



# MEHARI 2007

## Concepts and Mechanisms

April 2007



Methods Commission

---

\*MEHARI is a registered trademark of the CLUSIF

---

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

30, rue Pierre Semard, 75009 PARIS

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 .....	3
2	Assessment of the security stakes and the classification of information and assets .....	5
2.1	Introduction .....	5
2.2	Defining the security stakes: malfunction value scale and classification .....	5
3	Assessing the state of security services .....	7
3.1	Introduction .....	7
3.2	Security services .....	7
3.3	Evaluating security service quality .....	8
3.4	The vulnerability review process .....	11
3.5	Summary of the Vulnerability Review .....	12
4	Analyzing risk situations .....	13
4.1	Introduction .....	13
4.2	Risk scenarios .....	13
4.3	Analysis of a risk scenario: overall view or "global" approach .....	14
4.4	Using the MEHARI knowledge bases .....	27
4.5	Risk situation analysis process .....	28
4.6	Summary of the risk analysis approach .....	29
5	Identifying risk situations .....	30
5.1	The direct approach using the malfunction value scale .....	30
5.2	Systematic identification using the knowledge base .....	30
5.3	The two approaches are complementary .....	31
6	Using the Mehari modules .....	32
6.1	Security plans based on risk analysis .....	32
6.2	Security plans based on an audit .....	38
6.3	Security of development projects .....	41
7	Review of the main improvements compared to previous versions of Mehari .....	44
7.1	Creating the intrinsic impact table .....	44
7.2	ISO 17799 compliance measures following a MEHARI audit .....	44
7.3	Recall of MEHARI previous improvements .....	44

## FIGURES

Figure 1. Critical assets + High vulnerability → Unacceptable risk.....	3
Figure 2. Using MEHARI modules for different approaches to security. ....	4
Figure 4: Risk acceptability table.....	26
Figure 5: Risk situation analysis .....	27
Figure 6: The Risk Analysis Process, and MEHARI aids and assistance .....	28
Seriousness function of Potentiality and Impact.....	30
Figure 7: Creating security plans based on risk analysis .....	38
Figure 8: Managing security through an audit .....	39
Figure 9: Security management by audit and stakes .....	41
Figure 10: Project security management.....	42

## ACKNOWLEDGMENTS

The CLUSIF wishes to thank everybody who has contributed to the creation of this document, and in particular:

Dominique Buc	BUC SA
Olivier Corbier	ORSID
Eric Deronzier	YSOSECURE
Jean-Philippe Jouas	
Gérard Molines	MOLINES CONSULTANTS
Jean-Louis Roule	

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

Please send your questions or comments to: [mehari@clusif.asso.fr](mailto:mehari@clusif.asso.fr)

# 1 INTRODUCTION

---

Every CISO (Chief Information Security Officer) faces the same two basic challenges on taking up a new appointment, these are:

- What is the mandate – how broad is the mission and what are the objectives?
- What should be the plan of attack – what methodologies and tools exist to meet the security management goals?

While it is relatively easy to agree on the mandate, there are many possibilities to face the second challenge.

Most people would agree that information system security involves minimizing the risks associated with the information system of the enterprise or organization. However, as “minimize” is not easily quantifiable, some people would suggest that the definition be better stated “the risks become acceptable”.

This, in itself, is hardly sufficient either, as it does not make clear what is acceptable or unacceptable. Again, most people have an idea of how to judge what is unacceptable; and a risk could be said to be unacceptable when a very valuable, or critical, asset is highly vulnerable.

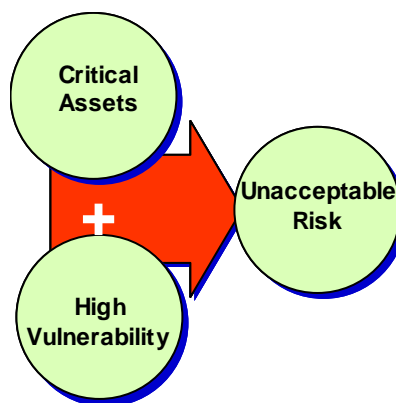


Figure 1. Critical assets + High vulnerability → Unacceptable risk

Formulating unacceptability in this simple way allows us to state that the goal of security management is to prevent valuable assets of the organization from being highly vulnerable.

With this in mind, it is now possible to look at some ways for finding possible responses to the second of the CISO’s challenges:

- Start with the most valuable assets, and analyze, for each one, how they could be put at risk. Then put into place appropriate protective and preventive measures as a result.
- Start with an assessment of the vulnerability of each asset, and proceed to reduce the vulnerability until an acceptable risk level is reached.
- Build risk scenarios that combine asset value and vulnerability. Then analyze the risks and decide what actions should be performed.
- “Mix and match” these three approaches depending on the circumstances.

It is clear, therefore, that there is not a *single* security management method, but a spectrum of approaches that can be used depending on the organization’s business model and size, its security culture, rules of governance, or even the CISO’s personal management style and approach.

While no magic formula exists to choose which approach should be used, all the approaches should make use of reliable tools. The real value of any methodology is to ensure a consistent and complete set of tools, with a means to flexibly move between them. This way, security professionals are assisted in implementing their security management system without having a specific approach or result imposed upon them.

MEHARI was developed in this spirit. It is more than a methodology. It is also a set of tools. Depending on the organization’s needs and circumstances, it ensures that an appropriate security management solution can be designed, whatever approach is used.

The different approaches, and the use of the MEHARI modules, are shown in the diagram below.

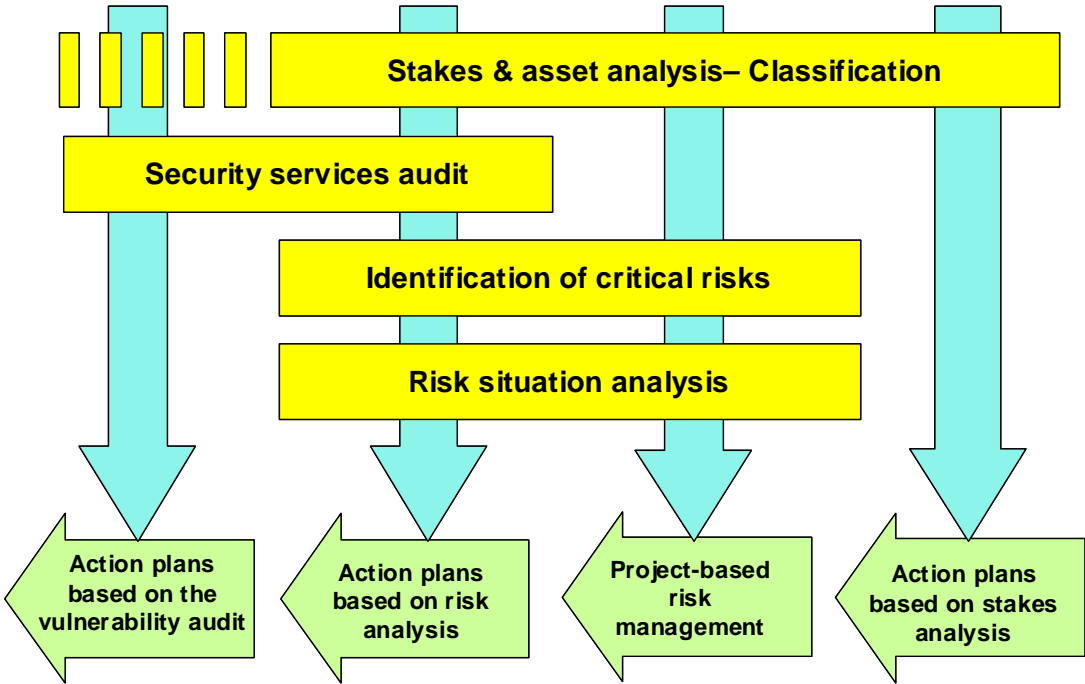


Figure 2. Using MEHARI modules for different approaches to security.

We shall start by describing the different components. Later, we shall show how MEHARI can be used in different circumstances. This will be presented as a learning exercise – and is certainly not intended to dictate the only way it can be used.

## 2 ASSESSMENT OF THE SECURITY STAKES AND THE CLASSIFICATION OF INFORMATION AND ASSETS

---

### 2.1 Introduction

In all forms of management, and managerial decisions, an evaluation must be made of what is at stake, and what will be the impact of the decision on company assets. In security management, this is exactly the case, except that the question is posed from a different angle. Instead of seeking to maximize gains, the goal is to minimize losses.

What is at stake in managing security is not to seek opportunities for profit, but to limit the possibility of loss.

#### 2.1.1 Goals of a security stakes assessment

Such an analysis seeks to find answers to the double question:

“What could happen and, if it did, would it be serious?”

This shows that, in the area of security, stakes can be seen as being the consequences of events that disturb the intended operations of an enterprise or organization.

#### 2.1.2 Why and when should an assessment be made?

The basic question: “What could happen and, if it did, would it be serious?” is the question that is asked each time we reflect on the way we should run operations. This could be when starting a new IT project, during a strategy review, or when a security plan is being created.

Wondering about what could happen is a good question that shows good sense and prudence. Thinking about how serious the effects might be comes from the need to spend more time and attention on the most serious events. Reasons behind this are both economic and cultural:

- Budgets are always limited, and it is therefore natural to give priority to the protection against serious events.
- Security often brings constraint. It is easier to accept them when the stakes are high.

If we agree that security measures should be appropriate to the level of the seriousness of potential malfunctions, then there are a number of ways to proceed:

- Specific analyses for each malfunction, accompanied by the choice of appropriate solutions,
- More systematic approaches with generic solutions used against typical malfunctions and seriousness thresholds for the malfunctions. This second approach leads to the notion of “classification”, which will be discussed later.

Whichever approach is chosen, the first step is to identify the potential malfunctions and their seriousness.

In so doing, it is preferable that this be done systematically, rather than informally, so that the required resources can be dedicated and coordinated properly.

### 2.2 Defining the security stakes: malfunction value scale and classification

Analysis of security stakes entails:

- The identification of suspected malfunctions,
- An evaluation of the seriousness of these malfunctions; in the form of a malfunction

- value scale,
- Classification of assets<sup>1</sup> using the three basic criteria (Availability, Integrity, Confidentiality). The tables used for risk analysis can then be completed.

The malfunction value scale and the classification of information and assets are two separate ways of expressing the security stakes.

The former is more detailed and provides more information to security managers. The latter is more global, and more useful in communicating the level of sensitivity, but less precise.

### **2.2.1 The malfunction value scale**

Identification of malfunctions or potential events is a process that starts with the activities of the enterprise and consists in identifying possible malfunctions in the operational processes. It will result in:

- A description of the possible types of malfunction,
- A definition of the parameters that influence the seriousness of each malfunction,
- An evaluation of the critical thresholds of these parameters that change the level of seriousness of the malfunction.

This set of results constitutes a scale of values for the malfunctions, called the malfunction value scale in MEHARI.

### **2.2.2 Classification of information and assets**

It is usual, in IT system security, to speak of the classification of information and of the classification of IT assets.

Such a classification consists in defining, for each type of information and for each IT asset, and for each classification criterion (classically: Availability, Integrity, and Confidentiality), representative indicators of the seriousness of this criterion being lost or reduced for this asset. So:

- The confidentiality classification for an information represents the seriousness of its being disclosed to an unauthorized person
- The integrity classification for an information represents the seriousness of its illicit or unauthorized modification
- The integrity classification of software represents the seriousness of its illicit or unauthorized modification
- The availability classification for an information represents the seriousness of its not being available when required to be processed
- The availability classification for a server represents the seriousness of its unavailability when required for running a process
- Etc.

The classification of information and supporting assets is the malfunction value scale defined earlier translated into sensitivity indicators associated with the IT assets.

### **2.2.3 The process for analyzing the security stakes**

The process for creating the malfunction value scale and the classification of assets of the information system are described in: « MEHARI stakes analysis and Classification Guide ».

---

<sup>1</sup> It is usual to distinguish primary assets (business activities and related information) and supporting assets.

# 3 ASSESSING THE STATE OF SECURITY SERVICES

---

## 3.1 Introduction

Every security manager, of whatever organization, has, at some point, to consider the current vulnerability of the organization, faced with different possible risks, such as accidents, human errors, or deliberate acts.

Vulnerability is defined in the dictionary as being the exposure to danger. The vulnerability of an information system is the addition of its weak points whereby an accident, error or deliberate act could damage the organization.

In practice, security measures, including control of events or human actions, etc. limit the level of vulnerability.

To this extent, vulnerability analysis requires the assessment of the state of security.

MEHARI considers that security is implemented through security services. An analysis of vulnerability therefore requires a review of the quality of those security services. For short, this review will be called a Vulnerability Review, or Security Audit.

