



MEHARI 2007  
Risk Analysis Guide

April 2007



Methods Commission

\* MEHARI is a trademark registered by the CLUSIF

---

**CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS**

30, rue Pierre Semard, 75009 PARIS, FRANCE  
Tel. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88

e-mail : [clusif@clusif.asso.fr](mailto:clusif@clusif.asso.fr) - Web : <http://www.clusif.asso.fr>

# Contents

|         |   |    |
|---------|---|----|
| 1.      | Introduction.....   | 2  |
| 2.      | Analysis of risk situations and use of Mehari automated procedures.....                 | 3  |
| 2.1.    | Review of the risk analysis process .....   | 3  |
| 2.2.    | Evaluation of natural exposure.....   | 4  |
| 2.2.1   | Standard natural exposure.....  | 4  |
| 2.2.2   | Enterprise-specific natural exposure for a given risk.....                              | 4  |
| 2.3.    | Evaluation of intrinsic impact.....   | 4  |
| 2.3.1   | The intrinsic impact table .....  | 5  |
| 2.3.2   | Extending the intrinsic impact table .....  | 5  |
| 2.3.3   | Evaluating intrinsic impact of scenarios .....  | 6  |
| 2.3.4   | Cartographic decomposition .....  | 6  |
| 2.4.    | Evaluating risk reduction factors through a MEHARI security audit.....                  | 6  |
| 2.4.1   | Efficiency indicators for security services by scenario and risk reduction measure..... | 7  |
| 2.4.2   | “Calculated” risk reduction factors.....  | 8  |
| 2.4.3   | Evaluating risk factors .....   | 9  |
| 2.5.    | Evaluation of potentiality and impact .....   | 9  |
| 2.5.1   | Automated potentiality evaluation: STATUS-P .....                                       | 9  |
| 2.5.2   | Automated impact evaluation: STATUS-I .....   | 9  |
| 2.5.2.1 | Impact reduction evaluation: STATUS-RI.....   | 9  |
| 2.5.2.2 | Impact evaluation: STATUS-I .....   | 10 |
| 2.5.3   | Evaluation table construction principles.....   | 10 |
| 2.5.4   | Evaluating potentiality and impact .....  | 10 |
| 2.6.    | Evaluating the seriousness of a scenario .....  | 11 |
| 2.7.    | Expressing security requirements.....   | 11 |
| 2.8.    | Practical advice.....   | 11 |
| 2.8.1   | The thinking behind the risk analysis approach.....                                     | 11 |
| 2.8.2   | Composition of a risk evaluation committee .....  | 11 |
| 2.8.3   | Using the approach in conjunction with a security audit .....                           | 11 |
| 3.      | Identification of risk situations .....   | 12 |
| 3.1.    | Systematic identification using the knowledge base .....                                | 12 |
| 3.2.    | Creating a specific scenario base .....   | 12 |
| 3.2.1   | The generic risk scenario base .....  | 13 |
| 3.2.2   | Customizing scenarios as a function of the assets involved .....                        | 13 |
| 3.2.3   | Taking specific security solutions into account .....                                   | 14 |
| 3.3.    | Automatic evaluation of scenarios .....   | 14 |
| 3.4.    | Selecting critical scenarios that should be considered during risk analysis .....       | 14 |

## Table of figures

|   |    |
|---|----|
| Figure 1: The risk analysis process and the assistance provided by MEHARI ..... | 3  |
| Figure 2: Identification of risk situations .....                               | 12 |

# 1. INTRODUCTION

---

An overview of the principles of risk analysis and the identification of risk situations is given in the document “*MEHARI – Concepts and Mechanisms*”. The main points are recalled below:

- A risk situation can be characterized by its intrinsic potentiality and impact, in the absence of any security measures.
- Intrinsic potentiality and intrinsic impact can be evaluated.
- Security measures can be applied to reduce intrinsic risk through significant risk reduction factors.
- These risk reduction factors can be evaluated.
- On the basis of these elements, it is possible to evaluate residual potentiality and impact, which are the characteristics of risk; and thereby deduce a risk level indicator.
- MEHARI provides tools to assist all through the analysis and evaluation process.

Analysis of a risk situation can be made directly using the general principles and explanations provided in the document “*MEHARI – Concepts and Mechanisms*”.

If the risk situation that is being analyzed corresponds to one of the scenarios held in the MEHARI knowledge base, it is also possible –for a direct evaluation of the level of risk – to use the “*Risk Scenario Reference Manual*”. The document provides, for each scenario, specific indications about the risk reduction factors.

In this document we describe how the MEHARI automated procedures should be used to assist in evaluating a risk situation. Examples that are used will be ones where the situation being analyzed corresponds to a scenario in the MEHARI knowledge base.

We shall also describe how to use the automated procedures to highlight risk situations and to select them for detailed analysis.

## 2. ANALYSIS OF RISK SITUATIONS AND USE OF MEHARI AUTOMATED PROCEDURES

### 2.1. Review of the risk analysis process

Figure 1, below, shows the overall process for risk analysis, as already described in the document "MEHARI – Concepts and Mechanisms".

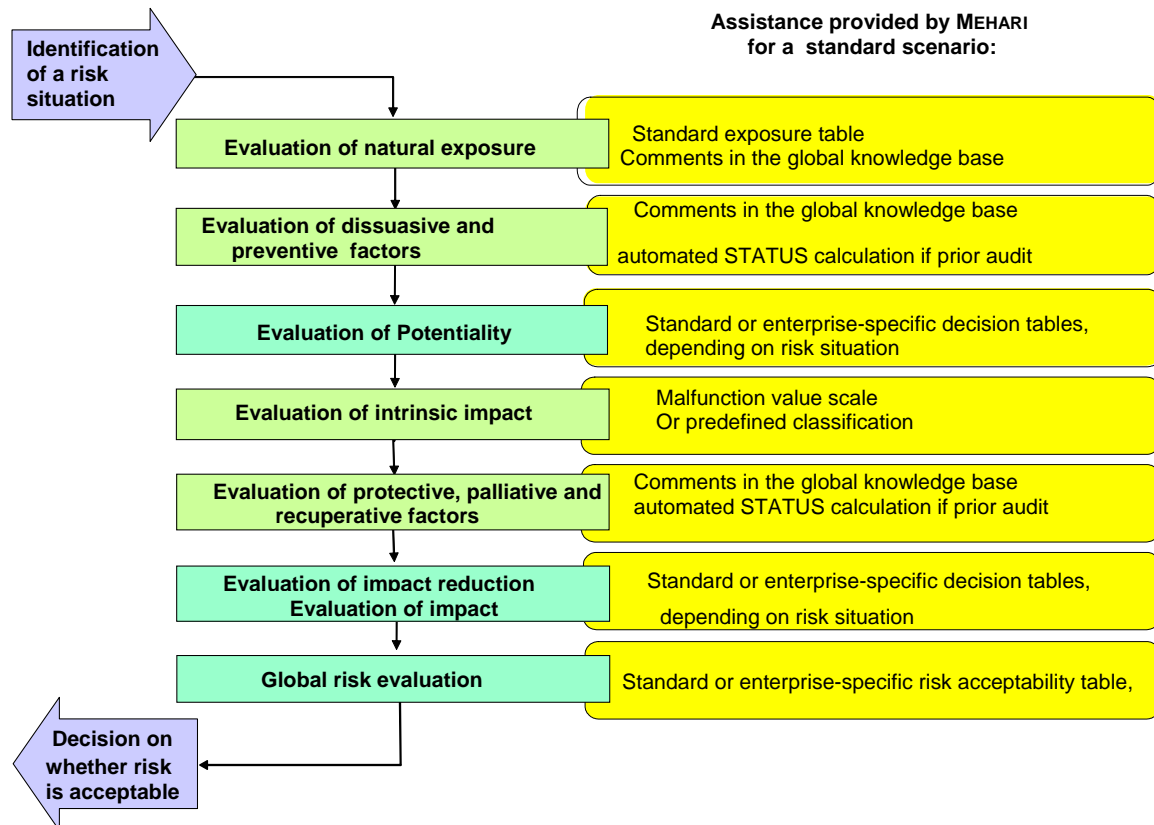


Figure 1: The risk analysis process and the assistance provided by MEHARI

Thus, through its knowledge base, MEHARI proposes various aids for risk analysis.

