - The type of actor
- A title enabling the scenario to be understood using a global description of the above elements.

3. Developments in several analysis procedures

The experiences and comments of practitioners of the method have led to a number of developments, which are described below.

3.1 Developments in measures to limit direct impact

These measures, previously known as protection measures, are of two types:

- Mechanisms intended to interrupt a progressive disaster (fire, propagating error, etc.) by detection and reaction measures,
- Mechanisms aimed at limiting the impact of a scenario, whether progressive or not, such as fragmentation measures, limiting the degrees of freedom of certain variables, etc.

Moreover, in this second case, for scenarios for which there are no possible palliative measures, the decision matrices previously used presented some difficulties.

To address these observations, MEHARI 2010 introduces the following developments:

- **Protection measures are now called containment measures (encompassing the various aspects described above).**
- **The scenarios previously defined as non-progressive are now called non-containable.**
- **An additional table for containable scenarios without palliative measures has been created.**

3.2 Distinguishing between individually sensitive data and data sets

The distinction between isolated data and data sets had been used only for application screens or for data transmission and mainly for confidentiality. Now MEHARI 2010 considers that the classification of data itself may reveal a difference in impact, whichever criteria, between an attack on one or more isolated data and an attack on a data set.

Individually sensitive data are therefore considered by MEHARI 2010, as a specific class of primary asset (D06).

They are therefore classified and presented in the relevant tables (T1 and intrinsic impact).

3.3 Handling "progressive" confidentiality scenarios

The previous knowledge base contained a number of scenarios of attacks on confidentiality considered to be "progressive" (such as *repeated copying of a file*), with possible containment measures intended to reduce the impact. The problem resulted from that it was not possible to say whether the intrinsic impact of revealing the content of a data file (in this example) had been evaluated for repeated copying or a single disclosure of the file (at least when the intrinsic impact is assessed from the classification).

It has been therefore considered wiser to modify the corresponding scenarios to address copying of a file (without the notion of repeated copying) and to consider such scenarios to be non-progressive (which leaves the option of considering later this point, supposing that containment

measures may have an effect, while declaring the scenario as being non-progressive and non-containable).

Scenarios of attack on confidentiality are always considered non-containable.

3.4 Handling integrity scenarios

Analyzing scenarios of attacks on integrity, in practice, reveals several types of scenario:

- Scenarios of loss of the integrity of a database or file for which, after the loss is detected, the palliative measures consist of repairing the damaged database or file in order to restart with clean data. Such scenarios might or might not be progressive (and containable).
- Fraud scenarios for which there are almost no palliative measures, and which are typically not progressive (the maximum impact is reached the instant the fraud action takes place) but for which there are measures to limit the direct impact (permanent monitoring, detection thresholds, etc.). Such scenarios are considered to be containable.
- Certain scenarios of errors or accidents having the same consequences as a fraud, that is, a containable impact but no palliative measures are possible.

Scenarios of the first type described above are, in fact, similar to loss of availability scenarios: the initial cause being a loss of integrity but as soon as this is identified, it is comparable to a loss of availability problem.

These scenarios are known as "Massive Data Pollution" and are now treated like scenarios of loss of availability.

In contrast, for loss of integrity scenarios by fraud or equivalent (the second and third types described above), the loss of integrity is considered to be undetected and there is therefore no service or palliative measure to reduce the impact. However, containment measures are possible.

Loss of Integrity scenarios are considered containable but there are, in general, no suitable palliative measures.

The impact evaluation table for integrity scenarios is retained (for the cases where palliative measures are applicable) and aligned with the table of containable scenarios.

The scenarios for loss of integrity by fraud on individually sensitive data can also be addressed by referencing data type D06 rather than D01 or D02, while database pollution scenarios continue to reference D01 data.

3.5 Performance degradation scenarios

The concept of performance degradation is difficult to quantify in terms of impact.

The "performance degradation scenarios" have been replaced by "overload scenarios".

4. Development of the knowledge base

4.1 Developments in the set of scenarios

The set of scenarios has been completely revisited allowing a comprehensive analysis of the possible combinations of primary and secondary assets, types of vulnerability, and types of threat (see section 2.5).

The number of scenarios in MEHARI 2010 knowledge base is now approximately 800.

Each scenario is defined in terms of the characteristic elements.

4.2 Developments in the audit questionnaires

The audit questionnaires have been revised, with three objectives:

- Clarify the questions that seemed to require 2 answers or ambiguous.
- For each question, indicate the type of question and the level of expertise, to enable construction of different questionnaires suitable to the level of advancement and expertise of an organization.
- Replace terms that could be misinterpreted or misunderstood in Quebec.
- Revise the weighting of some questions.

The following new domains have also been added:

- A domain specific to management of the set of users' equipment
- A domain specific to telecommunications operation
- A domain for non-conformities to the management processes (replacing the previous legal domain)
- A domain for the information security management system (ISMS)

The new audit base now contains:

- 14 domains
- Approximately 300 security services

Note: Some weightings have been revised, so the results of diagnostics made using MEHARI 2010 knowledge base may differ from those made with the previous version.

4.3 Calculation functions included in the knowledge base

Functions for calculation and simulation (using Excel or Open Office) have been included:

- Calculation of the quality of the security services
- Calculation of risk reduction factors (as a function of the quality of the security services)
- Calculation of the intrinsic seriousness and residual seriousness of scenarios
- Options to simulate selection of security action plans and see a projection of the outcome of the selected plans on the (expected) level of residual seriousness of the scenarios.

THE SPIRIT OF EXCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11, rue de Mogador
75009 Paris
✆ 01 53 25 08 80
clusif@clusif.asso.fr

Load CLUSIF productions from

www.clusif.asso.fr