A security audit to analyze existing security may be the basis, or an integral part, of a number of approaches to security management. **Whatever the approach to security management, an assessment of the quality of the security services is often considered as indispensable.**

There are a number of reasons for this:

- Firstly, it is always better to know one's weak points. Even if, in the present configuration of the information system, a weakness can be considered acceptable because no serious consequences would result, it is better to make a note of it so as to take it into account in any evolution of the system, its environment, or new potential attacks.
- Secondly, for many users, a security weakness left in that state is considered as a demonstration that top management does not attach much importance to security in the organization. The more important and the more visible the weakness, the more negative will be the perception of security.
- Finally, any attack that succeeds in exploiting a weakness always gives a negative impression if it is talked about, whatever the real consequences are (managing to access a system belonging to military intelligence and then talking about it, always has a media impact, even if the system was not sensitive).

## 3.2 Security services

### 3.2.1 Definition

A security service is a response to a security need, expressed in generic and functional terms that describe what the service should do, and generally referring to certain types of threat.

A security service describes a security function.

This function is independent of the real mechanisms or solutions that ensure the effective implementation of the service.

For example: the access control service is designed (as its name implies) to control user access, or to only allow access by authorized users.

### 3.2.2 Security services and sub-services

Security services provide functions that can, themselves, require complementary services, or sub-services, as they will be called. In the previous example, access control requires the identification of the people authorized to access specific assets, which in itself calls on an authorization service to know who the user is, which calls upon an authentication service to filter access, which calls on a filtering service, and so on.

A security service can, therefore, be composed of a series of sub-services that are combined to respond to a specific need. **Each component is, in MEHARI terminology, a sub-service of the main security service.** Each sub-service maintains its own characteristics for its own specific function.

### 3.2.3 Mechanisms & security solutions

A "**Mechanism**" is a specific way of ensuring the function of a service or sub-service (whether totally or partially). This may take the form, for example, of a procedure, an algorithm, or some specific technology.

For the authentication sub-service, mentioned above, the possible mechanisms for authenticating to information systems are passwords, tokens, processes and algorithms based on smart card, biometric systems, and so on.

A number of mechanisms are generally possible for a given sub-service. Their selection may often have a direct effect on the quality of the sub-service in question.

A **security solution** is the real implementation of a mechanism and includes the hardware and/or software components required for its deployment, the installation procedures, and operational support, as well as the organizational structures needed for its correct use

### 3.2.4 Types of security services

Some services can be considered to be general measures, where others are technical.

- General measures are security measures that are considered to be generally useful, or even necessary, to the security of the information system. However, their effect may be felt at the level of the organization, security operation or awareness, but with no direct influence on specific risk situations.
- Technical measures have a specific role, a direct objective and have an immediate effect in certain risk situations that can be defined.

### 3.2.5 The security services knowledge base

MEHARI includes a knowledge base of security services and sub-services. This combines more than 200 sub-services applicable to information system security. These are the services that will be audited.

## 3.3 Evaluating security service quality

Security services may vary in performance; they will be more or less efficient in their function, and more or less robust in their ability to resist direct attacks, depending on the mechanisms and processes used.

### 3.3.1 Mandatory parameters

To measure security service performance, a number of parameters must be taken into account:

- Efficiency,

- Robustness,
- Permanency.

### 3.3.1.1 Security service Efficiency

For services of a technical nature, efficiency is a measure of their ability to effectively ensure the required function faced with more or less competent users or more or less unusual circumstances.

Let us take, as an example, the sub-service “Information system access authorization management”, which involves the attribution of users’ access rights. The function of this service is to ensure that only those people who have their management’s authorization actually get the appropriate information system access.

In practice, the efficiency of the service depends on the strictness of the controls on the authenticity of the authorization request, and on the correlation of the hierarchical relationship between the requestor and the user. If all that is required is a simple mail, without any signature or certificate, anybody who knows a little about the authorization process would be able to inappropriately allocate themselves access rights, and the quality of the sub-service would be considered poor.

The efficiency of a service that manages human actions is thereby the measure of the competence required to let a user pass through the checks in place, or even to abuse them.

For services that target natural events (such as fire detection, fire extinction, and so on), their efficiency corresponds to their ability to apply to more or less exceptional or usual events.

If this concerns, for example, a dam that is intended to prevent a river from overflowing due to heavy rains, the efficiency is directly linked to the height of the water (the flood’s strength) which it resists. **In practice, the strength will often be measured as a function of the more or less exceptional character of the event.**

Services providing general measures cannot, in principle, be evaluated as a function of their direct effect, but only on their indirect role.

The efficiency of general measures corresponds to their ability to create action plans or significant behavioral changes.

### 3.3.1.2 Security service Robustness

The robustness of a security service measures its ability to resist an action that is intended to bypass the service, or to restrict its efficiency.

Robustness only concerns those services that are considered technical.

In the preceding example (access authorization management), the robustness of the sub-service depends – in particular – on how easy it is to directly modify the user access rights table, which would thereby allow someone to attribute themselves access rights without need to follow the normal control processes.

When we are dealing with services for managing accidents or natural events (such as fire detection, automatic fire extinction, and so on), their robustness will also cover their ability to avoid being short-circuited or avoided (whether accidentally, or on purpose).

### 3.3.1.3 Security service Permanency

The global quality of a security service requires that the service be **guaranteed over time**.

For this, any disruption of the security service or change in parameters which may interact with its efficiency or robustness must be detected and corrective measures applied.

Permanency depends, therefore, on the speed of detection and the capacity to react.

The Permanency of general measures represents their capability to be rated in terms of implementation or effectiveness and it also requires that indicators and control procedures are effectively in place.

### 3.3.2 Definition of quality levels for security services

The quality of a security service rates its efficiency, its robustness, and permanency. Globally, therefore, the quality of a security service includes its ability to resist an attack on its defenses – although no castle can be considered totally defensible.

Security service quality is scored on a scale between 1 and 4. This scale reflects the competency or determination that is required to break through the defenses, to short-circuit them, or to inhibit or render useless the detection of the service's neutralization.

While this scale of values allows for decimal values, it is useful to give some indication of the integer values for a security service.

#### *Evaluated security service quality level of 1:*

This service has a minimum level. It could be totally inefficient (or not resist) faced with an ordinary user, without any particular qualification, or slightly educated, likewise, in the domain of natural events, it is likely to be of no use in day-to-day problems. For general measures, they will have little or no effect on the behavior or efficiency of the organization.

#### *Evaluated security service quality level of 2:*

The service is generally efficient and remains resistant to the average or slightly competent hacker. However, it is certainly insufficient when faced with an experienced professional in the specific domain (this could be an IT professional, a well equipped burglar, or an expert in physical break-ins). As far as natural events are concerned, the service will be rarely sufficient to cover serious events – even though these are rare. For general measures, a service at this level would only improve day-to-day situations.

#### *Evaluated security service quality level of 3:*

The service is more efficient and resists against attacks and events described above, but could be insufficient against specialized attacks (well equipped and experienced hackers, specialized system engineers, particularly if they have tools or expertise applied to the domain, professional spies, and so on), or against really exceptional natural disasters. For general measures, a service at this level would have some effect across a large number of circumstances, however, it would certainly not provide any guarantees for serious problems or attacks.

#### *Evaluated security service quality level of 4:*

This is the highest level, and the security service will remain active and efficient in the face of all events and aggressions described above. It could however be breached in exceptional circumstances: the world's best code breakers with the world's best code breaking tools (which is possible if some countries want it to happen) or an exceptional combination of exceptional circumstances.

The process used by MEHARI to evaluate security service quality was built to provide quality evaluations corresponding to the above definitions.

### 3.3.3 MEHARI questionnaires for the evaluation of security services

The MEHARI methodology set, besides the method itself, also includes knowledge bases. One of these bases is a security services audit base. It takes the form of questionnaires, with a weighting system applied to the responses.

The detailed structure of the questionnaires and the weighting system are described in "*MEHARI: Evaluation Guide for security services*".

### 3.3.4 Direct assessment of the quality of security services

MEHARI also provides, for those security services defined in the knowledge base, a "*Security Services Reference Manual*", that describes each service, its function, mechanisms and possible solutions, as well as those criteria that might be used to measure the quality of service.

It is thereby possible to directly evaluate the quality of the security services using the quality of service definitions and the indications provided in the manual mentioned above.

## 3.4 The vulnerability review process

Security services, as defined in MEHARI, are security functions and these functions are implemented through security solutions that are, or will be, installed in the organization.

*In practice, assessing vulnerability consists in analyzing or auditing those solutions that have been implemented to ensure the security functions.*

However, there are generally a number of different solutions inside a given organization to ensure the same security function.

For example, physical access control to premises is certainly provided by different mechanisms and solutions – like for access to computer rooms, or other technical centers, such as PABX installations, conference rooms, and major electrical installations.

It is also possible that logical access control to different systems (mainframes, UNIX, NT, and so on) may be managed in different ways depending on the system.

Before even thinking about a process of analysis and evaluation of security services, it is necessary, first of all, to identify those solutions to be analyzed and audited.

In MEHARI this is the reason for what is called the “audit plan” or “audit schema”.

### 3.4.1 The audit schema

Ideally, each single security service should be examined, and all of the solutions that provide these services in the organization should be identified, so that they can be individually audited.

This would probably lead to a heavy workload for a result whose level of detail would be largely superfluous.

Effectively, often a single team or service selects the different solutions to be used. The choices are often made on the basis of practical constraints rather than on different visions of security requirements. The various security solutions may use different mechanisms while remaining consistent as far as security is concerned.

*On this basis, MEHARI suggests the creation of an audit schema distinguishing between variations that will be analyzed at the technical level, coinciding with responsibility domains.*

It may be decided that it is best to analyze the physical security of the management offices, the information system rooms, and other areas separately from one another. The detailed process for building an audit schema is described in detail in the "*MEHARI Evaluation Guide for security services*".

This approach may seem to over-simplify the need for analyzing each variation at the sub-service level, but experience proves that, exceptional cases apart, it is well adapted to a global vulnerability and risk analysis.

### **3.4.2 The vulnerability review process itself**

Once the audit schema has been defined, and the useful variations have been identified, all that remains is to assess the state of the corresponding security services. This may be done through the MEHARI audit questionnaires (some of which may need to be duplicated), or by direct analysis as explained earlier. The process will result in a statement of the quality of the security services. For a more detailed description, see the "*MEHARI Evaluation Guide for security services*".

## **3.5 Summary of the Vulnerability Review**

In summary, the vulnerability review results in the following deliverables:

- An audit schema that distinguishes between different solution domains that have to be analyzed separately.
- An evaluation, for each domain, of the security services. This will take into account the efficiency of each service, its robustness, and its permanency. This evaluation is performed either directly, or using the MEHARI questionnaires.
- A summary of the vulnerabilities.

# 4 ANALYZING RISK SITUATIONS

---

## 4.1 Introduction

Just about every document concerning security speaks of risk management or risk analysis. However, the concept of what constitutes a risk is not necessarily clear or universally understood.

Is fire a risk?

Is the non-payment of a bill or an insolvent client a risk?

Is defamation by a competitor a risk?

Does risk describe a situation, a series of events, or a measure of danger?

So many questions, which cannot be fully answered in this document!

This section will discuss clearer concepts that are easier to understand:

- Risk scenarios or risk situations
- Evaluation of risk levels, or risk evaluation for short.

***A risk scenario is the description of a malfunction and the way in which the malfunction can happen. The malfunction states the potential damage, or the direct deterioration caused by the malfunction, and any indirect consequences. It is usual to speak of a risk situation, where it is understood that the organization is potentially exposed to such a scenario.***

A risk situation is often identified as a result of a stakes analysis. However, it could also be identified at the level of a project, or detected through systematic search. MEHARI assists in these areas by providing a knowledge base of risk scenarios.

This section assumes that the risk situation(s) have been identified. The structured method for identifying risk situations will be covered in chapter [5](#) of this document.

***Evaluating the risk level seeks to quantify the notion of danger.*** The evaluation method used by MEHARI will be described in this Chapter.

## 4.2 Risk scenarios

Earlier in this document, it was explained that analysis of the stakes requires the identification of potential malfunctions and an evaluation of their seriousness.

The description of the malfunction only highlights the type of the potential consequence and possibly the initial degradation of the process. In order to better describe and analyze the complete risk scenario, it is necessary to define the causes and origins of the risk, or the circumstances that give rise to the scenario.

Each scenario will therefore be described as follows:

- The type of consequence (sometimes in relation with the predefined value scale),
- The type of assets implicated by the scenario (sometimes in relation with the predefined critical assets),
- The types of causes that can lead to the risk situation.