- Assistance in evaluating natural exposure.
- Automated procedures for the evaluation of risk reduction factors (dissuasive, preventive, protective, palliative and recuperative factors) depending on the quality of security services, if these have been evaluated through a MEHARI audit.
- A generic table of intrinsic impact can be created as a result of classification or directly using a scale of malfunction values.
- Automated procedures for calculating current potentiality and impact, as a function of natural exposure, intrinsic impact, and risk attenuation factors.

All of these aids are automatically available for all the scenarios held in the MEHARI knowledge base.

## 2.2. Evaluation of natural exposure

We have already explained, in the document *"MEHARI – Concepts and Mechanisms"*, that natural exposure can vary for the same organization depending on conjunctural phenomena.

However, for many organizations, it remains true that “normal” or “standard” exposure to a type of risk (i.e.: in the absence of any particular exceptional phenomena) is in conformity with what can be generally observed, and a prior evaluation can be made.

### 2.2.1 Standard natural exposure

The scenarios<sup>1</sup> in the MEHARI knowledge base are cross-referenced with a limited list of characteristic events, whether they are accidents, errors or voluntary actions (malicious or not), and for which a prior “standard” evaluation of exposure is proposed.

So, for example, it is estimated that the “standard” natural exposure to fire for an enterprise is level 2 (fairly unlikely); to loss of service of ICT equipment is level 3 (fairly likely); and to an error during the data input process is level 4 (very likely).

The list of these events and standard natural exposure is given in Appendix 1.

Each scenario refers to an event type, as shown by the example below:

|  |                             |           |
|--|-----------------------------|-----------|
| 10.31: Loss of data file, through malevolent media deletion by the operations staff. |                             |           |
| TYP-EXPO   | EFF-DISS                    | EFF-PREV  |
| MA010  | MAX(MIN(07C02;08E02);08C01) | 08A02     |
| EFF-PROT   | EFF-PALL                    | EFF-RECUP |
| MAX(08C01;08C05)   | MAX(MIN(08D05;09D03);09D02) | 01D02     |

The MA010 type of exposure in the table in Appendix 1 is: «Voluntary deletion of data or stealing of media» and is evaluated with a standard value of level 3 (fairly likely).

### 2.2.2 Enterprise-specific natural exposure for a given risk

It should be made clear that the standard evaluation provided is only a default evaluation, and that the specific evaluation of the exposure of the enterprise to the risk situation under analysis is preferable by far. For such an evaluation, refer to the definitions of levels of exposure given in the document *"MEHARI – Concepts and Mechanisms"*. These are resumed in Appendix 2.

For a specific scenario, you should also see the *"Risk Scenarios Reference Manual"*, which contains specific information about the evaluation of natural exposure

#### NOTE:

If risk situations are to be systematically analyzed, or if several risk situations are to be examined, it is preferable to start by reviewing all the events, and to give an overall judgment on the enterprise’s exposure to each of them.

## 2.3. Evaluation of intrinsic impact

The definition of intrinsic impact of a scenario, given in *"MEHARI – Concepts and Mechanisms"*, is the evaluation of the consequences of the risk event actually happening, independently of any security measures.

<sup>1</sup> The scenarios in the MEHARI knowledge base are grouped by families that have similar consequences. In this version, there are 12 standard families of scenario.

For each of the scenarios defined in the MEHARI knowledge base, there is a target of the scenario (an asset that will be deteriorated or affected by the scenario).

This might be a type of data or information that is stolen, a type of asset whose availability is reduced, or an asset that is modified. This will depend on whether the scenario will affect the confidentiality, the availability, or the integrity of the asset. These are the three basic criteria that MEHARI covers as a standard.

Evaluating intrinsic impact under such conditions implies the evaluation of the criticality or seriousness of the loss of availability, integrity or confidentiality, depending on the type of scenario, and the type of asset implicated in the scenario.

The classification approach used by MEHARI enables the creation of a generic classification table. This table shows the kinds of assets specifically identified through the knowledge base scenarios. The classification approach is described in the document “*MEHARI Concepts and mechanisms*” and in the “*Security Stakes Analysis and Classification Guide*”.

**2.3.1 The intrinsic impact table**

The approach used to evaluate intrinsic impact can then be organised. It consists of filling in an intrinsic impact table, based on the table provided in Appendix 3, of which an extract is shown below.

| <b><i>Intrinsic impact table</i></b>  |   |   |   |
|---|---|---|---|
| <b><i>Classification of data, information and infrastructure elements</i></b> | A | I | C |
| <b>Data and information</b>   |   |   |   |
| D01 Data files, or application databases                                      |   |   |   |
| D07 Mails and faxes   |   |   |   |
| .../...   |   |   |   |
| <b>IT and telecom infrastructure</b>  |   |   |   |
| R02 local area network equipment and links                                    |   |   |   |
| S01 Mainframes, application servers,  |   |   |   |

This table is completed by transcribing the level of the consequence or impact on availability, integrity or confidentiality for each type of identified asset. However, certain entries will not be filled, for example that for confidentiality of a hardware component.

The basic approach uses the classification tables, as described in “*MEHARI Security Stakes Analysis and Classification Guide*”.

At the worst, it can be done directly, but the classification approach defined in “*MEHARI Concepts and mechanisms*”, as completed by the above process, is undoubtedly better.

The general principle for completing the intrinsic impact table is to copy across the highest classification value found during the classification process for each type of information and for each criterion. Details on the way to complete the intrinsic impact table from the results of classification are described in the “*MEHARI Security Stakes Analysis and Classification Guide*”.

This thereby produces a synthesis that can be used to define the intrinsic impact level for each of the scenarios in the MEHARI knowledge base that impacts the type of information or asset under examination.

**2.3.2 Extending the intrinsic impact table**

The standard MEHARI table only refers to three standard criteria: availability, integrity and

confidentiality. Other criteria can, of course, be used. The table can be extended to include such criteria as proof, trace-ability, audit-ability, and so on.

To perform such an extension, scenarios should be created which bring the new criteria into play (or modify existing scenarios). Additionally, the corresponding evaluation tables should be defined.

The Risicare<sup>2</sup> software package enables up to eight criteria to be taken into account.

### 2.3.3 Evaluating intrinsic impact of scenarios

Intrinsic impact of each scenario of the knowledge base is evaluated quite simply. Each scenario has a reference to an asset type in the intrinsic impact table and a criterion to apply (A, I or C – or, potentially, others).

Put another way, each scenario of the knowledge base explicitly references an asset type affected by the scenario, and the way in which it is affected (A, I or C). This way, intrinsic impact can be evaluated using the table in Appendix 3.

### 2.3.4 Cartographic decomposition

The standard intrinsic impact table, as provided in Appendix 3, shows only one line for all of the application servers or mainframes. Likewise, there is only one line for all the application databases - and in general only one reference for each type of asset.

This global approach allows the analysis of risk situations taking into account the maximum sensitivity of the assets concerned, without differentiating between assets, or naming them. This is a simplification that restricts the situations that can be analyzed, with no practical consequences, as there will always be an opportunity, when building the action plans, to limit the corrective actions to those assets that are the most sensitive.

However, it is possible to distinguish between different variations of asset types, in the same way as security service variations can be differentiated during a MEHARI audit. For further details, see the audit schema in the “Security services audit guide”.

Creating variations of asset types in the intrinsic impact table is known as *cartographic decomposition*. It allows the differentiation, for example, between servers into a number of different domains, domains of application databases, software into domains, and so on. The use of cartographic decomposition allows the specific treatment of one or more specific domains of activity.

The Risicare<sup>TM</sup> software package uses this possibility to create variations of scenarios depending on the cartographic variations that are created<sup>3</sup>.

**WARNING:** Using this option can, however, seriously complicate the task, as it will inevitably create more scenarios.

## 2.4. Evaluating risk reduction factors through a MEHARI security audit

Evaluating the potentiality and impact of a risk scenario depends on the analysis of the existence of risk reduction factors, and an evaluation of their levels.

