Journal of Applied Business Information Systems

http://www.jabis.ro

Risk analysis and risk management using MEHARI

Vladimir Lucian MIHAILESCU*

* Master Student at Master in Business Information Systems, West University of Timisoara, Faculty of Economics and Business Administration, Timisoara, Romania

Abstract: *In the new information society, risks are all over, every day, each minute. The present study presents MEHARI- methodology set for risk analysis and risk management developed by CLUSIF (Club de la Securite de l'Information Francais. For many years, numerous security publications have been considering risk analysis to be the foundation of security actions and referring to it as such. This is still true for the most recent standards in the domain of information security management, in particular ISO/IEC 27001, which explicitly refers to risks identifying, evaluating and treating processes. These standards that explicitly call on the idea of "risk" and the need to evaluate and control risks do not propose any methodology for analyzing risks, stating simply that organizations must choose their own methodology. It seems that even the expression "risk management" can be interpreted differently from one organization to another, and that the supporting methodologies can be significantly different depending on the objectives targeted. MEHARI -methodology set– presents ways to secure your every byte and reduce organization risks to minim.*

Keywords: *Risk analysis, risk management, MEHARI 2010, information system audit.*

1. INTRODUCTION

MEHARI is above all a method for risk assessment and management [5].

In practice, this means that MEHARI and its associated knowledge bases have been designed for a precise analysis of risk situations described through scenarios.

In day-to-day terms, security management is a function or activity that evolves over time. Corrective actions are different depending on whether the organization has not done anything in the domain, or - on the contrary - has made substantial investments in time and effort. In taking the first steps in security, it is no doubt advisable to take stock of the state of the existing security measures and policies of the organization, and to benchmark these against best practices, to clarify the gap to be filled.

Following this status assessment and the decision to implement organizational security, concrete actions will have to be decided. Such decisions, which will usually be grouped into plans, corporate rules, policies or a security reference framework, should be made using a structured approach. This approach can be based on risk analysis, as required by ISO/IEC 27001 as part of a ISMS (Information Security Management System). Other means exist, such as benchmarking, whether internal, professional or inter-professional.

At this stage, it is true that, without specifically mentioning risk analysis, the question of the stakes involved in security must be addressed. Quite often, however the decision has been made, the person with the final decision for allocating the appropriate budget will no doubt ask the question “is this really necessary?”. Due to the lack of a preliminary assessment of - and general agreement on - the stakes involved, many security projects are abandoned or delayed.

Often later, but sometimes right from the start of a security approach, the real risk that the organization or enterprise runs is questioned. This is often formulated in similar terms to this: “Have all the risks to which the organization could be exposed been identified, and is there some assurance that their levels are acceptable?”. This question could just as easily be asked at a corporate level, or in reference to a specific

project. A methodology that includes risk analysis is required [1].
MEHARI is founded on the principle that the tools required at each stage of security development must be consistent. By this, it should be understood that any results generated at one stage must be reusable by other tools later or elsewhere in the organization.
The various tools and modules of the MEHARI methodology set, designed to accompany a direct and individual risk analysis, can be used separately from each other at any step of security development, using different management approaches, and guarantee a consistency of the resulting decisions [6].
All these tools and modules - briefly described below – compose a consistent risk assessment method with the required supporting tools and modules for analyzing the stakes and auditing the quality of security measures, etc.
For many years, numerous security publications have been considering risk analysis to be the foundation of security actions and referring to it as such. This is still true for the most recent standards in the domain of information security management, in particular ISO/IEC 27001, which explicitly refers to risks identifying, evaluating and treating processes.

2. NECESSITY OF A METHODOLOGY TO COMPLEMENT THE STANDARDS

These standards that explicitly call on the idea of "risk" and the need to evaluate and control risks do not propose any methodology for analyzing risks, stating simply that organizations must choose their own methodology.
Even the ISO/IEC 27005 standard, which provides a general framework for risk management leaves considerable room for interpretation and may lead to numerous risk management approaches and processes.
In this context, the need for a formal risk management methodology is clear. It is also obvious that this methodology must meet certain requirements, themselves a function of the type of risk management an organization is seeking.
It seems that even the expression "risk management" can be interpreted differently from one organization to another, and that the supporting methodologies can be significantly different depending on the objectives targeted [2][3][4].