A risk scenario that could be envisaged is described below:

<i>Scenario description</i>	
<i>Description of the event and its consequence(s)</i>	<i>Description of its cause and origin</i>
Destruction of basic data used for paying salaries (calculations & parameters)	... due to an operational error: a disk crash preventing data from being read
Destruction of basic data used for paying salaries (calculations & parameters)	... due to deliberate deletion of the files by a member of the operations staff

### 4.3 Analysis of a risk scenario: overall view or "global" approach

The goal of this analysis is to evaluate two characteristic parameters of risk being run by the organization, supposing that the scenario occurs. These parameters are:

- The potentiality of the risk. This represents, in a qualitative way, the probability that the risk occurs. The occurrence cannot be modeled in terms of probability, which is a quantitative view, and so MEHARI prefers the term "potentiality". Potentiality is a function of the context and the security measures in place.
- The impact of the risk on the organization, which represents the seriousness of the direct and indirect consequences of the occurrence of the risk. This impact is a function of the maximum impact, or intrinsic impact, that was defined during classification in terms of stakes (or level on the value scale), reduced by whatever appropriate security measures have been implemented.

To quantify the risk corresponding to the scenario under analysis, evaluations of potentiality and impact will be made on a scale of 4 levels. These levels are described below.

#### 4.3.1 Evaluation of the potentiality of a risk scenario

The objective here is to reply to the simple question:

***"How likely is the occurrence of the risk being analyzed, that is that the scenario completes and creates real damage?"***

Many factors can come into play to make the occurrence of the risk more or less probable. MEHARI provides an analytical approach that distinguishes between different risk factors. It highlights what can make the risk more likely or, conversely, what security measures could reduce the likelihood of its occurrence

Before examining these factors, it is useful to understand the scale of potentiality values.

***Scale of Potentiality values:***

***Level 4:*** very likely

At this level, the scenario can be considered to certainly occur, and in the relatively short term. When it occurs, nobody is surprised.

***Level 3:*** Likely

These are scenarios that could easily occur, in the more or less short term. Hope that the risk does not occur is not ridiculous, but surely shows a certain level of optimism. When it occurs, people are disappointed, but nobody is surprised.

***Level 2:*** Unlikely

These are scenarios that, reasonably, could be considered never to happen. Past experience shows that they have never occurred. They remain, however, "possible", and are not unrealistic.

**Level 1:** very unlikely

The occurrence of the risk is totally improbable. Such scenarios are not strictly impossible as there is always an infinitely small possibility of them happening.

**Level 0:** Not considered

These are scenarios that are so impossible that they are not included in the set of scenarios to be analyzed. Often, and for different reasons, scenarios that are not to be analyzed are classified under this level.

Direct evaluation of potentiality is often quite difficult. The MEHARI approach recommends the analysis of a number of factors:

- Natural exposure to the risk situation
- For scenarios that concern voluntary acts, the risk taken by the perpetrators
- The conditions in which the scenario occurs

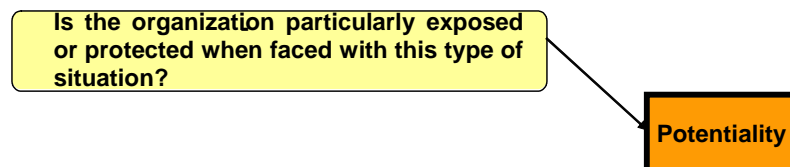
#### 4.3.1.1 Natural exposure

The first question concerning potentiality is the level of exposure to the risk.

The activities of an organization, its economic, social or geographic context, all influence the way in which it is exposed to different types of risk, independently of the measures in force.

- A market-leading high-tech company is more exposed to piracy and industrial espionage than others.
- A company situated on the banks of a river is more exposed to the risk of flooding than others.
- An organization handling many financial transactions is more exposed to the possibility of fraud.

The possible existence of factors that could expose the organization to a given type of risk must therefore be examined.



*For a given risk situation, certain organizations are more exposed than others. The more exposed the organization, the higher the risk.*

Exposure to a given risk can depend on a number of factors:

- Where it is located and its environment, for natural risks,
- The potential gains for the perpetrators of a voluntary act: such as theft, robbery, or intellectual satisfaction.
- The probability that a deliberate act targets the organization (inversely proportional to the number of potential targets)

It is relatively common that natural exposure to a type of risk increases through a combination of circumstances:

- The announcement of a redundancy plan, for internal malevolence,
- Media focus on circumstances or events that might disturb external populations (such as environmental accidents), or bring special attention on the organization (for instance, the announcement of strong security measures).

Conversely, it is sometimes possible to implement measures to reduce natural exposure. These measures are called, in MEHARI, structural measures:

- Management of the environment (physical, social, etc): moving,
- Dispersal of potential targets of intentional attacks,
- Motivation and crisis management.

The natural exposure of the organization to a given risk will be classified on a scale from 1 to 4, as described below:

### ***Natural exposure to risk***

***Level 1:*** Very low exposure

Independently of any security measures, the probability that such a 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 such a scenario will occur, in the short or medium term, 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, such a 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, such a scenario is inevitable in the very short term.

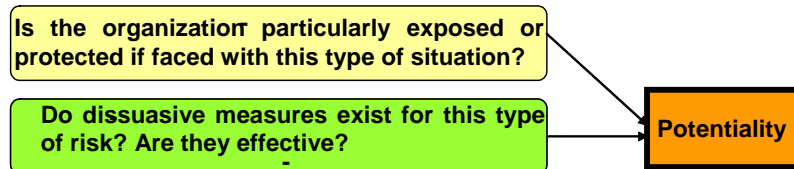
This evaluation is, in fact, a first reflection on the level of potentiality of a scenario in the absence of any security measures.

In the earlier example "Destruction of basic data used for paying salaries (calculations & parameters) due to intentional deletion of the files by a member of the operations staff", analysis should be made of whether there are conflicting relations with the operations staff, whether they are particularly motivated or unmotivated, and whether such a malevolent action is likely to benefit anyone in particular. When no specific reasons can be found, the entity is considered to be hardly exposed (in noting that this has never actually occurred), with an exposure level of 2.

***A good way of evaluating natural exposure is to consider it as a measure of intrinsic potentiality, or the potentiality without any security measures in force.***

#### **4.3.1.2 The risk perceived by the perpetrator of an intentional act**

The second question is limited to those scenarios concerning deliberate acts perpetrated by a real person. Many of these acts are of a malevolent nature. Such an act can represent a risk for the perpetrator, which will have a dissuasive effect. The existence of dissuasive factors should be examined in order to curb the desires of potential perpetrators.



Setting out on a malevolent act can clearly represent a risk for the perpetrator.

*The higher the perception of risk, the less likely that the perpetrator will attempt it, and therefore the risk for the organization is lower.*

The risk as perceived by the perpetrator of an intentional act depends on:

- Existing means to detect the action and to be able to find the perpetrator,
- The quality of proof for the imputation,
- Sanctions incurred,
- The perpetrator's knowledge of means used in previous cases.

As a corollary to this, some actions or measures that generate risk reduction, called dissuasive measures in MEHARI, exist:

- **Detection** of attempted voluntary actions and **recording** of the actions performed,
- **Attribution** of intentional, attempted and performed actions,
- Incontestable strong **authentication**,
- Regulation, with **severe sanctions**,
- **Communication** about detection and recording systems.

The existence of these measures must therefore be examined, but so must their effectiveness.

This effectiveness will be measured on a scale from 1 to 4, as described below:

***Effectiveness of dissuasive measures:***

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

The potential attacker can logically consider that he or she runs no personal risk, as it is unlikely that there is any way to identify the perpetrator. He can therefore consider that he 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, and should realize that he 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. He should realize that he will certainly be identified, and that the resulting punishment will well outweigh any potential gain.

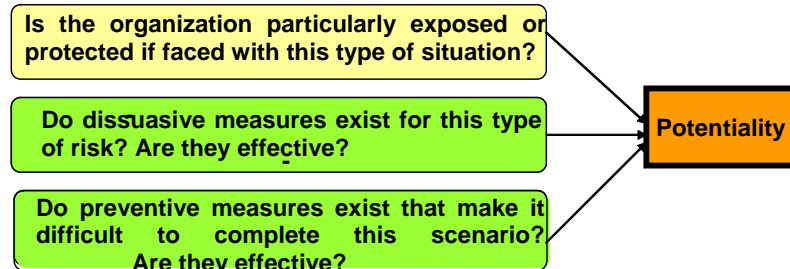
This evaluation provides a second level of thought on the potentiality of the scenario.

For the example scenario described earlier "Destruction of basic data used for paying salaries (calculations & parameters) due to intentional deletion of the files by a member of the operations staff", there is a need to examine the number of people who have access to database file storage cassettes, to see whether these people often have the opportunity to be alone in the computer room, and to check whether the storage cassettes are under CCTV surveillance. Without any strict and visible surveillance, staff can reasonably consider that they run no risk. Such a thinking could lead to considering that

no dissuasive measures are in force for this scenario (level 1).

#### 4.3.1.3 Conditions for a risk to occur

The third and last question that needs to be asked concerns the conditions in which the scenario could happen, and the more or less ordinary nature of these conditions.



*A risk scenario will only end up as a real disaster if certain conditions are fulfilled simultaneously.*

*The more ordinary these conditions, the higher the risk of occurrence.*

The ordinary nature of conditions of occurrence may depend on:

- The ordinary or exceptional nature of external conditions (weather, type of accident, etc.),
- The relatively low level of competence required for an intentional act,
- The knowledge, that is more or less required, of the organization and its context,
- The means and resources required (human, financial, time, etc),
- The degree of luck or chance required.

*As a corollary to this, actions or measures that generate risk reduction, called in MEHARI "preventive measures", exist :*

- Physical security measures,
- Access control measures,
- Preventive controls integrated into computer processes and applications.

The existence of these measures must therefore be examined, but so must their effectiveness.

This effectiveness will be measured on a scale from 1 to 4, as described below:

#### ***Effectiveness of preventive measures***

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

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.

This evaluation provides a third and final level of thought on the potentiality of the scenario.

For the example scenario described earlier "Destruction of basic data used for paying salaries (calculations & parameters) due to intentional deletion of the files by a member of the operations staff", there is a need to analyze whether all, or nearly all, the operations staff is capable of succeeding in such a scenario, or whether specific expertise is required to succeed, or whether special expertise is required. In the case of this example, all of the operations staff could be considered capable of succeeding, and therefore the level of preventive measures is low (level 1).

#### **4.3.1.4 Evaluation of the potentiality of a risk scenario**

*Once natural exposure to the risk under analysis has been evaluated, and the effectiveness of the dissuasive and preventive measures to limit potentiality have been evaluated, then the next step is to evaluate the resulting potentiality of the scenario.*

The global evaluation will make use of the previous reflections and results, and apply the definitions of the levels of potentiality described earlier.

For the example scenario described earlier "Destruction of basic data used for paying salaries (calculations & parameters) due to intentional deletion of the files by a member of the operations staff", with a natural exposure of level 2 and dissuasive and preventive measures of level 1, the resulting potentiality could be considered to be 2, or "Unlikely".

Potentiality is, therefore, a global evaluation of the probability of the scenario happening to completion, on a scale of 4 levels. It includes intrinsic potentiality, measured through natural exposure, and two risk reduction factors: dissuasion (for intentional acts) and prevention.

#### **4.3.2 Evaluation of the impact of a risk scenario**

Here, the objective is to answer the simple question:

*"If the risk being analyzed actually occurs, what would be the final seriousness of the consequences?"*

Many factors can make the consequences of the risk, or its impact, more or less serious. MEHARI provides an analytical approach that identifies the risk factors, while highlighting the influences that can make the consequences more serious, or on the contrary, what security measures could reduce the seriousness of its impact.

Before analyzing these factors, an impact scale is defined below, identical in every way to that introduced in the stakes analysis section above in this document and more detailed in the "Stakes analysis and classification guide".

**Impact scale:**

**Level 4: Vital**

At this level, the possible malfunction is so serious that it endangers even the existence or the survival of the organization or one of its main activities.

If the organization were to survive, there would be durable and serious traces remaining.

**Level 3: Very Serious**

This represents very serious malfunctions for the organization, without necessarily compromising its future.

In financial terms, this would seriously reduce the annual results, although shareholders may well continue to hold on to their shares.

In terms of image, the level of loss of brand image would require many months to recuperate, although the cost of so doing is difficult to evaluate.

Disasters that create notable disorganization for a duration of several months would also be evaluated at this level.

**Level 2: Serious**

This level represents malfunctions that have a marked impact on the operations of the entity, its results or its image, but the consequences are generally supportable.