---

<sup>2</sup> Registered trademark of BUC S.A.

<sup>3</sup> When Risicare is not used for this work, and when the Excel sheets of the Clusif standard knowledge base are used, the T1 classification table described in the “Mehari Basic Principles and General Concepts” document should be modified. The intrinsic impact table provided in Appendix 3 should also be modified to take cartographic decomposition into account.

Risk reduction factors are dissuasion and prevention for potentiality; protection, palliation and recuperation for impact.

In its knowledge base, MEHARI provides evaluations of the levels of these risk reduction factors, depending on the quality of security services appropriate to the scenario being analyzed.

This automated evaluation is carried out in two steps:

- The calculation of efficiency indicators for the security services, for each type of risk reduction factor,
- The calculation of the risk reduction factors themselves.

#### 2.4.1 Efficiency indicators for security services by scenario and risk reduction measure

MEHARI defines an efficiency indicator for each scenario and each type of risk reduction measure.

The efficiency for each risk reduction measure is shown under the following notations:

EFF-DISS for the efficiency of *dissuasive measures*

EFF-PREV for the efficiency of *preventive measures*

EFF-PROT for the efficiency of *protective measures*

EFF-PALL for the efficiency of *palliative measures*

EFF-RECUP for the efficiency of *recuperative measures*

These indicators are calculated using formulae that make reference to the security services.

The formulae provided in the MEHARI knowledge base call on:

- Either a security service directly, by its identifier<sup>4</sup>, when the service is the only one to have this type of effect on the scenario;
- Or formulae that contain functions: MIN(arg1 ; arg2 ; ...) or MAX(arg1 ; arg2 ; ...), the parameters (arg1 ; arg2, ...) being identifiers of security services of the MEHARI knowledge base.

The formulae can therefore have the following formats, for example:

EFF-PALL = 06B01

EFF-PREV = MAX(04B04;MIN(04B01;04B02;04B03))

The first formula signifies that the (proposed) efficiency of the palliative measures is a direct function of the service 06B01 and takes as a value the quality level of that service.

The second formula signifies that the (proposed) efficiency of the preventive measures equals the greater value between the service quality of 04B04 and the function representing the minimum of the services 04B01, 04B02, and 04B03.

#### NOTE:

The MIN function signifies that the services called as parameters are complementary. If the level of one is low, the level of the whole will be low. An example of such a case is in the management of user access and authentication; if one of them is of a low level, the whole of access control is of a low level.

The MAX function signifies that the services called as parameters are alternatives. If one of the services is of a high quality level, so the whole will be of a high quality level. An example of

---

<sup>4</sup> the identifier of a sub-service is composed of a domain number, a letter indicating the service to which it is attached, and a sub-service number (e.g.: 06B01)

such a case, depending on certain scenarios, is in data access control and the encryption of the data itself.

It may be that none of the existing security services has an influence on a given type of risk reduction for a given scenario.

As an example, the illustration below shows the content of the MEHARI knowledge base for scenario 10.31:

| <b>10.31: Loss of data file, through malevolent media deletion by the operations staff.</b> |                              |           |
|---|------------------------------|-----------|
| TYP-EXPO  | EFF-DISS                     | EFF-PREV  |
| MA010   | MAX(MIN(07C02;08E02);08C01)  | 08A02     |
| EFF-PROT  | EFF-PALL                     | EFF-RECUP |
| MAX(08C01 ;08C05)   | MAX(MIN(08D05 ;09D03);09D02) | 01D02     |

**2.4.2 “Calculated” risk reduction factors**

Clearly, the efficiency coefficients evaluated above (EFF-XXXX) are calculated on the basis of service quality values, which have no reason to be integer values, and the efficiency coefficients are not themselves integer values either. To make the final evaluation of potentiality and impact easier, MEHARI transforms them into integer values for the evaluation of risk reduction factors.

In MEHARI, risk reduction factors are scored under the notation STATUS-XXXX (for example STATUS-DISS for the dissuasion factor).

The values for the STATUS are obtained by rounding the value to the nearest integer:

$$\text{STATUS-XXXX} = 1 \quad \text{if } \text{EFF-XXXX} < 1,5 \quad \text{STATUS-XXXX} = 2 \quad \text{if } 1,5 \leq \text{EFF-XXXX} < 2,5$$

$$\text{STATUS-XXXX} = 3 \quad \text{if } 2,5 \leq \text{EFF-XXXX} < 3,5 \quad \text{STATUS-XXXX} = 4 \quad \text{if } 3,5 \leq \text{EFF-XXXX}$$

Where XXXX can be DISS, PREV, PROT, PALL or RECUP

**Note:**

The value for the evaluation of natural exposure will be similarly provided under the notation STATUS-EXPO.

These risk reduction factors are the “calculated” factors. This means that the value obtained may not be totally pertinent in the specific context of the enterprise or organization. There may well be situations, for example, where staff are hardly sensitive to dissuasive measures, where staff are experts, where preventive measures are meaningless, and situations where protective or palliative measures would have no effect on the real impact.

**MEHARI aids by providing calculated values for risk reduction factors. These values should, however, be checked before applying them.**

A particularly frequent case is that of scenarios for which it could be considered that protective measures would not significantly reduce the intrinsic impact of the scenario (because the detection of fraud or disclosure of information, for example, would not reduce the seriousness of the risk, whatever measures are applied). Such a scenario can be considered non-evolutive, and can be declared as such<sup>5</sup>.

<sup>5</sup> In Riscicare, this option is available for scenarios that are initially considered evolutive. Selecting this option has the effect of forcing the application of a specific evaluation table that does not take into account the protective measures.

### 2.4.3 Evaluating risk factors

The risk factors for a given scenario should be checked against their basic definitions before applying them to the scenario. (see Appendix 4).

## 2.5. Evaluation of potentiality and impact

### 2.5.1 Automated potentiality evaluation: STATUS-P

MEHARI provides an automated evaluation of potentiality, starting with an evaluation of natural exposure (STATUS-EXPO), on the one hand, and the levels of dissuasive and preventive measures (STATUS-DISS and STATUS-PREV), on the other.

From the expression of the above STATUS in whole numbers, MEHARI evaluates the potentiality under the denomination STATUS-P. This is deduced directly from STATUS-EXPO, STATUS-DISS and STATUS-PREV by the evaluation tables.

Three standard evaluation tables are used by MEHARI, depending on the reasons for the accident or events leading to the scenario:

- Natural event or accident
- Human error
- Human voluntary action (malicious or not)

These standard tables can be modified if required.

#### **Note:**

The logic behind these evaluation tables is to consider that for each type of cause (accident, error or voluntary action), the same reasoning should be followed independently of the precise description of the scenario. With equal levels of exposure, dissuasion, and prevention, the potentiality of two scenarios should be the same.

### 2.5.2 Automated impact evaluation: STATUS-I

MEHARI also provides an automated evaluation of impact, starting from the intrinsic impact of the scenario on the one hand and the levels of protective, palliative and recuperative measures (measured by STATUS-PROT, STATUS-PALL and STATUS-RECUP), on the other.

The evaluation is made in two steps:

- Evaluation of an impact reduction indicator: STATUS-RI
- Impact evaluation: STATUS-I

#### 2.5.2.1 Impact reduction evaluation: STATUS-RI

MEHARI initially provides an evaluation of **impact reduction**, represented by the STATUS-RI indicator. This is directly deduced from STATUS-PROT, STATUS-PALL and STATUS-RECUP by evaluation tables. This impact reduction factor measures the attenuation of the consequences of the risk, compared to the intrinsic impact previously evaluated.

MEHARI uses three standard evaluation tables to evaluate STATUS-RI, depending on the type of consequence of the scenario :

- Loss of availability
- Loss of integrity

- Loss of confidentiality

These tables also take into account whether the scenario is evolutive or not. This characteristic is explicitly defined in the knowledge base. It can be forced to a non-evolutive status for those scenarios that were initially declared in the base as evolutive.