3. RISK ASSESSMENT

3.1 INTRODUCTION IN RISK ASSESSMENT

Assessing risks consists in identifying, as exhaustively as possible, all the risks which a company or organization is exposed to, estimating the seriousness of each risk and judging whether each risk is evaluated as acceptable or not [2][4].
Each step in this process must be performed with a view to ensuring an accurate evaluation of the seriousness of each risk, according to the context and especially the existing security measures.
The three steps constituting the overall process of assessing risks are [6]:
- Identifying risks,
- Estimating risks,
- Evaluating risks.

3.2 IDENTIFYING RISKS

This step aims not only to look for and recognize risk situations, which is to say situations presenting certain types of risks, but also to characterize each of these risks accurately enough to be able to estimate how serious it is.
This raises two questions:
- What characteristic elements of risks must be highlighted, and in how much detail must they be described?
- What is the best way to do this?

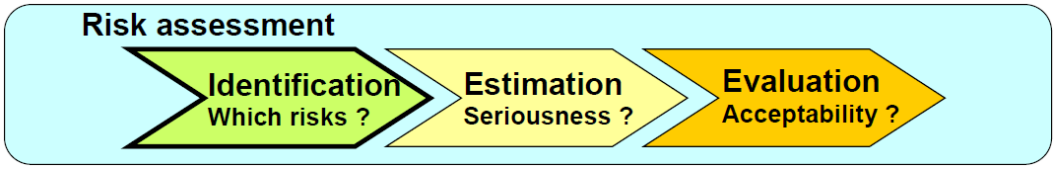

Figure 1. Risk Assessment
Source: Mehari 2010

3.2.1 THE CHARACTERISTIC ELEMENTS OF RISKS

The following paragraphs define and describe the elements that must be included in risks descriptions, and justify why. These elements are:
- The asset,
- The intrinsic vulnerability of the asset damaged by the risk,
- The asset damage,
- The threat.

3.2.1.1 THE ASSET RATIONALE

Assets are the main objects of the risk. They are what will be damaged, and a risk comes from the fact that a certain form of asset is susceptible to some particular damage. Clearly, the consequences and seriousness of occurrence of a risk depend on the nature of the assets threatened, which must therefore be included when characterizing a risk.

DESCRIBING ASSETS

a. Primary assets

Asset descriptions will be used to evaluate the consequences of the risks that the asset is exposed to. Consequently, the key features should refer to the needs of organizations, which may be divided into three main categories:
- Services (IT Services and general),
- Data necessary for the services to function,
- Management processes.

Within each category, different types of primary assets must be distinguished based on:
- The type of needs,
- The type of service providers.

And possibly:
- The field of activity and different areas of responsibility,
- The technology used,
- The users concerned.

These classifications must correspond to types of needs, and be described on a functional level.

b. Secondary or supporting assets

Assets have vulnerabilities, and it is the exploitation of these vulnerabilities that causes the risk.
To find these vulnerabilities, it is crucial to distinguish the following for each primary asset:
- The different forms that asset may take,
- The different contingencies on which that asset may depend.

These forms and contingencies may be grouped under the label of "secondary" or "supporting" assets.
Primary assets correspond to functional needs, while secondary assets correspond, on a physical and concrete level, to the means required to meet functional needs.

c. Characterizing the asset concerned by the risk

To meet the objective of direct risk management, each risk must be characterized by an asset, and each asset according to its category, its primary asset type and its secondary asset type.

3.2.1.2 INTRINSIC VULNERABILITY AND CONTEXTUAL VULNERABILITY

Risks arise from the fact that a given asset has one or more vulnerabilities.
Defining what "vulnerability" means is therefore important. Two different definitions may be used.
The first one consists in defining vulnerability as an intrinsic feature of a system, object or asset that may be susceptible to threats (e.g. the fact that the material on which a document is written is degradable).
This will be referred to as an 'intrinsic' vulnerability.
Vulnerability can also be defined in terms of security processes and their potential shortcomings. In this case, it is defined as a shortcoming or flaw in a security system that could be exploited by a threat to strike a targeted system, object or asset (e.g. lack of protection against storms).
This will be referred to as a 'contextual' vulnerability.
This second definition is not particularly suitable for identifying risks due to the major disadvantage it has of making identified and managed risks dependent on security measures, and therefore on knowledge of these measures, which is not always the case.
Intrinsic asset vulnerabilities, on the other hand, are central to describing risks and must therefore be looked for and identified.
Intrinsic vulnerabilities depend on the type of secondary asset, as they are essentially caused by the nature of the asset (e.g. hardware medium, software medium), which is defined by the secondary asset type.
It is also important to note that the intrinsic vulnerability of an asset may be described as a specific susceptibility to asset damage.