**Level 1: Insignificant**

The damages resulting from a malfunction at this level have practically no noticeable impact on the results of the entity or on its image, even if a number of people will have to spend a lot of time and energy in restoring the situation to its original state.

Directly evaluating the final, residual, impact of a risk is often difficult. In the MEHARI approach, intrinsic impact is analyzed first, then a number of reduction factors. These are:

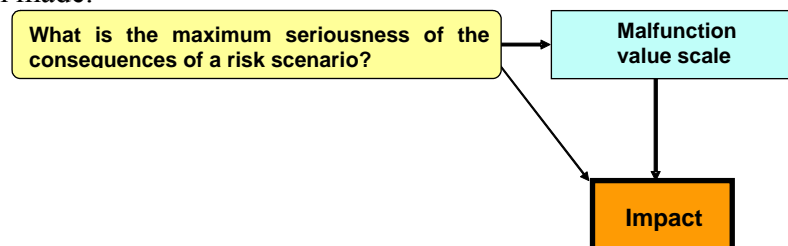
- The attenuation of the direct consequences of the risk through its confinement or isolation,
- The attenuation of the direct consequences of the risk through palliative measures,
- The transfer of all or part of the risk onto a third party.

**4.3.2.1 Intrinsic impact**

If the scenario being analyzed has been created as a result of a stakes analysis and starting with a potential malfunction, the seriousness of the malfunction has already been evaluated using the value scale.

If the scenario is created without any prior stakes analysis, for example as a part of a project, the intrinsic seriousness should be evaluated using the process described in the “*MEHARI stakes analysis and classification guide*” .

It is therefore supposed that a preliminary evaluation of the impact of the scenario on the value scale has been made.



It is worth noting that this first estimation is a maximum estimation. In fact, during that step, the

security measures that could reduce the seriousness of the consequences of the potential risk should not be taken into account.

It is during the risk analysis that these measures will be taken into account.

***The first impact evaluation, deduced from the malfunction value scale or evaluated directly, can be considered as the intrinsic impact, in other words the worst case (or maximum value) for the consequences of the risk without any security measures.***

For the example scenario described earlier "Destruction of basic data used for paying salaries (calculations & parameters) due to intentional deletion of the files by a member of the operations staff", the malfunction value scale provides a reference value for the deletion of such data (and if no malfunction concerning pay data appears in the value scale, the corresponding impact would be considered negligible). To continue with the example, the malfunction value scale for the loss of this data would be considered to show level 3 (very serious).

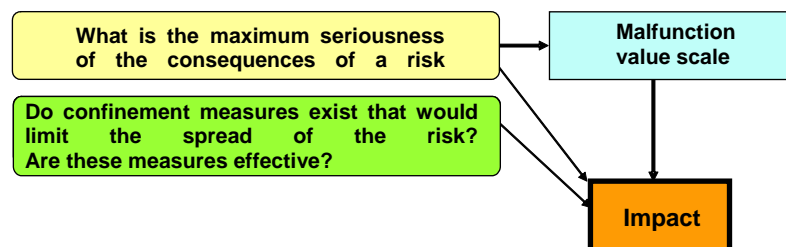
#### 4.3.2.2 Limitation of direct consequences: risk confinement

The first question to be asked concerning risk limitation is the limitation of the direct consequences of the occurrence of the risk.

Certain damages resulting from an event can, in effect, be limited in space or time by prior intervention or precautions:

- A fire can be limited to an area by a number of means (firewalls, other separators,..) or by direct intervention (detection and extinction).
- Flooding can be limited in its direct consequences through intervention (detection of leaks or damp, shutting of pipes,..) or through specialized means (overflows, natural drainage,..).
- An error can be limited in its spatial effects (propagation) or in time, by detection systems or control procedures.
- The proliferation of a virus can be stopped using anti-virus systems.
- Hacking can be limited in time or importance through intrusion detection systems and associated means.

Clearly, questions must be asked as to whether there exist factors that would limit the seriousness of the direct consequences of a risk, spatially or temporally, and this compared to the initial maximal seriousness level originally evaluated.



***The direct consequences of a risk scenario that actually happens can spread or propagate in time and space, or be confined.***

***The risk will be greater if the confinement is weaker.***

The confinement of direct consequences of a risk may depend on:

- Isolating assets from one another, or compartmentalization.
- Detection measures specific to the risk in question,

- The organization's ability to react when faced with this type of risk.

**Corollary :** Actions or risk reduction measures exist, that are confinement measures, exist, also called "protection<sup>2</sup> measures" in MEHARI.

- Measures for isolation and physical compartmentalization,
- **Detection measures** (intrusion, accidents, errors, etc.)
- **Post-controls** integrated into computer processes and applications,
- Investigative capabilities on anomaly detection.
- Rapid intervention capabilities.

The existence and effectiveness of these measures needs to be examined.

Their effectiveness will be evaluated on a scale of 1 to 4, following the description below:

### ***Effectiveness of protective or confinement measures***

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

Either the damage and its direct consequences cannot be limited, or it will not be detected for some time.

The possible corrective measures will 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 possible corrective measures may have a certain influence on the impact, 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 possible corrective measures will have a certain 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 and measures are immediately set in train.

Direct consequences are limited to deterioration immediately due to the accident, error or deliberate (sometimes malevolent) action.

This evaluation provides a first level of reflection on the real level of the direct consequences of the scenario.

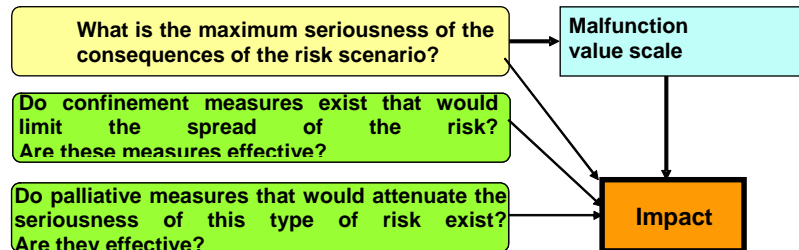
For the example scenario used throughout this section "Destruction of basic data used for paying salaries (calculations & parameters) due to intentional deletion of the files by a member of the operations staff", an examination should be made to identify if any confinement measures exist that ensure intervention before the culprits have totally deleted the data files and their histories. The answer is probably no, if the historical data does not have a specific management system, permitting anomaly detection. .

<sup>2</sup> These measures, called protection measures in MEHARI, are often detection/reaction measures.

### 4.3.2.3 Limitation of indirect consequences of a risk: palliative measures

The second question to ask, concerning the consequences of a risk, is about the possible reactions once the event has been detected and the damage contained.

No organization would fail to react, however the level of the real consequences will depend on the quality of the reaction.



*The crisis situation brought about by the occurrence of a risk can be anticipated and prepared.*

*The less preparation, the higher will be the risk.*

The level of preparation for a crisis situation depends on:

- The prior identification of acceptable degraded modes of operation: minimum functions to be fulfilled and indispensable services,
- Anticipation and preparation of appropriate palliative solutions,
- Preparation and training of staff to deal with crisis situations (crisis management, crisis communication, etc).

**Corollary:** actions or measures exist for the reduction of indirect consequences. These are called "palliative measures" in MEHARI, and include:

- Prior examination of which minimum services should be provided as well as contingency planning,
- **Preparation of maintenance and recovery plans** (back-up plans, business continuity plans, restoration plans, etc),
- Preparation and training of teams (technical tests, media-training, etc.).

The existence and effectiveness of these measures needs to be examined.

Their effectiveness will be evaluated on a scale of 1 to 4, following the description below:

#### ***Effectiveness of Palliative measures***

**Level 1:** The effects of the limitation of the indirect consequences are very low or null. Either totally improvised measures are used or it is considered that they will have no effect.

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

The recovery 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 measures. The time to re-establish normal operations cannot be precisely predicted, or will not fundamentally change the seriousness 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 will continue without any noticeable interruption.

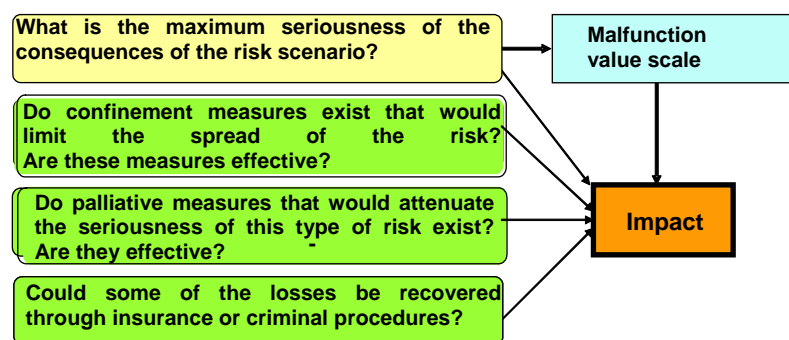
This evaluation provides a second type of reflection on the real level of the indirect consequences of the scenario.

For the example scenario used throughout this section "Destruction of basic data used for paying salaries (calculations & parameters) due to intentional deletion of the files by a member of the operations staff", an analysis should be made to see whether back-ups are made as palliative measures, and whether these back-ups will ensure the restoration of the database, at least for the past years' historical data. This would reduce the impact level to 2 (the destruction of the current year's data having been evaluated to level 2 during the stakes analysis), or even to limit the data loss to the current month, which would reduce the impact to level 1. The result will of course depend on whether back-ups are made, but also on their maximum possible age (and therefore their frequency).

#### 4.3.2.4 Limitation of overall losses: risk transfer

The third and last question about consequences of a risk concerns the possibility of reducing the losses by transferring some of them onto a third party.

Typically, this would concern insurance or criminal procedures.



**Overall losses can be potentially partially transferred onto third parties such as insurance, or through criminal procedures.**

The effective character of this transfer depends on:

- The prior identification of specific IT risk situations that should be covered by insurance,
- Insurance policies appropriate to the risks that should be covered,
- Precise analysis of situations that are excluded, and subsequent measures that are taken,
- Preparation of elements of proof, with a view to potential criminal proceedings, and the validation of their acceptability in a court of law (“forensics”).

**Corollary:** actions or measures exist to reduce the risk, called "recuperative measures" in MEHARI. These include:

- Specific analysis of risks that should be covered by insurance policies,
- Coverage of risks that are above a level accepted by insurers,
- Specific preparation of criminal proceedings.

The existence and effectiveness of these measures will be evaluated on a scale of 1 to 4, following the description below:

#### **Recuperative measures:**

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

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 is expected to remain supportable.

**NOTE:**

The above definitions correspond to what insurers generally expect. In fact, insurance policies are not intended to make consequences of a risk completely negligible but usually to avoid the insupportable, or at least to limit the scope of the consequences of serious but supportable risks.

This evaluation provides a third and final level of reflection on the real level of the global consequences of a scenario

For the example scenario used throughout this section "Destruction of basic data used for paying salaries (calculations & parameters) due to intentional deletion of the files by a member of the operations staff", an analysis should be made to see whether insurance policies would reduce the level of risk, and whether a legal case would be successful (which would suppose, among other things, that the person concerned would be found guilty, and would have enough money to cover the damages). In the case of this example, the answer would appear to be no.

#### **4.3.2.5 Evaluating the global impact of the risk scenario**

*The intrinsic impact that was defined through the value scale and the evaluation of the effectiveness of attenuation measures that would limit the impact of the risk (protective, palliative and recuperative measures) will provide the global impact of the scenario.*

For the evaluation of the global level of risk, see the definitions given earlier.

The preceding levels of reflection should be taken into consideration during the global evaluation.

In the example scenario used throughout this section, the residual global impact can be evaluated at level 2 (serious), or even 1 (negligible) if, despite the absence of protective or recuperative measures, the palliative measures are considered to be sufficiently effective.

*Impact is therefore a global evaluation of the level of the consequences, on a scale of 4 levels, which takes into account the intrinsic impact and three risk attenuation factors (protective, palliative and recuperative).*

#### **4.3.3 The resulting seriousness of a risk situation**

The seriousness of a risk scenario or risk situation is a function of its potentiality and its impact.

This is not a simple mathematical formula using the two values, but rather a judgment on the acceptability (or not) of the situation.

As a function of the potentiality and impact of the risk being analyzed, the only remaining question is:

***Is this risk situation acceptable as it stands, otherwise what should be done?***

For the example scenario used throughout this section "Destruction of basic data used for paying salaries (calculations & parameters) due to intentional deletion of the files by a member of the operations staff", a decision has to be made as to whether it is acceptable that the operation staff might be able to delete the database, even though the occurrence is unlikely while its impact is limited, but high all the same.

If several risk situations are to be analyzed, at different points in time, it may be worth creating a decision table to ensure the coherency of decisions taken at different times or by different people.