These standard tables can also be modified if required.

**Note:**

The logic behind these evaluation tables is to consider that for each type of consequence (loss of availability, integrity or confidentiality), the same reasoning should be followed independently of the precise description of the scenario. With equal levels of protective, palliative, and recuperative measures, the reduction of intrinsic impact for two comparable scenarios should be the same.

**2.5.2.2 Impact evaluation: STATUS-I**

The residual impact is deduced from the intrinsic impact and the impact reduction indicator through the following formula:

$$I = \text{MIN}(\text{INTRINSIC IMPACT}; 5 - \text{STATUS-RI})$$

Which signifies that STATUS-RI has the effect of defining the maximum level of impact :

- Maximum impact level of 4 if STATUS-RI is 1
- Maximum impact level of 3 if STATUS-RI is 2
- Maximum impact level of 2 if STATUS-RI is 3
- Maximum impact level of 1 if STATUS-RI is 4
- 

Evaluation of STATUS-I can also be represented by the table below:

| <b>STATUS-I calculation table</b> |   |   |   |   |
|-----------------------------------|---|---|---|---|
| STATUS-RI →                       | 1 | 2 | 3 | 4 |
| Intrinsic impact ↓                |   |   |   |   |
| 4                                 | 4 | 3 | 2 | 1 |
| 3                                 | 3 | 3 | 2 | 1 |
| 2                                 | 2 | 2 | 2 | 1 |
| 1                                 | 1 | 1 | 1 | 1 |

**2.5.3 Evaluation table construction principles**

In practice, standard tables, whether for potentiality or impact, are built using a certain number of principles (described in Appendix 5 – Principles for building STATUS evaluation tables). To modify these tables, one should start with the principles, and modify them as necessary, then rebuild the tables as a result.

Standard evaluation tables are documented in Appendix 6.

**2.5.4 Evaluating potentiality and impact**

As for risk reduction factors, the automated procedures provided through the decision tables only provide an aid in judging the values of the indicators called *STATUS* in MEHARI.

A final judgment should be made, as a general rule, on the pertinence of the levels of potentiality

P and impact I.

## 2.6. Evaluating the seriousness of a scenario

The seriousness of a scenario will be deduced from the evaluations of potentiality and impact (P and I), through the risk acceptability table, as defined in the document “*MEHARI – Concepts and Mechanisms*”.

## 2.7. Expressing security requirements

This step is only used when entity-level risk management is used. It consists in evaluating the consolidated requirements, after evaluating the seriousness of all risk situations identified during a security services audit.

This approach is based on “**service requirements**” definition, as detailed in Appendix 7.

## 2.8. Practical advice

### 2.8.1 The thinking behind the risk analysis approach

We have intentionally shown how the automated procedures of MEHARI can be used in evaluating risk levels.

***It is important to remember that this is an evaluation process, and that the consensus of an evaluation committee is always more reliable than automated procedures.***

### 2.8.2 Composition of a risk evaluation committee

The approach that we have described works even better when a representative working group or committee does the risk evaluation. The composition of this committee is particularly important, and should contain:

- Users in the area concerned. They should be of a profile that enables them to judge whether the security measures will really bring about the required attenuation of the consequences.
- IT staff who are able to explain, to the other members of the committee, the efficiency of different security measures and how these measures could be inhibited or bypassed (robustness and control/monitoring).
- A facilitator who is well versed in the method itself, and who has specific IT security competency.

### 2.8.3 Using the approach in conjunction with a security audit

We have already said that the automatic procedures should only be considered as an aid in the evaluation process. However, it is also possible, even with a competent and representative committee, that the quality of security services can be over-evaluated - whether through involuntary optimism or political will.

A security audit can additionally ensure the overall quality of the approach, and provide a reference point to bring out further questions.

***Evaluating high risks using automated procedures can bring out weaknesses or vulnerabilities that would have passed unnoticed in a direct evaluation. Any difference between these two approaches requires further examination.***

In this sense, the confirmation of direct evaluation by the use of automated procedures should be considered a best practice.

### 3. IDENTIFICATION OF RISK SITUATIONS

---

In the previous chapter, we discussed the analysis of a specific risk.

Identifying situations to be analyzed is therefore a preliminary step for which tools are also needed.

There are two principal ways of identifying risks:

- A direct approach, using a scale of malfunction values (cf. “*MEHARI – Concepts and Mechanisms*”).
- An organized and systematic identification using an automated evaluation of the scenario base provided by MEHARI

This section will examine the second of these options.

#### 3.1. Systematic identification using the knowledge base

We shall cover here the assistance brought by MEHARI in the systematic identification of risk situations.

Systematic identification will use the risk scenario knowledge base that has already been described and, in particular, the automated procedures described in the previous section. It is based on a preliminary analysis resulting in a scale of malfunction values, a classification of information system assets and a security audit.

The process used by MEHARI is based on the selection of a set of scenarios that are specific to the organization under study; the whole enterprise, an operational unit, etc.

There are two main steps in the process, as shown in the figure below:

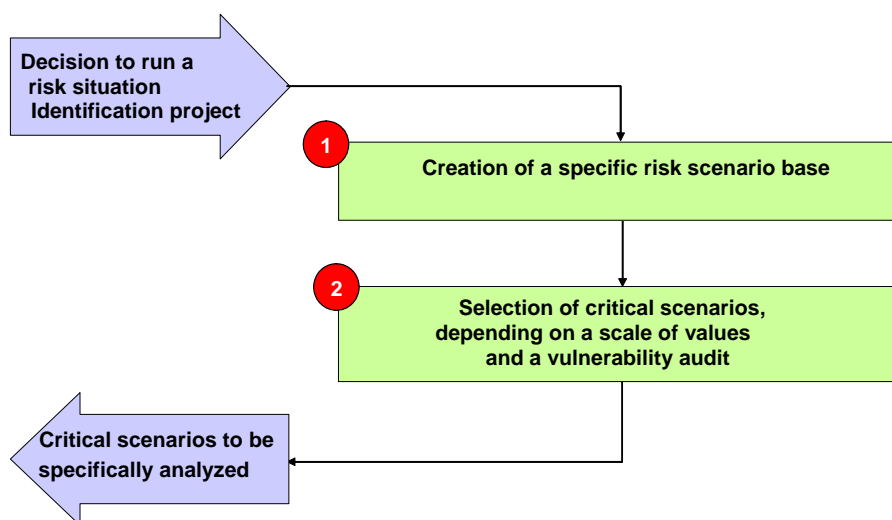


Figure 2: Identification of risk situations

#### 3.2. Creating a specific scenario base

A specific scenario base may be derived from the generic scenarios that are a part of the MEHARI knowledge base.

### 3.2.1 The generic risk scenario base

The MEHARI knowledge bases comprise a scenario base that was already discussed in the previous chapter.

It is a set of scenarios, classified by family of consequence type (in this version, there are about 170 scenarios and their variations classified into 12 families). For each scenario, there is:

- A description of the consequences of the scenario.
- A description of the cause and the origin of the scenario.
- The characteristic event type, to evaluate natural exposure.
- The type of asset concerned, to evaluate intrinsic impact.
- The pertinent security services for the scenario, depending on the expected result (dissuasive, preventive, protective, palliative, or recuperative).
- The formulae used by the automated procedures to calculate the efficiency of the security measures for the scenario.
- Global indicators of the type of consequence (A, I, or C, for Availability, Integrity, or Confidentiality), of the evolutive nature (or not) of the scenario, and the type of cause (A, E or V, for Accident, Error or Voluntary act). These indicators are also used by the automated procedures to calculate potentiality and impact reduction (for the selected evaluation tables used).

Additionally, the knowledge base includes, for each scenario, an analysis assistant (called the global approach). This is composed of definitions adapted to each type of security measure, and comments to directly assess the efficiency of the security measures.

### 3.2.2 Customizing scenarios as a function of the assets involved

As previously described, the generic scenarios in MEHARI only cover the assets involved by referencing them by type, at a relatively global level. One may wish to differentiate each scenario, depending on the assets involved.