Consequently, describing the asset damage or the intrinsic vulnerability comes down to the same thing.
Only one intrinsic vulnerability is implicated for each risk.

3.2.1.3 ASSET DAMAGE

The type of consequence can be inferred from the vulnerability exploited, but there are times when it is still necessary to specify the consequence (e.g. in the event of theft, the anticipated consequence may be loss of availability or loss of confidentiality).
For assets belonging to the Data or Services categories, it is important to specify at least one of the consequence criteria (Availability, Integrity or Confidentiality), referring to other consequence criteria such as evidence value if necessary.
For Management Process assets, there is not always a specific list of criteria to identify, as it is directly specified by the asset damage.
In all cases, though, the asset damage must be indicated.

3.2.1.4 THE THREAT LEADING TO RISK OCCURRENCE

There can be no risk without a cause that leads to the intrinsic vulnerability actually being exploited. Security standards and references, including ISO/IEC 27005, use the idea of a "threat" to describe this cause.
It remains necessary, however, to include more than just the simple cause when describing the threat.
Anything that can be used to describe how the damage may occur and, most importantly, anything that may influence the likelihood of the risk occurring should also be indicated.
Consequently, the following must be described:
- The event originating the risk occurring (this event is often already described by the type of vulnerability),
- Whether this event is voluntary or accidental,
- The actor,
- The circumstances in which this event occurs.

Each of these parameters clearly has an influence on the probability of the risk occurring.

Description
The first two categories are often combined in the same description, as is the case in this document.

a. Events
Events can be described by categories and then by type within each category.
At least three categories should be considered:
- Accidents,
- Errors,
- Voluntary acts, whether malicious or not.

Within each category, types of events must be defined and described based on aspects such as:
- Whether the cause is internal or external to the entity,
- Whether the event is material or immaterial,
- Any other factor that may influence the probability of the event occurring.

b. Actors
In the case of threats that are originated by people, it is important to distinguish categories of people according to their rights and privileges.
According to these rights:
- Actors may be more or less capable of originating the threat, which means the probability of the risk occurring will be greater or smaller,
- The security measures that should be implemented will be different, which means, depending on which measures are actually implemented, the probability of the risk occurring will be greater or smaller.

c. Circumstances in which the risk occurs
Circumstances can include factors such as:
- Process or process steps: for example, modification of files during maintenance operations,
- Location: for example, theft of media from one location or another, inside or outside the company,
- Time: for example, actions occurring during or outside working hours.

Specific circumstances that merit extra attention should be identified to finalize the description of each risk.

3.2.1.5 RISK SCENARIOS

The different elements required to describe a risk can be used to create a risk scenario, which reiterates the various aspects listed above in a less structured format.
As such, the knowledge base of risk scenarios in the MEHARI 2010 knowledge base contains a free description of each scenario.

3.2.2 THE RISK IDENTIFICATION PROCESS

The process of identifying risks is crucial because no risk that is ignored by this process can be analyzed or addressed in an action plan.
Of course, it is possible to refer to a list of generic risks described in a database, such as MEHARI, but the principles on which such a list is based must be known before it can be relied upon.
Consequently, the process used to identify risks must be specified.
Three steps must be followed to ensure that the list of risks is as exhaustive as possible:
- Listing the characteristic elements of risks,
- Listing the risks that are theoretically possible,
- Selecting all the risks from this list that are possible within the specific context of risk management already in place.

Each of these steps is described in more detail below.

3.2.2.1 LISTING THE CHARACTERISTIC ELEMENTS OF RISKS

This involves identifying and detailing the classifications of each category of elements mentioned earlier in this document:
- Types of primary assets,
- Types of secondary assets,
- The intrinsic vulnerabilities linked with each type of secondary asset,
- Types of triggering events,
- Types of actors.

It will be easier to describe the circumstances in which risks occur in the next step on determining possible risks.

3.2.2.2 LISTING THE RISKS THAT ARE THEORETICALLY POSSIBLE

This involves looking for all the possible and plausible combinations of elements and completing them, if need be, with circumstances in which the risk may occur.
It is best to create this list starting with the assets.
More often than not, referring to the primary or secondary assets makes it possible to highlight the specific risk circumstances, such as process steps, times of the year or periods in time, or even specific geographical situations.
The overall process is illustrated below.