This decision table can be represented by a "risk acceptability table" or "risk aversion table" that defines, as a function of estimated impact and potentiality, whether the risk is acceptable.

MEHARI proposes three categories of risk:

- Unsupportable risks, which require urgent measures, above and beyond normal budget cycles.
- Inadmissible risks, which need to be reduced or eliminated at some point in time. This should be integrated into the planning cycle (security plan).
- Tolerable risks.

The first two categories correspond to what has previously been called unacceptable risks.

A sample risk acceptability table is shown below. In this example, S is the global seriousness evaluated as a function of the impact (I) and potentiality (P). A seriousness level of 4 corresponds to an unsupportable risk, level 3 to an inadmissible risk and the lower values to tolerable risks.

I = 4	S = 2	S = 3	S = 4	S = 4
I = 3	S = 2	S = 3	S = 3	S = 4
I = 2	S = 1	S = 2	S = 2	S = 3
I = 1	S = 1	S = 1	S = 1	S = 2
	P = 1	P = 2	P = 3	P = 4

Figure 4: Risk acceptability table

**4.3.4 Overview of the risk analysis process**

The approach that has just been described can be summarized by the figure below:

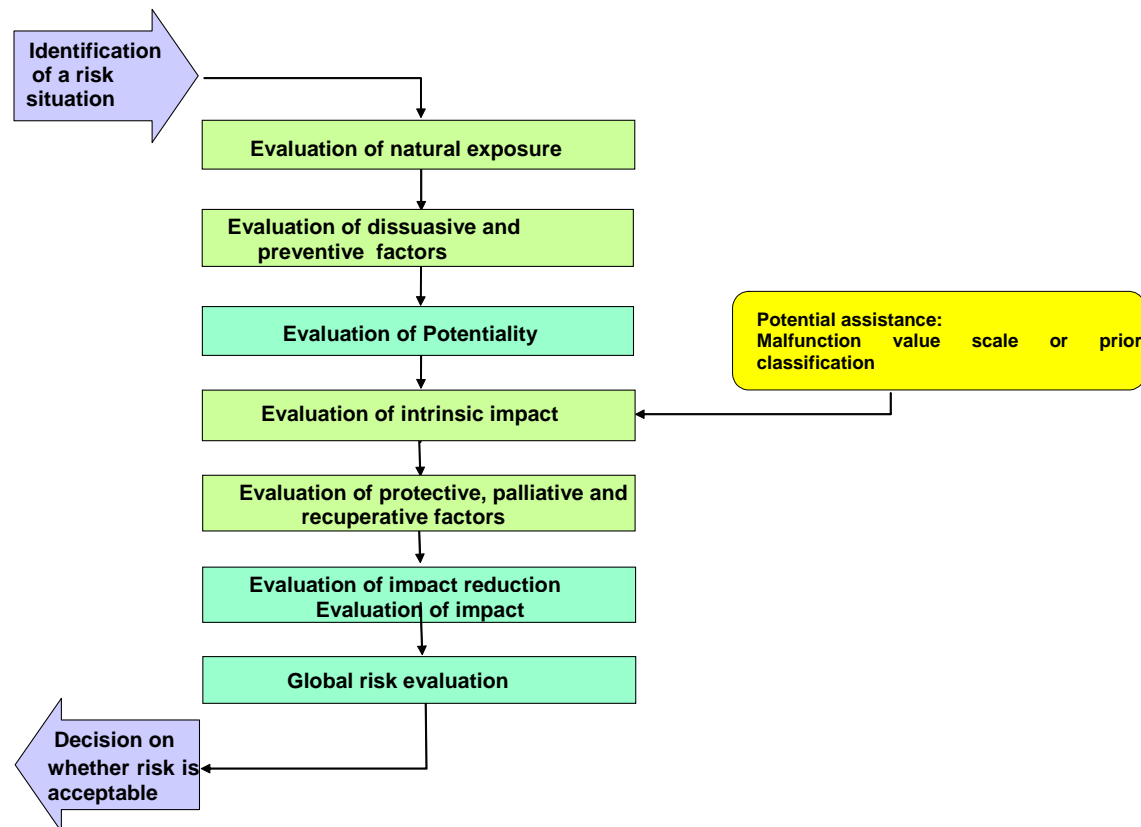


Figure 5: Risk situation analysis

## 4.4 Using the MEHARI knowledge bases

Among its knowledge bases, MEHARI provides a risk scenario base (“*MEHARI scenario reference manual*”).

A number of situations exist where it is appropriate to use this knowledge base:

- The scenarios of the knowledge base are described in a general way, so that they can be used for the more frequently encountered risk situations. Frequently, a specific risk situation, detected during a project or due to management's request for more detail, corresponds very closely to one of the scenarios in the base. So, the example scenario used throughout this section "Destruction of basic data used for paying salaries (calculations & parameters) due to intentional deletion of the files by a member of the operations staff", corresponds to scenario 10.31 of the MEHARI base: "massive destruction of archives and data by operations staff".
- Approaches also exist that consist of analyzing all the risk situations that appear critical. The knowledge base can be used to select the scenarios, and then proceed with their analysis.

### 4.4.1 Using the risk scenario reference manual

The previous paragraphs have given generic definitions of natural exposure to risk and of the effectiveness of dissuasive and preventive measures. Similarly, generic definitions were given for intrinsic impact, the effectiveness of protective, palliative and recuperative measures.

The MEHARI scenario reference manual gives, for these different factors, and for each scenario in the base, definitions that are properly adjusted to the case in question. In addition to the definitions, the base provides, in comment form, details relating to pertinent questions that help in evaluating each of these parameters.

The detailed risk analysis process using the MEHARI knowledge bases is described in a specific document: "*MEHARI Risk Analysis Guide*".

#### 4.4.2 Using MEHARI automated procedures

MEHARI provides, in its knowledge bases, a number of aids for risk analysis:

- Assistance in evaluating natural exposure,
- Automated procedures for evaluating risk attenuation factors (dissuasive, preventive, protective, palliative and recuperative) as a function of the quality of the security services if previously evaluated by a MEHARI audit.
- A generic intrinsic impact table that can be enhanced as a result of a classification procedure or directly from a malfunction value scale.
- Automated procedures for calculating potentiality and impact, as a function of natural exposure, and of intrinsic impact and risk attenuation factors.

In order to facilitate the global approach of MEHARI, these aids are applicable for each of the scenarios referenced in the MEHARI scenario base.

The risk analysis process using MEHARI scenario base and its automated procedures are detailed in "*MEHARI Risk Analysis Guide*".

### 4.5 Risk situation analysis process

In summary, the risk situation analysis process includes a basic, or global, approach, with the possible assistance of automated procedures, depending on the way the situation is described and on the existence of a prior audit of the security services.

The overall process and the assistance capabilities that MEHARI may provide for the study of risk situations (either extracted from MEHARI base or similar) are shown below:

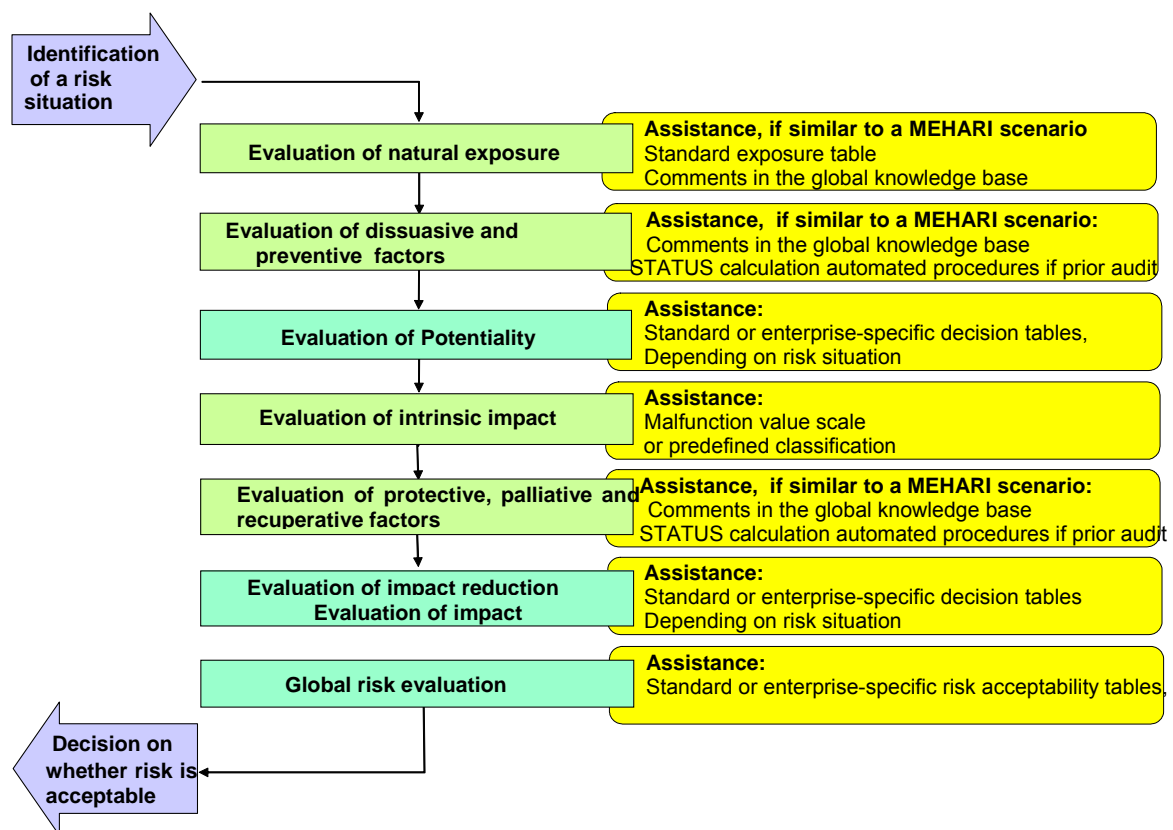


Figure 6: The Risk Analysis Process, and MEHARI aids and assistance

It is worth noting that the automated procedures mentioned above are optional at each step. Practically, this means that the results they generate should always be considered as propositions, and be validated before being accepted and applied in the organization.

## **4.6 Summary of the risk analysis approach**

In summary:

- A risk situation can be characterized by its intrinsic potentiality and impact, in the absence of any security measures.
- Intrinsic potentiality and impact can be evaluated.
- Security measures can reduce the intrinsic risk through significant risk reduction factors.
- Risk reduction factors can, themselves, be evaluated.
- On this basis, it is possible to evaluate real potentiality, residual impact, characteristic of the risk, and to deduce a risk seriousness indicator.
- MEHARI provides tools to assist throughout this process of analysis and evaluation.

## 5 IDENTIFYING RISK SITUATIONS

---

The previous chapter covered the analysis of a specific risk situation. The identification of those risk situations to be analyzed is obviously an important prior stage for which tools are key.

There are two main ways to identify risks:

- A direct approach, using the malfunction value scale,.
- An organized and systematic approach with an automated evaluation using the scenario base provided by MEHARI.

### 5.1 The direct approach using the malfunction value scale

To each type of malfunction, identified during a security stakes analysis and listed in the malfunction value scale, corresponds a set of scenarios that have been identified by finding the possible causes for the malfunction, or through its possible origins (see the explanation in subsection [Risk scenarios](#)).

It is, therefore, easy to build a risk scenario base as a result of the malfunction value scale.

All of the scenarios with a high level of consequences (levels 3 or 4) should be considered as critical and examined in further detail.

### 5.2 Systematic identification using the knowledge base

MEHARI also provides assistance in the systematic identification of risk situations.

The systematic identification will use MEHARI knowledge base of risk scenarios and the automated procedures already described in the previous chapter. This is based upon:

- A preliminary security stakes analysis, embodied by a malfunction value scale and a classification of primary and supporting assets.
- A security audit.

The automated procedures are used to highlight those scenarios that could have an unacceptable seriousness (generally 3 and above) using the risk acceptability table.

From the specific scenario base and the automatic evaluation of their seriousness, it is easy to select critical scenarios. This means those that need to be analyzed using a risk analysis approach as described in the previous chapter.

**NOTE:** It would be wise to consider, for this automatic selection, an acceptability table that is relatively severe. This table can be different when used to identify critical scenarios than the one used for identifying the final and overall seriousness of the risk situation. Consider the (relatively severe) table shown below:

I = 4	S = 3	S = 3	S = 4	S = 4
I = 3	S = 2	S = 3	S = 3	S = 4
I = 2	S = 1	S = 2	S = 3	S = 3
I = 1	S = 1	S = 1	S = 1	S = 3
	P = 1	P = 2	P = 3	P = 4

Seriousness function of Potentiality and Impact

### **5.3 The two approaches are complementary**

Clearly, the two ways of identifying critical risk situations (direct selection, using malfunction value scales, and the automatic identification, using the knowledge bases) start with different points of view and will, inevitably highlight different scenarios.