Particularly, if a classification has been made for each set of servers or other IT assets, and each set of specific data for each application domain, it is tempting to analyze each scenario as many times as there are application domains. In other words, to create as many scenario instances as there are application domains.

Let us take, as an example, one of the MEHARI generic scenarios, which is “stealing data through access to the system and copying the files, by a hacker”. It is possible to create separate instances of the same scenario for different types of data (Human resources, sales, and so on). This would involve creating, from the generic scenario, specific scenarios for each set of assets for which a classification has been made.

This approach is possible, and uses what we termed earlier in this document “Cartographic Decomposition”.

This could lead to a considerable number of scenarios; and care should be taken in using this approach so as not to make life unnecessarily complicated.

***In practice, the basic MEHARI approach consists of using a generic scenario only with a general asset type, referenced by the scenario, and whose sensitivity is taken from the intrinsic impact table.***

This simplification can be justified by the fact that the reason for this analysis is to identify which risk situations might be critical and will require a more detailed analysis. It will identify what scenario can implicate which assets having what level of sensitivity.

### 3.2.3 Taking specific security solutions into account

In identifying which scenarios might be critical, the existing security solutions used will, of course, have an influence. The more efficient these solutions, the less critical the scenario will be.

It is therefore clear that those scenarios for which there exist, for example, different environments or systems, or - more generally- different sorts of security solutions, should be treated separately. This is exactly the same approach as is used during an audit and *the schema that was used for the audit should be re-used to select critical risk situations*.

Another way of applying the audit schema to the selection of critical scenarios is to consider that, to make the selection, we are going to base the selection on the results of a security audit. If therefore, during the audit, it was considered important to distinguish between different instances, then as many different scenarios (different instances of the generic scenario) should be considered during the selection process as required. This way, the different security services implicated in the scenario can be treated separately, and evaluated independently of the others.

It should be borne in mind that this could very quickly create a large number of scenarios. A very simple<sup>6</sup> audit schema can easily lead to multiplying the number of generic scenarios by quite a high factor.

### 3.3. Automatic evaluation of scenarios

The MEHARI automated procedures were described in the previous chapter.

These automated procedures make use of the results of a security audit (and, in particular, the audit schema used to build the specific scenario base).

The automated procedures are used to evaluate the detailed STATUS and, depending on the potentiality and intrinsic impact of each scenario, the resulting potentiality and impact for each scenario.

The global seriousness for each scenario and its criticality (or not) can therefore be deduced from a risk acceptability table.

### 3.4. Selecting critical scenarios that should be considered during risk analysis

Starting with the specific scenario base, and the automatic evaluation of their seriousness, it becomes easy to select the critical scenarios; that is to say, those scenarios that should be taken into account in a risk analysis performed using the process described in the previous chapter.

Scenarios whose seriousness is above a certain level will be selected for analysis. Usually, scenarios with a seriousness of 3 and above (on a scale of 1 to 4) are selected, but there is no hard and fast rule.

---

<sup>6</sup> For example, one organizational unit, two types of geographical sites (HQ and regional agency), two types of premises (technical and IT on the one hand, and other, office areas, on the other), a single network type with a single network operation, 2 types of system (mainframe and open systems) with a single IT operation, 2 types of applications (one on the mainframe and one on the open systems) and 2 types of development (mainframe and open systems).

**Note:**

Given the prudence recommended in the previous section concerning automatic evaluation, we recommend using a relatively severe risk acceptability table for the automatic selection. Effectively, the risk acceptability table can be different at the critical scenario selection level from the one used in the final judgment of the seriousness of a risk situation.

A relatively severe table for seriousness, such as the one shown below, could be used.

|       |       |       |       |       |
|-------|-------|-------|-------|-------|
| I = 4 | 3     | 3     | 4     | 4     |
| I = 3 | 2     | 3     | 3     | 4     |
| I = 2 | 1     | 2     | 3     | 3     |
| I = 1 | 1     | 1     | 1     | 3     |
|       | P = 1 | P = 2 | P = 3 | P = 4 |

**Important:**

Generally, we consider that scenarios with a seriousness of 4 are unsupportable, that those with seriousness of 3 are inadmissible and those with lower levels of seriousness are tolerable.

# APPENDIX 1 : STANDARD NATURAL EXPOSURE

## TABLE

| Evaluation of natural exposure                            |   |               |                 |                 |               | Status-Expo |
|---|---|---------------|-----------------|-----------------|---------------|-------------|
| Evaluation of the potentiality of the events listed below |   | Very unlikely | Rather unlikely | Rather probable | Very probable |             |
| <b>Accidents</b>  |   |               |                 |                 |               |             |
| AC01  | Short-circuit : either power cable or equipment.  |               | X               |                 |               | 2           |
| AC02  | Lightning   |               | X               |                 |               | 2           |
| AC03  | Fire : internal origin : paper bin, ashtray etc.  |               | X               |                 |               | 2           |
| AC04  | Accidents due to water or liquids (leak of a pipe, accidentally spilled liquid, etc.).  |               | X               |                 |               | 2           |
| AC05  | Flooding due to a leaking or broken pipe  |               | X               |                 |               | 2           |
| AC06  | Flooding due to river or ground water rise  |               | X               |                 |               | 2           |
| AC07  | Flooding due to the extinction of a nearby fire   |               | X               |                 |               | 2           |
| AC08  | Power shortage of long duration due to an external cause  |               | X               |                 |               | 2           |
| AC09  | Unavailability of premises : prohibition decided by the authorities (risk of pollution, rioting, etc.)  |               | X               |                 |               | 2           |
| AC10  | Loss of strategic personnel   |               | X               |                 |               | 2           |
| AC11  | Auxiliary equipment breakdown (power supply, air conditioning, etc.)  |               | X               |                 |               | 2           |
| AC12  | IT or telecom equipment breakdown   |               | X               |                 |               | 2           |
| AC13  | Hardware failure of an IT or telecom equipment unsolvable by the maintenance or maintenance provider unavailable                              |               | X               |                 |               | 2           |
| AC14  | Software deadlock unsolvable by the maintenance: editor or maintenance provider unavailable   |               | X               |                 |               | 2           |
| AC15  | Accidental saturation of resources (CPU, memory, disk, etc.)  |               |                 | X               |               | 3           |
| AC16  | Accident during operation, resulting in data distortion   |               |                 | X               |               | 3           |
| AC17  | Data or configuration erased or polluted by a virus   |               |                 | X               |               | 3           |
| AC18  | Accidental loss of data files caused by an automated process  |               |                 | X               |               | 3           |
| AC19  | Accidental loss of data files caused by obsolescence, pollution, etc.   |               | X               |                 |               | 2           |
| AC20  | Accidental loss of data files caused by an equipment failure (disk crash, etc.)   |               | X               |                 |               | 2           |
| <b>Malevolence</b>  |   |               |                 |                 |               |             |
| MA01  | Vandalism from outside: bullets or objects thrown from the street, etc.   |               | X               |                 |               | 2           |
| MA02  | Vandalism from inside: by people authorized within the premises (personnel, sub-contractor, etc.).  |               | X               |                 |               | 2           |
| MA03  | Terrorism: sabotage, explosives left close to sensitive premises  | X             |                 |                 |               | 1           |
| MA04  | Malicious and repeated saturation of IT resources by a group of users   |               | X               |                 |               | 2           |
| MA05  | Saturation of the network caused by a worm  |               | X               |                 |               | 2           |
| MA06  | Malicious erasure (directly or indirectly) of software on its storage   |               | X               |                 |               | 2           |
| MA07  | Malicious modification (direct or indirect) of the functionalities of a program or of the operation of an office program (Excel, Access, etc) |               |                 | X               |               | 3           |
| MA08  | Distorted data entry or fiddling of data  |               |                 | X               |               | 3           |
| MA09  | Intended access to data or information and disclosure of information  |               |                 | X               |               | 3           |
| MA10  | Diversion of files or theft of data media   |               |                 | X               |               | 3           |
| MA11  | Intentional erasure (direct or indirect), theft or destruction of program or data containers  |               |                 | X               |               | 3           |
| MA12  | Theft of portable PC outside the premises of the organization   |               |                 | X               |               | 3           |
| MA13  | Malicious erasure of networking configurations  |               | X               |                 |               | 2           |
| MA14  | Malicious erasure of systems' or applications' configurations   |               | X               |                 |               | 2           |
| MA15  | Diversion of program source code  |               | X               |                 |               | 2           |
| MA16  | Spying by a foreign state or a mafia (using important resources)  | X             |                 |                 |               | 1           |
| MA17  | Theft of IT or networking equipment, within the organization  |               |                 | X               |               | 3           |
| <b>Intentional, though not malicious, actions</b>         |   |               |                 |                 |               |             |
| AV01  | Absence or strike of IT operational personnel   |               | X               |                 |               | 2           |
| AV02  | Departure or resignation of strategic personnel   |               |                 | X               |               | 3           |
| AV03  | Intrusion into the IT resources of a third party, initiated from the organization or by its personnel   |               |                 | X               |               | 3           |
| AV04  | Illegal use of licensed software or products  |               |                 | X               |               | 3           |
| <b>Errors</b>   |   |               |                 |                 |               |             |
| ER01  | Unintended downgrade of performances, resulting from a maintenance operation  |               | X               |                 |               | 2           |
| ER02  | Unintended erasure of software program by accident or human error   |               |                 | X               |               | 3           |
| ER03  | Fortuitous alteration of data during a maintenance operation  |               |                 | X               |               | 3           |
| ER04  | Error during data entry   |               |                 |                 | X             | 4           |
| ER05  | Bug of operating system, middleware or software package   |               |                 |                 | X             | 4           |
| ER06  | Bug in application program  |               |                 |                 | X             | 4           |
| ER07  | Error introduced during the modification of functions or macro in a spreadsheet   |               |                 | X               |               | 3           |