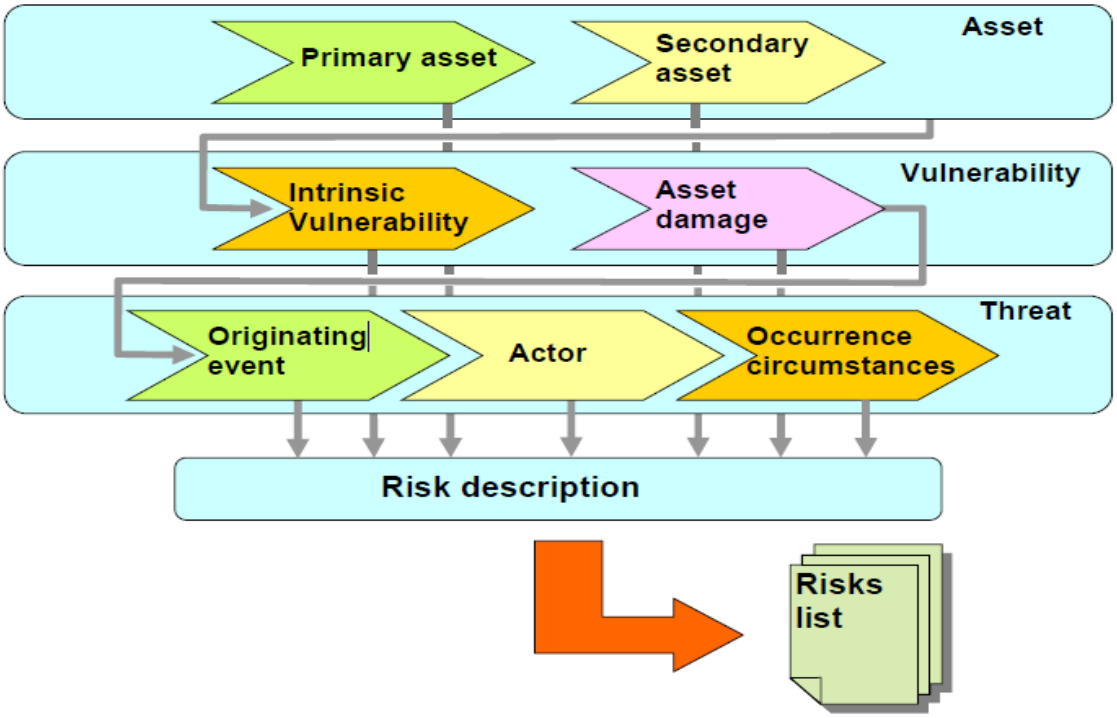

Figure 2. Risk process
Source: Mehari 2010

3.2.2.3 DEVELOPMENT OF A KNOWLEDGE BASE OF TYPICAL RISKS

The majority if not entirety of the process described above is very general and may produce the same result for many entities. As such, it makes sense to carry out this process in a generic way to develop a knowledge base of typical risks that can be used by numerous entities either as is or with a few adjustments.
Such a knowledge base provides the advantages of sharing development tools and enriching the knowledge base with input from a community of users.
MEHARI includes a knowledge base of typical risks, the "risk scenarios" knowledge base.

3.2.2.4 SELECTING RISKS TO TAKE INTO ACCOUNT

The last step in identifying risks involves striking from the list above all risks deemed impossible in the specific context of the organization concerned or that are irrelevant to the risk management concerned.
This is especially applicable in the case of typical risk knowledge bases such as the one provided by MEHARI.

3.2.3 SUMMARY OF RISK IDENTIFICATION

Identifying risks is a process that includes multiple steps, each having well-defined deliverables and contributing to the development of a list of risk scenarios to evaluate, as illustrated in the diagram below.