The first approach will highlight the scenarios that are closest to the organization's core activities and to the managers' concerns, so they will be more relevant to users. The second approach is more detailed, though more generic, and will additionally bring out those scenarios that are of lesser impact but higher potentiality that might otherwise have passed unseen in using a direct approach.

The two approaches are complementary and should be run concurrently.

---

## 6 USING THE MEHARI MODULES

---

The MEHARI modules can be applied in a wide range of ways. Similarly, there are many different security management approaches that can benefit from MEHARI and its knowledge bases. There is, therefore, no reason to impose a standard use of the modules.

This chapter aims to illustrate the added value of MEHARI in security management, through three structured approaches that its designers have had the opportunity to implement, and which have proven their effectiveness.

### 6.1 Security plans based on risk analysis

Generally, security plans are created to define, deploy and implement or reinforce security services.

This subsection will describe plans that are created using an organized and methodical risk analysis.

Before proceeding further, it would seem useful to distinguish between two different levels of decision:

- Firstly, a central level of decision, which ensures consistency of actions and that they are appropriate to the corporate stakes of the organization.
- A second level is that of autonomous units, who make local decisions required for security. This is a classic situation for large organizations, but is becoming more commonplace, with organizations divided into separate Business Units, each responsible for their own results.

The decisions at the first level are strategic, while those of the second are of an operational nature.

Another way to distinguish between the strategic and operational aspects is to consider the long- or short-term character of the decisions.

- The strategic level concerns long-term decisions, those that are associated with the core functions of the organization and independent of the processes or technology that is implemented.
- The operational level deals with day-to-day decisions that may be changed as a function of evolving processes or technology.

The strategic level ensures consistency of decisions over time by accentuating the importance of the decisions that have a long-term impact.

**NOTE:**

The distinction between strategic and operational decisions may be inappropriate or inapplicable to certain situations.

Such a distinction is, however, appropriate to the vision of large organizations with many separate units. It can also be appropriate for long-term actions. It is, however, useful to make this distinction for reasons of consistency or planning cycles.

For selected or limited actions, the formal distinction between strategic and operational decisions may bring extra complexity, and it should then be ignored.

However, whatever the management style or approach, it makes good sense to distinguish between fundamentals that drive long-term actions from short-term operational plans.

## **6.1.1 The approach at the strategic level: identifying permanent and independent elements of the operational security plans**

The aims of the strategic level are:

- To define the security goals that will guide managers who have to make decisions concerning risk management,
- To identify the types of solutions that should be implemented as a priority.

It therefore represents a global, strategic view that responds to two distinct needs:

- To implicate the top management of the company or unit in the selection of security objectives. This entails their acceptance of a certain number of risks and the adoption of management tools appropriate to their level.
- To provide security managers, and management in general, with the appropriate elements to maintain consistency in the operational decisions that are taken.

There are three main components at this level, which can make up three separate steps when a strategic plan is being created:

- The formal creation or validation of a corporate security policy.
- Fixing security goals and agreeing risk measurement parameters.
- The formal creation or validation of a corporate security management charter.

The content of these different elements will be described below. Note that these elements can be considered independent from operational plans, given that, for actions that are limited in time or space, certain aspects can be considered as superfluous, and may be ignored.

### **6.1.1.1 Security policy**

Security policy dictates the general security orientations of the organization.

It is an important foundation document that should be distributed to all staff. It should, therefore, be totally independent of any professional working method or technology.

Creating a security policy is not always part of the creation of security plans. Indeed, it is preferred that this document should have been created some time previously. However, if it does not exist, its creation is strongly recommended if the organization is committed to global and sustainable risk analysis based security management.

The security policy should cover four principal domains:

- The overall organizational structure, and in particular, the structures that are involved in security management:
  - Roles and functions of security managers in the different units (central function, local function, local security correspondents, etc.).
  - Roles and responsibilities of operational managers and their hierarchy.
  - Individual responsibility of each member of staff.
  - Structure of the organization's expert council (whether formal or informal) and how expertise is shared.
- The foundation elements of an enterprise security culture:
  - The declaration of a number of basic principles that should be common to all departments. Among these common principles, the following could be examples:
    - The need to act as a function of the sensitivity of information and assets; and

therefore the need to define a classification of them.

- The identification and role of owners of information or assets,
- Conditions in which rights and privileges are granted,
- The principle by which every action can be audited,
- The possibility to monitor the work of every manager, and the rights and obligations of their management in this area.

This list is not exhaustive and all principles that contribute to ensuring the *consistency of behavior* of all those involved in security throughout the organization are the subject of this chapter.

- The general common classification schema used for all parts of the organization: classification levels, classification criteria, general definitions of sensitivity levels, etc.
  - The obligation to raise awareness and train staff in security and key elements that ensure that such training shares common principles.
  - Federating elements that ensure consistency of solutions that are implemented. In considering implemented technical security solutions, two points should be particularly considered:
    - The security of those elements that are, by nature, common, such as the global enterprise network and certain infrastructures that have to be shared.
    - The choice of security architecture elements that push the organization in a particular direction for structuring solutions, and which by nature have an important strategic influence on the ability of future evolution of information systems.
  - These two elements represent high stakes for each of the departments and for the whole organization or enterprise. It is therefore very important to define in the security policy:
    - How actions in this domain are carried out,
    - Who takes the initiative for them, and who ensures coordination,
    - Who has the last word in decisions that commit the organization to a direction?
- In addition to these two specific aspects, all those principles that contribute to ensuring *consistency of technical decisions* concerning the global security of the organization are of concern in this chapter.
- Ways and means for ensuring operational management of security.
    - The choice of security management methods,
    - The security audit tools, means and structure inside the organization,
    - The security monitoring structure and the creation of measurement systems at both the departmental and corporate levels.

### 6.1.1.2 Security objectives and tuning of risk measurement parameters

In management through risk analysis, the decision to accept or refuse a risk situation is an essential management action. Security goals are composed of criteria that define whether a risk is acceptable or not.

MEHARI, no doubt the most advanced approach to risk management, suggests the use of an acceptability table (see [resulting seriousness of a risk situation](#)). Such a table should be defined at this stage in the use of the approach.

In terms of measurement, creating this table will enable the conversion of the evaluation of the two parameters, potentiality and impact, into a single measurement, namely the seriousness, of a

risk.

In any case, for ensuring consistency while using MEHARI automated procedures in the various business units or over time, certain parameters used by these procedures need to be fixed. These parameters are described in the "*MEHARI Risk Analysis Guide*".

### **6.1.1.3 The management charter**

The management charter covers security policy aspects concerning the relationship between the organization and its employees. It is separate from the security policy itself as, often, there are aspects that are not for total distribution to the entire staff.

Generally, the rights and obligations of staff should be covered, but also those of the enterprise.

Sanctions, and how these are qualified, should also be clearly defined

The sort of points that should be covered are:

- The trace-ability of individual actions, and the ability to attribute actions,
- The possibility to monitor activity in real-time,
- The possibilities for audits and control procedures,
- The obligations and responsibilities of staff,
- Sanctions that are applicable when there is a breach of company ethics,
- The possibilities of, and limits to, investigations in the case of anomalies or incidents,
- etc.

It is important, since this strategic level, that the rules that the enterprise or organization will follow and apply, be properly defined for the staff.

Certain measures, in particular those that cover dissuasion, are only effective if the organization has a clear policy and ensures that it is firmly applied, and therefore applies sanctions in case of breach of procedures. If human resources or general management are not determined to apply a rigorous policy, to follow the necessary investigations when anomalies or incidents occur, do not instigate control and audit procedures throughout the organization concerning all actions performed by staff, it is better to know immediately so as to not base a strategy on principles that will never be followed.

In any case, managers who will have to make decisions concerning risk management will need to know what to do.

#### **NOTE:**

This kind of document can be difficult to create and sensitive in its communication. Its formal creation is therefore not always the rule. However, in the spirit of MEHARI, this step, led by the CISO or a consultant would seem essential.

### **6.1.2 The creation of operational security plans**

At the operational plan level, the approach is more concerned with functional specifications of solutions that should be implemented, and the planning of such solutions.

This process is run internally to an entity with independent powers of decision and results in a plan, known in MEHARI as "**operational plan**".

Its goals are:

- To have a precise analysis of the risks involved,
- To provide a detailed specification of solutions and security measures that should be implemented,
- Plan the necessary improvements over time.

The approach is essentially the responsibility of the CISO or risk managers (who could be

operational managers), or both.

There are five main steps to creating an operational plan:

- Stakes analysis and classification of information and information system assets,
- A security vulnerability review,
- Identification and evaluation of potential risks for the entity,
- The expression of needs for improvement in security,
- The creation of a security action plan.

#### **6.1.2.1 Stakes analysis and classification**

The MEHARI approach is described in detail in the “*MEHARI stakes analysis and classification Guide*” and distinguishes between:

- The malfunction value scale,
- The classification of information and information system assets,
- The creation of the intrinsic impact table used by the risk scenarios knowledge base.

It should be noted that, for risk analysis based management, the malfunction value scale is mandatory, while the formal classification step is optional. It is sufficient to use the value scale to evaluate the intrinsic impact for each risk scenario analyzed. In practice, MEHARI suggests that the evaluation of intrinsic impact be systemized through the use of an intrinsic impact table. This being used later by the automated procedures provided by MEHARI.

NOTE: The stakes analysis can be considered as a part of the strategic approach, as it usually remains valid for a long period of time.

#### **6.1.2.2 The vulnerability review, or security audit**

This is the security audit that was described in [Assessing the state of security services](#). The term "security audit" is often used, although it is often no more than a review. It is worth noting here the difference between a review that uses questionnaires and a true audit that checks whether the policies and rules are effectively applied.

#### **6.1.2.3 Risk identification and evaluation**

This concerns the identification of risk situations, as described in [Identifying Risk situations](#), and their quantitative evaluation, as described in [Analyzing Risk Situations](#).

This step results in a set of risk situations that can be considered inadmissible, and which must be reduced to an acceptable level through an action plan.

#### **6.1.2.4 Expressing needs of improvement in security**

This step is specific to this type of management, as it effectively concerns the analysis of a set of risk situations that should be treated globally.

Before creating a real action plan, there is a need to define what is required of security services that might transform inadmissible risk situations into tolerable ones.

In the usual case, where risk analysis and vulnerability review have been run with the help of a security professional, the CISO or an external consultant, there is little need for an additional methodology or specific tools to express these needs:

- The analysis, for each risk situation, of the types of measures that are already used and an evaluation of their effectiveness will give an immediate idea of the additional measures required to reduce the risk level.
- The vulnerability review or security audit additionally provides a clear idea of the major problems that must be solved, independently of any risk analysis.

- A comparison of the state of security, as evaluated through the security audit, and the security policy will result in the identification of specific needs.
- 

MEHARI provides, among other tools, an algorithm for selecting security measures. This is described in the "*MEHARI Risk Analysis Guide*".

#### **6.1.2.5 Taking general or organizational measures into account**

The chapter [Assessing the state of security services](#) discussed general measures that do not have any direct effect on risk scenarios.

However, any weakness, detected in the general measures, must be covered during the creation of operational plans. These measures, although they may not have any direct effect on the risk scenarios, may be indispensable in motivating staff and in making them adopt the security goals of the organization.

More often than not, this simply requires good sense. The assistance of a security professional will usually be enough to ensure that the most important points are covered.

#### **6.1.2.6 Creating an operational security plan**

As in the definition of security needs, there is rarely need for any specific tools or methodology to build a security plan from the expressed requirements.

Experience would recommend, however, that it is better as a first step to group measures around projects with the same theme (logical security, backup planning, etc), or in more specific sub-projects (in backup planning there are "making backups", "restoring from backups", "mission continuity planning", etc) . The sub-projects should then be allocated a priority level, taking into account their impact on the seriousness of scenarios and the potential difficulty of implementation (given that some projects impose constraints on others).

#### **6.1.3 Consolidating operational plans from different independent departments**

This phase, which is enterprise-wide, ensures the consolidation and consistency of operational plans of the different independent departments and provides a framework for arbitration, should it be required.

This can also be the opportunity to re-balance different departments, if the group responsible for the consolidation has this mandate.

The figure below illustrates the overall approach.