## APPENDIX 2 : DEFINITION OF NATURAL EXPOSURE LEVELS

---

### *Natural exposure to risk*

Level 1 : Very low exposure

Independently of any security measures, the probability that a given scenario will occur is very low and practically negligible.

level 2 : Low exposure (hardly exposed).

Even without any security measures at all, the combination of the environment (cultural, human , geographic or other) and the context (strategic, competitive, social,...) make the probability that a given scenario will occur, in the short or medium term, very low.

Level 3 : Medium exposure (not particularly exposed)

The environment and context of the enterprise are such that, if nothing is done to avoid it, the given scenario is bound to happen in the more or less short term.

Level 4 : High exposure : (particularly exposed).

The environment and context of the enterprise are such that, if nothing is done to avoid it, the occurrence of the given scenario is likely to happen in the very short term.

## APPENDIX 3 : INTRINSIC IMPACT TABLE

| Intrinsic Impact table  |  |   |   |   |
|---|--|---|---|---|
| Classification level of data, information and infrastructure components       |  | A | I | C |
| <b>Data and Information</b>   |  |   |   |   |
| D01   | Data files or data bases accessed by applications  |   |   |   |
| D02   | Shared office files and data   |   |   |   |
| D03   | Personal office files (on PC, etc.)  |   |   |   |
| D04   | Written or printed information and data kept by users and personal archives                                      |   |   |   |
| D05   | Listings or printed documents  |   |   |   |
| D06   | Exchanged messages, screen views, etc. (partial data)  |   |   |   |
| D07   | Mails and faxes  |   |   |   |
| D08   | Patrimonial archives or documents used as proofs   |   |   |   |
| D09   | Data and information published on public or internal sites   |   |   |   |
| <b>Infrastructure : telecommunications and systems</b>                        |  |   |   |   |
| R01   | Wide Area Network equipment and links (networking systems and associated software)                               |   |   |   |
| R02   | Local Area Network equipments and links (networking systems and associated software)                             |   |   |   |
| R03   | WAN Configuration data   |   |   |   |
| R04   | LAN Configuration data   |   |   |   |
| S01   | Main systems, servers hosting applications and their peripheral equipments, shared file servers                  |   |   |   |
| S02   | Configuration files related to main systems et servers   |   |   |   |
| S03   | Workstations and user terminals (PC, local printers, peripherals, specific interfaces, etc.)                     |   |   |   |
| A01   | Application software, package or middleware (executable code)  |   |   |   |
| A02   | Source code  |   |   |   |
| A03   | Configuration files related to applications  |   |   |   |
| A04   | User or client software and applications   |   |   |   |
| <b>General infrastructure</b>   |  |   |   |   |
| E01   | User workspace and environment   |   |   |   |
| E02   | Equipments used for vocal exchanges (telephone, etc.)  |   |   |   |
| I01   | Entirety of the computer room and the telecom premise  |   |   |   |
| <b>Intrinsic impacts (global objects or not related to a specific object)</b> |  |   |   |   |
| <b>Complete loss or destruction of an installation</b>                        |  |   |   |   |
| <b>Personnel unavailability</b>   |  |   |   |   |
| P01   | Teams of specialists (business related)  |   |   |   |
| P02   | IT operation personnel   |   |   |   |
| <b>Legal and regulatory non compliance</b>                                    |  |   |   |   |
| C01   | Non compliance to laws and regulations relative to private life protection                                       |   |   |   |
| C02   | Non compliance to laws and regulations relative to financial controls  |   |   |   |
| C03   | Non compliance to laws and regulations relative to intellectual property rights                                  |   |   |   |
| C04   | Non compliance to laws and regulations relative to information system protection                                 |   |   |   |
| C05   | Non compliance to laws and regulations relative to endangerment of personnel and public and environmental safety |   |   |   |

## APPENDIX 4: DEFINITION OF RISK REDUCTION FACTOR LEVELS

### **Dissuasive measures**

Level 1: The effect of dissuasive measures is low or nil.

The potential attacker can logically consider that he or she runs no personal risk. They can consider that they will not be identified, or will have the possibility of using strong arguments to refute any accusations concerning actions performed, or that any punishment will be very light.

Level 2: The effect of dissuasive measures is medium.

The potential attacker can logically consider that he or she runs only a small risk. In any case, any potential personal prejudice will be supportable.

Level 3: The effect of dissuasive measures is high.

The potential attacker can logically consider that he or she runs a high risk. They should realize that they will undoubtedly be identified, and that punishment will be serious.

Level 4: The effect of dissuasive measures is very high.

The potential attacker can logically consider that he or she should abandon any idea of performing the action. They should realize that they will certainly be identified, and that the resulting punishment will well outweigh any potential gain.

### **Preventive measures**

Level 1: The effect of the preventive measures is low or nil.

Any person in the organization, or close to it, or even someone who knows something about it, is capable of setting this scenario in motion, with the means at their disposal (or easy to obtain).

Perfectly ordinary circumstances can be the cause of this scenario (misuse, error, ordinary unfavorable conditions).

Level 2: The effect of the preventive measures is medium.

A professional can set off the scenario, without the need for special means or tools outside of those available in the profession.

Rare natural circumstances can produce the same result.

Level 3: The effect of the preventive measures is high.

Only a specialist, or a professional with special tools or means, or a group of professionals in collusion and using their collective means and tools could succeed.

This is usually the result of the conjunction of rare or exceptional circumstances.

Level 4: The effect of the preventive measures is very high.

Only a few determined experts, with exceptional means, could succeed.

Only the conjunction of very rare or extremely exceptional circumstances would permit this scenario to happen.

### **Protective measures or confinement**

Level 1: The effects of the confinement and the limitation of the direct consequences are very low or nil.

Either the damage and its direct consequences cannot be limited, or it will not be detected for some time. The possible protective measures then only have a restricted influence on the level of the direct consequences.

Level 2: The effects of the confinement and the limitation of the direct consequences are medium.

Even if the damage and its direct consequences can be limited, the time to detect it is long, or reaction is slow.

The protective measures that are used have a real influence on the result, but the direct consequences are still very big.

Level 3: The effects of the confinement and the limitation of the direct consequences are high.

The event is rapidly detected, with immediate reaction.

The protective measures that are used have a real influence on the direct impact, which remains real but limited in scope, and manageable.

Level 4: The measures have a very strong effect.