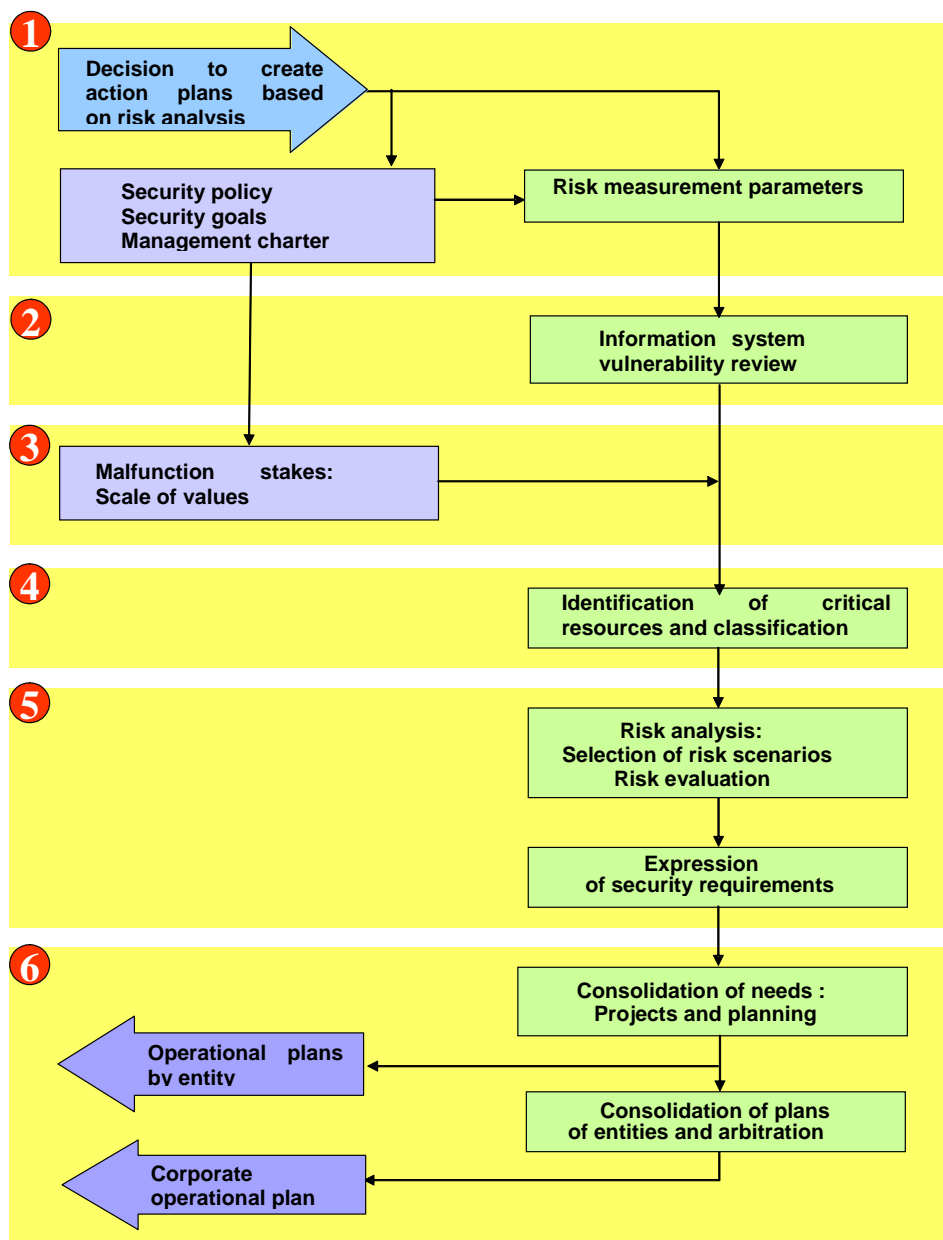


Figure 7: Creating security plans based on risk analysis

## 6.2 Security plans based on an audit

A relatively common approach is to create security plans directly as a result of a security audit, or after a vulnerability review.

Many people, who used the Marion methodology in the past, simply applied step 3 of that methodology: an action plan based on an audit.

Depending on the circumstances, this approach may be practical, and MEHARI provides the means to do so.

### 6.2.1 The process for creating security plans based on an audit

The process for running an audit is extremely simple: it comprises a vulnerability review and the resulting action plans for improving those services that do not have a sufficient quality level.

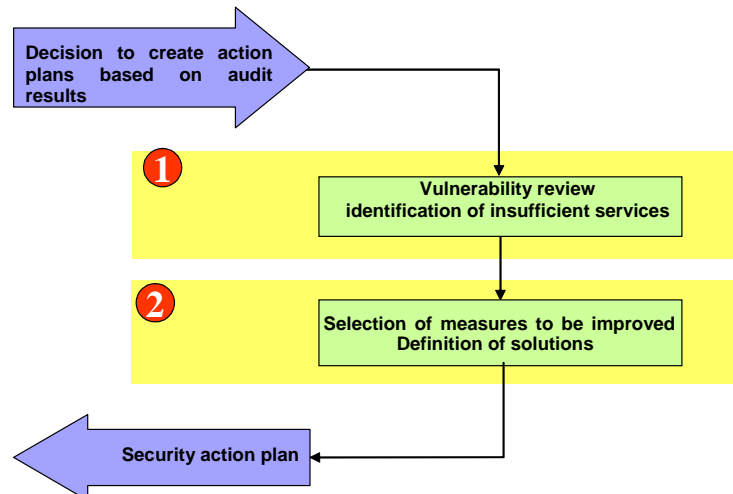


Figure 8: Managing security through an audit

## 6.2.2 The audit questionnaire and weighting of questions

Two points need to be raised concerning the questionnaire used during an audit:

- Can a questionnaire that is specific to this approach be the same one that is used during risk analysis?
- Can, and should, the weighting of responses be the same?

There is no universal response to these questions, and their answers will depend on how mature the organization is in terms of security.

If the organization is only at the stage of first reflections on information system security, a lightweight assessment should be sufficient. However, if there has already been a serious approach to information system security for some time, a more detailed audit would be more appropriate. The first case would seek to identify the most obvious weaknesses and correct them while raising management awareness and accepting that certain weaknesses will remain. In the second case, however, a complete plan will be created so as to have homogeneous coverage providing a satisfactory level of security.

### 6.2.2.1 Security reference policies and scoring for a light assessment audit

The term "security reference policies" refers in general to the set of rules that will be verified during an audit. In this case, it includes the set of questions that will be asked.

In a light assessment audit, it is neither necessary nor desirable to spend a lot of time with technical managers in asking numerous questions whose answers will more often than not be negative. It is by far preferable that the number of questions is limited.

In a light assessment, it is not intended that deeper questions be asked, but rather to seek an overall assessment of the state of security and its principal weaknesses.

Very often, only the basic functions will be analyzed, without seeking to verify the robustness or permanency of the solutions that are implemented.

The light assessment uses a specific questionnaire that seeks to identify which security domains are presently covered and which are not.

With this in mind, the weighting of questions is simple and there is no reason to introduce the finer weighting system as used by a MEHARI vulnerability review.

The questions will only be scored by a simple weighting system.

### **6.2.2.2 Security reference policies and scoring for a detailed audit**

As opposed to the light assessment, a detailed audit seeks to verify all aspects of security services (effectiveness, robustness and permanency). It is therefore globally the same approach as that required for a risk analysis. The same questionnaires and weighting system as for risk analysis can be used.

However, as the audit does not have the same position in the two overall approaches, a few points of clarification are required.

In a risk analysis, after the vulnerability review, there exists an analysis stage where the reality of the review can be questioned, whether by technicians or users. The review can be counterbalanced by the risk analysis.

*The audit, in a risk analysis approach, can be based on responses to questions, without need to check the truth of the answers given.*

With a management approach based on audit only, this is not the same. No stage allows the outcome to be contested. The responses have therefore to be checked, to ensure a viable result. This was not important in the case of the light assessment, but is key for a security plan based on audit.

*It is therefore important to complete a vulnerability review by an audit of real practices of security professionals and users.*

### **6.2.3 The acceptability threshold of security service quality**

Just as there is a decision to be made concerning unacceptable risks during the risk analysis, there is, in this management approach, a decision to be made concerning the threshold below which the security service quality is considered unacceptable.

Deciding on the level of this threshold will depend, again, on the maturity of the organization.

During a light assessment, there is no point in being overly ambitious. It only aims to correct those weaknesses that are the most obvious. The service quality threshold can therefore be relatively low (between 2 and 2.5).

For a detailed audit, and for managing security based on audit, it would seem better and more appropriate to choose a higher threshold (3, for example).

### **6.2.4 Creating action plans**

The creation of action plans is particularly simple with this approach, as it is a direct result of the review itself.

Simply analyzing why a service did not have a satisfactory score, in other words those questions with a negative response will provide a choice of actions.

As already explained for security plans by entity based on risk analysis, it is often best to group the different measures decided upon into consistent projects (logical security, backup plans, and so on), or even into specific sub-projects. Then, respective priorities can be allocated to these projects, potentially including the constraints of implementation.

### **6.2.5 Taking the stakes into account**

It is clear with this approach that the basic process does not explicitly foresee the inclusion of the security stakes when decisions are made, but only the vulnerability values.

In practice, the stakes are often informally included during the creation of action plans by the security experts who participate in the step. The pertinence of the action plans will then depend on their appreciation of the stakes, or the way that they have been able to evaluate them.

Clearly, the inclusion of a step for value scale creation and classification can seriously improve the pertinence of audit-based security action plans.

The corresponding approach is summarized in the figure below:

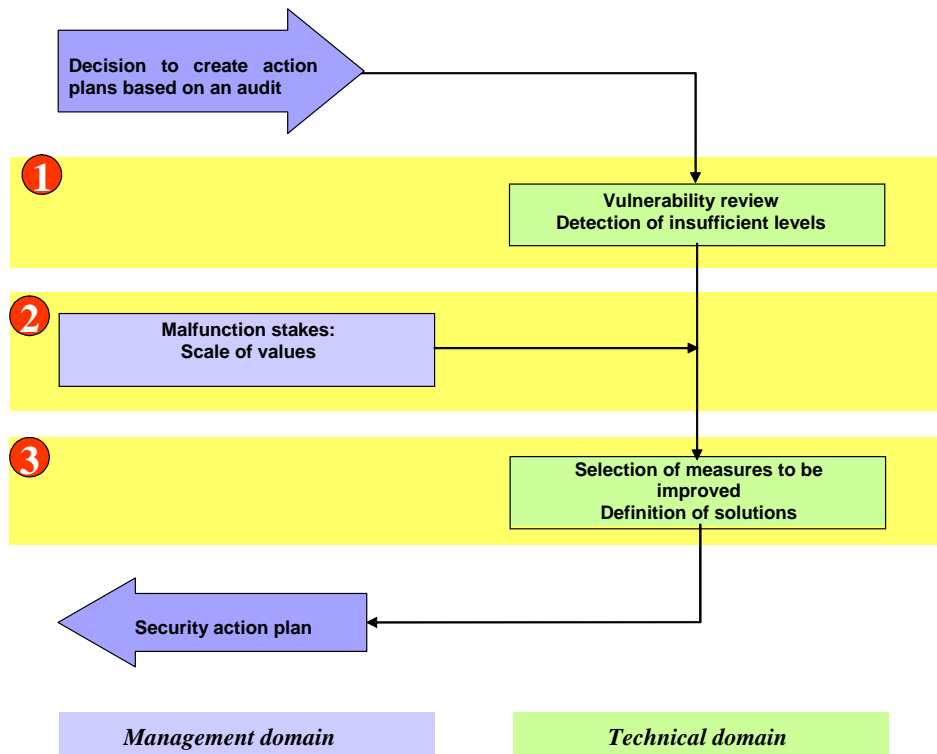


Figure 9: Security management by audit and stakes

### 6.3 Security of development projects

Until now, this document has discussed different management methods that can be used to create general action plans.

Here, the question of security management in a specific project, and not a global (or operational) security plan, will be discussed.

The general approach used for a risk analysis based plan will be reused, but with obvious need for adaptation.