The start of the scenario is detected in real time, before any major damage can be done, and the protective measures are immediately set in train.

Direct consequences are limited to small deteriorations immediately due to the accident, error or voluntary action.

### **Palliative measures**

Level 1: The effects of the limitation of the indirect consequences are very low or nil.

Either totally improvised measures are used, or it is considered that their effect will be low.

Level 2: The effects of the limitation of the indirect consequences are medium.

The relief or palliative solutions have been broadly planned, but the fine detail is missing. It can be considered that, due to the lack of detail, there will be a corresponding lack of efficiency of the palliative measure. The time to re-establish normal operations cannot be precisely predicted, or will not fundamentally change the nature of the damage caused.

Level 3: The effects of the limitation of the indirect consequences are high.

The palliative measures have not only been finely planned and organized, but also tested and validated. The time to re-establish normal operations can be precisely estimated or known, and is such that it will measurably reduce the seriousness of the indirect consequences of the scenario.

Level 4: The effects of the limitation of the indirect consequences are very high indeed.

Normal operations continue without any noticeable interruption.

### **Recuperative measures**

Level 1: The effect of the recuperative measures is low or nil.

Whatever can hopefully be recuperated through insurance claims or legal processes is nothing compared to the damage caused by the global impact of the scenario and its consequences.

Level 2: The effect of the recuperative measures is medium.

Whatever can hopefully be recuperated is not negligible, but the organization has the responsibility for the greater part of the impact of the scenario. In the case of a major incident, it is not certain that the risk transfer would allow the organization to continue operations.

Level 3: The effect of the recuperative measures is high.

Whatever is recuperated through insurance claims or legal processes is enough to seriously attenuate the impact of the scenario. In any case, operations can continue.

Residual impact would be, at the worst, very serious, but would not reach the « Vital » level.

Level 4: The effect of the recuperative measures is extremely high.

However bad the disaster, the residual impact remains supportable (level 2).

# APPENDIX 5: PRINCIPLES FOR BUILDING STATUS EVALUATION TABLES

---

The principles described below are those that have been used to create the STATUS-P and STATUS-RI tables for converting detailed STATUS into global STATUS,.

## STATUS-P evaluation table

The table is based on the following rationale:

- Natural exposure having been defined as being the evaluation of intrinsic potentiality without any other measure, the maximum value of STATUS-P is that of STATUS-EXPO (in the absence of any other measure, that is to say, if STATUS-DISS et STATUS-PREV both have a value of 1)
- If the value of STATUS-PREV is 3 or 4, for accidents or errors; then STATUS-P has a maximum value of 2 or 1, respectively.
- If the value of STATUS-PREV is 4, for voluntary action; then STATUS-P has a maximum value of 2
- If the value of STATUS-PREV is 4, for voluntary action; and if the exposure is less than or equal to 3, then STATUS-P has a maximum value of 1

It is on this rationale that the standard MEHARI knowledge base tables have been built.

## STATUS-RI evaluation table

The table is based on the following rationale:

- If the value of STATUS-RECUP is 3, then the value of STATUS-RI is at least 2
- If the value of STATUS-RECUP is 4, then the value of STATUS-RI is at least 3
- If the value of STATUS-PALL is 3 or 4, for availability scenarios, then the value of STATUS-RI is at least 3 (if relief planning is properly prepared, then the resulting impact cannot be serious).
- If the value of STATUS-PROT is 4 in an integrity scenario, everything can be avoided if rapid restoration is possible, and therefore STATUS-RI is aligned on the value of STATUS-PALL, which, in this case, deals with restoration.
- If the value of STATUS-PROT is 3 in an integrity scenario, if rapid restoration is possible (STATUS-PALL = 3 or 4), no doubt the worst will have been avoided, but the situation can still be serious: STATUS-RI = 2. However, if rapid restoration is not possible (STATUS-PALL = 1 or 2), nothing is attenuated, and STATUS-RI = 1
- If the value of STATUS-PROT is 1 or 2 in an integrity scenario, then the value of STATUS-RI is 1, unless there is a planned action identified in STATUS-RECUP (low protection, no palliative measure, because these are only composed of restorative measures that have no effect on the indirect consequences, and only the restorative measures play a role.).

It is on this rationale that the standard MEHARI knowledge base tables have been built.

# APPENDIX 6 : STANDARD EVALUATION TABLES

Grids of evaluation for STATUS-P for scenarios resulting from:

## 1. An Accident

|     | EXPO = 1 |   |   |   | EXPO = 2 |   |   |   | EXPO = 3 |   |   |   | EXPO = 4 |   |   |   |
|-----|----------|---|---|---|----------|---|---|---|----------|---|---|---|----------|---|---|---|
| D   |          |   |   |   |          |   |   |   |          |   |   |   |          |   |   |   |
| I   |          |   |   |   |          |   |   |   |          |   |   |   |          |   |   |   |
| S   |          |   |   |   |          |   |   |   |          |   |   |   |          |   |   |   |
| S 1 | 1        | 1 | 1 | 1 | 2        | 2 | 2 | 1 | 3        | 3 | 2 | 1 | 4        | 4 | 2 | 1 |
|     | 1        | 2 | 3 | 4 | 1        | 2 | 3 | 4 | 1        | 2 | 3 | 4 | 1        | 2 | 3 | 4 |
|     | P        | R | E | V | P        | R | E | V | P        | R | E | V | P        | R | E | V |

## 2. An Error

|     | EXPO = 1 |   |   |   | EXPO = 2 |   |   |   | EXPO = 3 |   |   |   | EXPO = 4 |   |   |   |
|-----|----------|---|---|---|----------|---|---|---|----------|---|---|---|----------|---|---|---|
| D   |          |   |   |   |          |   |   |   |          |   |   |   |          |   |   |   |
| I   |          |   |   |   |          |   |   |   |          |   |   |   |          |   |   |   |
| S   |          |   |   |   |          |   |   |   |          |   |   |   |          |   |   |   |
| S 1 | 1        | 1 | 1 | 1 | 2        | 2 | 2 | 1 | 3        | 3 | 2 | 1 | 4        | 4 | 2 | 1 |
|     | 1        | 2 | 3 | 4 | 1        | 2 | 3 | 4 | 1        | 2 | 3 | 4 | 1        | 2 | 3 | 4 |
|     | P        | R | E | V | P        | R | E | V | P        | R | E | V | P        | R | E | V |

## 3. A Malevolent action

|     | EXPO = 1 |   |   |   | EXPO = 2 |   |   |   | EXPO = 3 |   |   |   | EXPO = 4 |   |   |   |
|-----|----------|---|---|---|----------|---|---|---|----------|---|---|---|----------|---|---|---|
| D 4 | 1        | 1 | 1 | 1 | 2        | 1 | 1 | 1 | 3        | 2 | 1 | 1 | 4        | 3 | 2 | 2 |
| I 3 | 1        | 1 | 1 | 1 | 2        | 2 | 1 | 1 | 3        | 2 | 2 | 1 | 4        | 3 | 2 | 2 |
| S 2 | 1        | 1 | 1 | 1 | 2        | 2 | 2 | 1 | 3        | 3 | 2 | 1 | 4        | 4 | 3 | 2 |
| S 1 | 1        | 1 | 1 | 1 | 2        | 2 | 2 | 1 | 3        | 3 | 2 | 1 | 4        | 4 | 3 | 2 |
|     | 1        | 2 | 3 | 4 | 1        | 2 | 3 | 4 | 1        | 2 | 3 | 4 | 1        | 2 | 3 | 4 |
|     | P        | R | E | V | P        | R | E | V | P        | R | E | V | P        | R | E | V |