### 6.3.1 The project based security management approach

An overview of the approach is shown in the figure below:

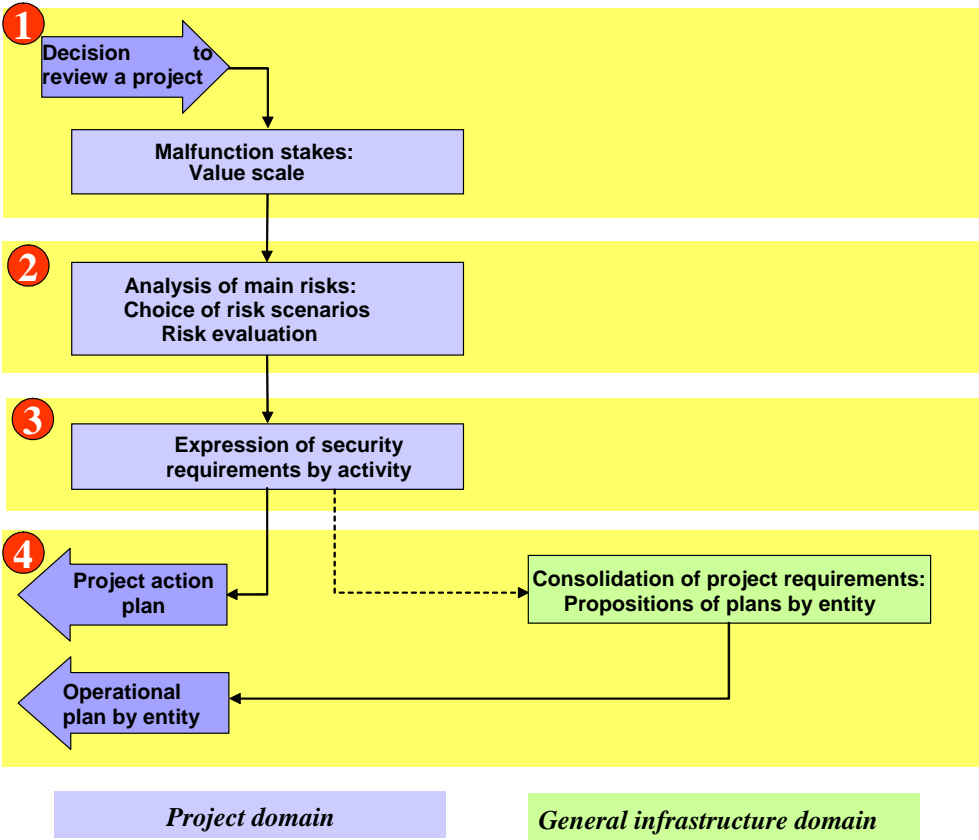


Figure 10: Project security management

### 6.3.2 Strategic and operational levels

No distinction will be made between these two levels.

It is obviously desirable that strategic elements be defined independently of any project. This can only facilitate the tasks of the project leaders, but this step is not a part of project security management.

Additionally, these elements no longer have the same level of need. It is altogether possible to use a risk analysis method in a project without the strategic elements being previously defined. This would be to the detriment of consistency between projects, but it could be considered secondary compared to the challenge of ensuring that the project leaders undertake a risk analysis for their projects and decide, as a result, action plans that they will integrate into their project plans.

### 6.3.3 Standard level of security services

The security service level that will be taken into account during the risk analysis does not result from a formal security audit. This is for the simple reason that the project is not yet in place and evidently, at the initial assessment, many points would not yet be decided.

Very often, standard security service levels, as defined by security reference policies, will be included in the project's risk analysis.

In the absence of globally defined standards, the analysis would consider quality service levels to be very low, with the supposition that nothing needs to be decided at the beginning. This way, the approach will lead to the creation of a description of the work that will have to be done to respond to the action plans resulting from the risk analysis.

#### **6.3.4 Stakes analysis and the malfunction value scale**

A general stakes evaluation process will be used and a malfunction value scale specific to the project will be created. However, it is not necessarily mandatory to deduce a classification.

#### **6.3.5 Analysis of major risks**

A risk analysis approach will be applied to a set of risk scenarios that are directly defined by the project leaders, as a result of the malfunction value scale.

A direct approach will be used, without using the automated procedures, and will concentrate on the major risks.

#### **6.3.6 Creation of action plans**

Security requirements will finally be deduced from the previous risk analysis. They will then be:

- Directly integrated into the project specifications, for the specific part that can be decided at this level,
- Distributed to the general infrastructure managers, so that they integrate them into their plans and into the plans of the concerned entities (or presented for arbitration).

#### **6.3.7 Global execution of the approach**

Globally, the approach is much more simple than one corresponding to the creation of security plans for an entity or activity.

# 7 REVIEW OF THE MAIN IMPROVEMENTS COMPARED TO PREVIOUS VERSIONS OF MEHARI

---

MEHARI 2007 brings improvements compared to previous versions in two principal areas:

- The creation of the intrinsic impact table,
- The provision, following a MEHARI audit, of a report on the status of security in a format using the ISO/IEC 17799:2005 control points.

A number of detailed improvements are also included in this new version of the knowledge base.

## 7.1 Creating the intrinsic impact table

To assist users in the creation of such a table, MEHARI 2007 includes a thoroughly detailed process

This process includes:

- The description of the tables to be completed during the analysis of the security stakes and the classification of assets,
- Indications and guidelines to assist in moving from these tables to the intrinsic impact table.

## 7.2 ISO 17799 compliance measures following a MEHARI audit

MEHARI and ISO 17799:2005 have different goals (see the “*MEHARI Overview*” document). However, there is a requirement to obtain ISO 17799 security compliance measures (with control points for the entity) as a result of a MEHARI vulnerability study.

MEHARI provides this measurement through exhaustive questionnaires that allow to map the control points required by the Standard.

Correspondence tables<sup>3</sup>, provided in the knowledge base, have been refined to take into account the requirements of ISO 17799:2005, repeated by ISO 27001. Certain questions have specifically been introduced into MEHARI audit questionnaires to this effect.

## 7.3 Recall of MEHARI previous improvements

### 7.3.1 Assessment of natural exposure

With MEHARI, natural exposure can be seen as an "intrinsic potentiality", or the potentiality that would be attained without any dissuasive or preventive measure. It is certainly a good way to consider exposure. It changes nothing apparently, but it is an easier dimension to understand and estimate.

With this in mind, it is clear that, even without any structural measures, not all scenarios have the same potentiality:

- The intrinsic potentiality of a terrorist attack can be considered as low for most organizations.
- That of a data entry error, however, is no doubt quite high.

### Definition of natural exposure

---

<sup>3</sup> RISICARE automatically produces audit reports.

Natural exposure is a measurement of intrinsic potentiality without any dissuasive or preventive measure.

In such conditions, as is explained in the "*MEHARI Risk Analysis Guide*", evaluation of natural exposure can be done by evaluating directly, with a questionnaire, the intrinsic potentiality of a certain number of characteristic events. This enables the direct calculation of STATUS-EXPO values for the scenarios.

**NOTE:** It is important to remember that natural exposure should be (re)evaluated at the time of each audit (e.g.: taking into account the age and growth in number of systems, changes to exposure – more frequent floods etc) .

### **Evaluation of natural exposure:**

The principles of the method allow to evaluate natural exposure as the intrinsic potentiality of a certain number of characteristic events.

A supporting table for this evaluation is provided in Appendix 1 of "*MEHARI risk analysis guide*".

This table is completed, by default, with mean values that are valid for most organizations. This way, unless the table is reevaluated, the values used for natural exposure will be more or less in conformity with the standard situation of most organizations. .

## **7.3.2 Introduction of the idea of intrinsic impact for risk scenarios and corresponding calculations**

### **7.3.2.1 The notion of intrinsic impact**

The MEHARI risk model has always implicitly made reference to maximal impact, because an impact reduction indicator (STATUS-RI) is evaluated. However, the assessment of intrinsic impact had not been included in the risk analysis.

#### **Intrinsic impact in MEHARI**

Intrinsic impact of a risk scenario is a maximal evaluation of the consequences of a risk, without any security measures..

Evaluation of intrinsic impact can be deduced from a malfunction value scale (which could lead to classification), or obtained directly. This is a formal step in risk analysis

### **7.3.2.2 Reference to intrinsic impact in the knowledge bases**

When the knowledge bases are used for a systematic search for risk situations, MEHARI requires the completion of an intrinsic impact table. This table includes the different types of assets that can be impacted by risk scenarios, and the different types of impact on these assets, in other words, by default, availability, integrity and confidentiality.

As the scenarios refer to the assets impacted, and the type of impact, the evaluation of intrinsic impact is automatic.

Note that it is possible to include other criteria than availability, integrity and confidentiality by completing the intrinsic impact table and generating the corresponding evaluation tables by creating ad hoc scenarios.

### **7.3.2.3 Customizing the intrinsic impact table for certain types of assets**

As already explained, some users want to differentiate between scenarios as a function of the specific type of asset that is impacted (for example: data of a specific department or of a specific

functional domain).

The fact that the scenarios explicitly reference asset types allows this differentiation. All that is required is to create asset variations in the intrinsic impact table (whether for data, servers, networks, or other assets), and to complete the table for each relevant criterion.

With MEHARI, this is called cartographic decomposition.

The reader should however be aware that asset variations thus created would be used to generate scenario variations. This can lead to a very large number of scenarios, and this possibility should be used with care.

### **7.3.3 The introduction of non-evolutive scenarios and corresponding calculations**

The way that protective measures were presented in some previous versions could have been confusing:

They were defined as having the objective, without preventing system deterioration, of limiting its scope. While this is correct, in practice they were mistaken for deterioration detection measures, where such detection might provoke a reaction, which is not always the case.

In fact, if the possible reaction does not reduce the seriousness of the consequences of the scenario, there is no point in including it.

In other words, protective measures should be taken into account only if they effectively reduce the intrinsic impact of the scenario, as it has been initially evaluated.

To simplify the inclusion of this nuance, the notion of a "non-evolutive" scenario was created.

#### **Non-evolutive scenario:**

*If a scenario does not evolve and is fixed in time and space, no protective measure can limit its direct consequences.*

*Certain scenarios, which are not fixed in time and space, can be such that potential protective measures have no effect on the intrinsic impact. They should then be considered non-evolutive, and treated as such.*

In particular, cases exist for which the real effect of protective measures can only be decided in the global context of the organization:

- When data is changed (fraud cases), or programs are modified (malevolence or errors), the intrinsic impact may (or not) be reduced through early detection depending on whether there is a right of error or not.
- When information is improperly disclosed, preventing the repetition by early detection may reduce the intrinsic impact depending on the context and the subject of the information..

Evidently, these examples of the evolutive character (or not) of a scenario do not depend solely on the knowledge base. They should also repose on the choice and decisions to be made by users.

Since the previous version of MEHARI, scenario management by automated procedures enable the declaration of a scenario as non-evolutive, where it was initially considered as evolutive.

### **7.3.4 Approaches proposed by MEHARI**

#### **7.3.4.1 A broad spectrum of approaches**

MEHARI 's risk model and knowledge bases have always enabled many approaches, but the past documentation set accentuated a specific approach that led to formalizing strategic and operational plans for the organization.

On the other hand the modular and complementary nature of tools of the methodology set are now stressed. This is an essential part of MEHARI.

For those who have already applied MEHARI, and prepared formal strategic or operational plans, there is no revolution – only evolution.

For those who found MEHARI too formal in strategic planning, they will find guides that allow to avoid certain constraints, that smaller structures do not need to face.

Those who want to use MEHARI only for projects will also find appropriate advice.

#### **7.3.4.2 Unicity of the Risk analysis approach**

In MEHARI, the risk analysis approach is unique and the notions of global approach and analytic approach are linked.

There is a fundamental approach that includes evaluation (of intrinsic impact, natural exposure and risk reduction factors), the reasoning and a final judgment on the potentiality and impact of the risk and, finally, the acceptability of the risk.

Automated procedures provide assistance in the basic process and are an essential aid in systematic search for risk situations, but can never be considered a replacement for human judgment.

#### **7.3.4.3 Complementary nature of MEHARI tools and design principles**

The complementary nature of the tools associated with the method imposes strict design principles, which need to be explained.

For this reason, even in previous versions of MEHARI, the design principles were laid down.

There are two foundation principles and a number of complementary ones. The foundation principles are:

- The automated procedures of the method must never lead to underestimation of a risk. It is always preferable for a risk to be initially over-estimated, with the possibility of its being reduced by a later detailed analysis, than for it to be underestimated and not selected for further examination.
- In any case, the automated procedures of the method must enable explanation and justification for the results obtained.

#### **7.3.5 Knowledge bases**

##### **7.3.5.1 Domain of application**

With MEHARI, the domain of application of the knowledge bases covers the information system in the broadest sense.

As a specific result, the dimensions of the user working environment are taken into account (documents, mail, office space, etc.).

##### **7.3.5.2 Security services knowledge base**

The building principles for the knowledge bases and questionnaires have already been described. Their application has led to a revision of the security services knowledge base. In addition, a descriptive sheet has been created (the “*security services reference manual*”).

##### **7.3.5.3 The scenario knowledge base**

The principles that were applied in defining this base have been clearly described.

#### **7.3.5.4 Risk reduction factor evaluation tables**

While the evaluation tables can be modified by users, it is preferable that their creation is founded on some clear principles. The principles used to create the tables are documented.