## Grids of evaluation for STATUS-RI (Impact Reduction)

The non evolutionary scenarios are represented as PROT = 0

### 1. Scenarios affecting Availability

|     | PROT = 1 |   |   |   | PROT = 2 |   |   |   | PROT = 3 |   |   |   | PROT = 4 |   |   |   | PROT = 0 |   |   |   |
|-----|----------|---|---|---|----------|---|---|---|----------|---|---|---|----------|---|---|---|----------|---|---|---|
| R 4 | 3        | 3 | 3 | 3 | 3        | 3 | 3 | 3 | 3        | 3 | 3 | 3 | 3        | 3 | 3 | 4 | 3        | 3 | 3 | 3 |
| E 3 | 2        | 2 | 3 | 3 | 2        | 2 | 3 | 3 | 2        | 2 | 3 | 3 | 2        | 2 | 3 | 4 | 2        | 2 | 3 | 3 |
| C 2 | 1        | 2 | 3 | 3 | 1        | 2 | 3 | 3 | 1        | 2 | 3 | 3 | 2        | 2 | 3 | 4 | 1        | 2 | 3 | 3 |
| U 1 | 1        | 2 | 3 | 3 | 1        | 2 | 3 | 3 | 1        | 2 | 3 | 3 | 2        | 2 | 3 | 4 | 1        | 2 | 3 | 3 |
| P   | 1        | 2 | 3 | 4 | 1        | 2 | 3 | 4 | 1        | 2 | 3 | 4 | 1        | 2 | 3 | 4 | 1        | 2 | 3 | 4 |
|     | P        | A | L | L | P        | A | L | L | P        | A | L | L | P        | A | L | L | P        | A | L | L |

### 2. Scenarios affecting Integrity

|     | PROT = 1 |   |   |   | PROT = 2 |   |   |   | PROT = 3 |   |   |   | PROT = 4 |   |   |   | PROT = 0 |   |   |   |
|-----|----------|---|---|---|----------|---|---|---|----------|---|---|---|----------|---|---|---|----------|---|---|---|
| R 4 | 3        | 3 | 3 | 3 | 3        | 3 | 3 | 3 | 3        | 3 | 3 | 3 | 3        | 3 | 3 | 4 | 3        | 3 | 3 | 3 |
| E 3 | 2        | 2 | 2 | 2 | 2        | 2 | 2 | 2 | 2        | 2 | 2 | 2 | 2        | 2 | 3 | 4 | 2        | 2 | 2 | 2 |
| C 2 | 1        | 1 | 1 | 1 | 1        | 1 | 1 | 1 | 1        | 1 | 2 | 2 | 1        | 2 | 3 | 4 | 1        | 1 | 2 | 2 |
| U 1 | 1        | 1 | 1 | 1 | 1        | 1 | 1 | 1 | 1        | 1 | 2 | 2 | 1        | 2 | 3 | 4 | 1        | 1 | 2 | 2 |
| P   | 1        | 2 | 3 | 4 | 1        | 2 | 3 | 4 | 1        | 2 | 3 | 4 | 1        | 2 | 3 | 4 | 1        | 2 | 3 | 4 |
|     | P        | A | L | L | P        | A | L | L | P        | A | L | L | P        | A | L | L | P        | A | L | L |

### 3. Scenarios affecting Confidentiality

|     | PROT = 1 |   |   |   | PROT = 2 |   |   |   | PROT = 3 |   |   |   | PROT = 4 |   |   |   | PROT = 0 |   |   |   |
|-----|----------|---|---|---|----------|---|---|---|----------|---|---|---|----------|---|---|---|----------|---|---|---|
| R 4 | 3        |   |   |   | 3        |   |   |   | 3        |   |   |   | 3        |   |   |   | 3        |   |   |   |
| E 3 | 2        |   |   |   | 2        |   |   |   | 2        |   |   |   | 2        |   |   |   | 2        |   |   |   |
| C 2 | 1        |   |   |   | 2        |   |   |   | 3        |   |   |   | 3        |   |   |   | 1        |   |   |   |
| U 1 | 1        |   |   |   | 2        |   |   |   | 3        |   |   |   | 3        |   |   |   | 1        |   |   |   |
| P   | 1        |   |   |   | 1        |   |   |   | 1        |   |   |   | 1        |   |   |   | 1        |   |   |   |
|     | P        | A | L | L | P        | A | L | L | P        | A | L | L | P        | A | L | L | P        | A | L | L |

# APPENDIX 7: EXPRESS SECURITY REQUIREMENTS

---

After having evaluated the seriousness of a set of risk situations and using the security services<sup>7</sup> audit results, it is possible to express security requirements as an evaluation of consolidated needs, followed by their priority ordering.

This approach uses the definition of “*service requirements*” described below.

## Service Requirements

A security service requirement is defined for each scenario, using the following basic principles..

### *Service requirement for a given scenario*

A given security service may have an influence on the seriousness of a scenario. **If this is the case, then a service requirement exists for this service for the scenario.**

Quantitatively, this service requirement will be even more important as:

- its influence (represented by its *influence factor*), for this scenario, will be high;
- the seriousness of the scenario will be considered high;
- the current quality of the service will be low.

So, for service **i** faced with scenario **k**, the service requirement can be calculated by the formula:

$$BS_{ik} = e_{ik} \cdot b^{G_k} \cdot (4 - \sigma_i)$$

where :

- $BS_{ik}$  = service requirement for service **i** for scenario **k**
- $e_{ik}$  = coefficient of influence of service **i** for scenario **k**
- $b$  = Sensibility parameter
- $G_k$  = Seriousness of scenario **k**
- $\sigma_i$  = Quality of security service **i**

The coefficient of influence “e”, with a value lying between 0 and 16, represents the degree of influence of the security service over the scenario. .

It is deduced from the formulae used by MEHARI to evaluate the efficiency of different types (dissuasive, preventive, protective, palliative, or recuperative) of measures over a scenario.

This coefficient is calculated using the formula below:

$$e_{ik} = \alpha_{ik} \cdot \beta_{ik}$$

If the service is referenced only for one type of measure, the value of  $\alpha_{ik}$  is established in this way:

- If the service is the only one to be used for the type of measure under consideration,  $\alpha_{ik} = 2$
- If the service is used by a formula of the type *min (serv\_A;serv\_B)*  $\alpha_{ik} = 2$
- If the service is used by a formula of the type *max (serv\_A;serv\_B)*  $\alpha_{ik} = 1$

---

<sup>7</sup> A security service of MEHARI usually bears a richer scope than an ISO 17799 Control.

In the case of a complex formula, only the (“min” or “max.”) function directly referencing this security service will be taken into account.

The value of  $\beta_{ik}$  is determined whether the security service  $i$  has:

- a dissuasive influence for scenario  $k$ ,  $\beta_{ik} = 4$
- a preventive influence for scenario  $k$ ,  $\beta_{ik} = 8$
- a protective influence for scenario  $k$ ,  $\beta_{ik} = 4$
- a palliative influence for scenario  $k$ ,  $\beta_{ik} = 8$
- a recuperative influence for scenario  $k$ ,  $\beta_{ik} = 2$

If the security service is used for several types of measures, as many coefficients of influence will be calculated, and the highest value of the coefficient of influence will be retained.

$b$ , which is used as the sensibility parameter, to anchor the seriousness of each scenario, has a heavy influence on the end-result :

- a value of 2 minimizes the effect of the seriousness of a scenario
- Generally, a value of 8 is considered a good choice.

### Consolidation of service requirements

The consolidation of service requirements:  $BS_i$ , for service  $i$ , will be evaluated by the simple sum:

$$BS_i = \sum_k BS_{ik}$$

$BS_i$ , the service requirement thus calculated, has even more importance is the service is used by a number of scenarios, and if these scenarios are serious, and if the service can influence the seriousness of the scenarios.

However, the choice of improving a service can be inconsistent with the choice made across the organization, at a strategic planning level (if a security policy as been defined). MEHARI therefore proposes the following approach:

- Sort scenarios so as to show clearly those that call on the security services with the strongest global requirements;
- Analyze whether these security services are consistent with the directives and recommendations of the global security policy. Any negative response at this level will inevitably put the security policy into question.
- If the answer is positive, evaluate the revised quality level of each security service as a function of the improvements already decided concerning it (additions or modifications to procedures and/or mechanisms);
- Re-estimate the resulting seriousness and new service requirements;
- Start again!

The RISICARE<sup>8</sup> software package includes automatisms to follow that process.

---

<sup>8</sup> RISICARE is produced by BUC S.A.