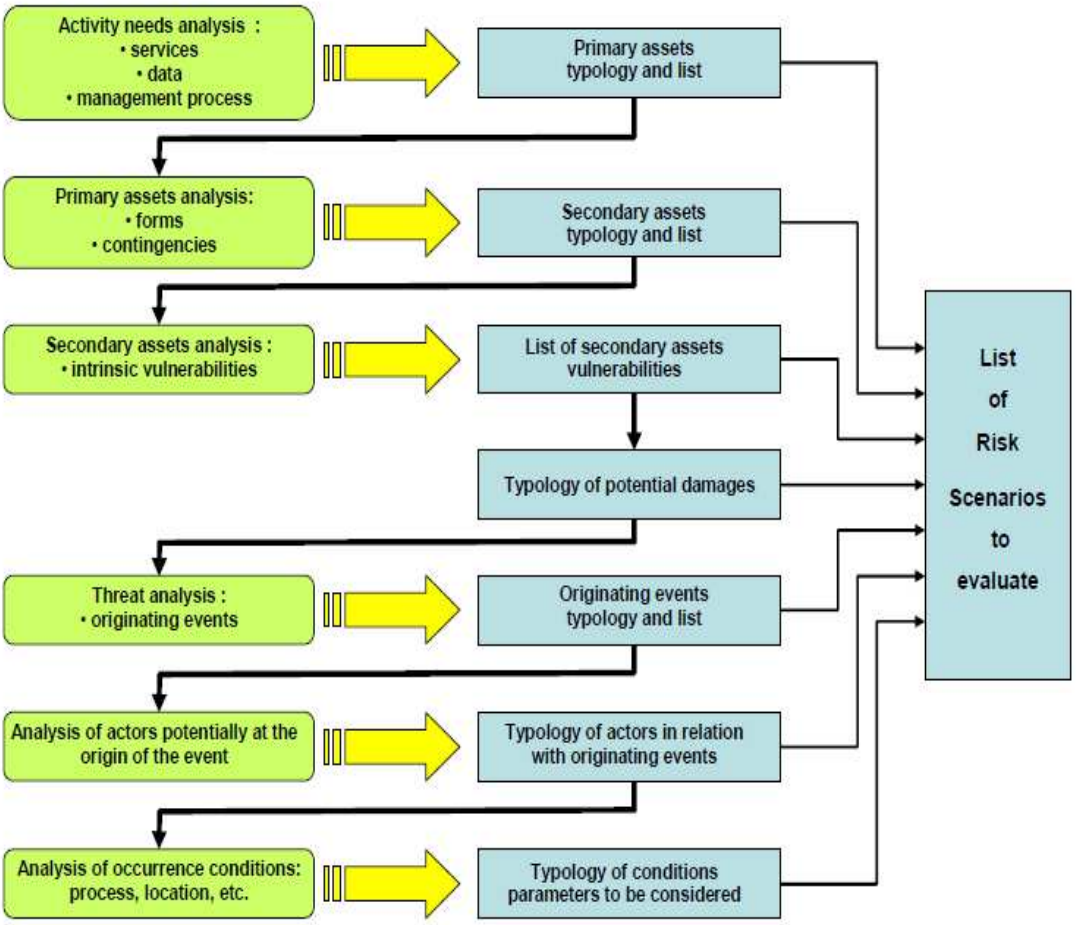

Figure 3. Risk identification
Source: Mehari 2010

3.3 ESTIMATING RISKS

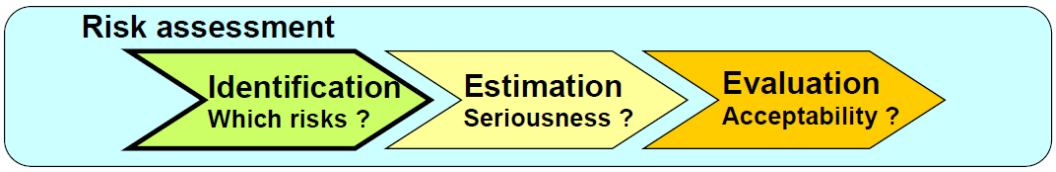

Figure 4. Estimating risks
Source: Mehari 2010

This step aims at estimating the seriousness of each risk previously identified, while taking into account the different security measures implemented.
That said, the list of risk scenarios may be long, in which case it may be desirable to go through and select a limited number of risks, namely those deemed to be "major", so as to reduce the number of risks to manage.
It may also be a good idea to select the risks that may be kept under control and "managed" without taking into account the security measures to avoid, in particular, losing control of a risk situation currently reduced to an acceptable level but that may, as the context or technology changes, become critical again.
Consequently, it is necessary to define and be able to estimate:
- The "intrinsic" seriousness of the risk, that is without taking into account the security measures,
- The "residual" seriousness of the risk, taking into account the security measures in place.
This raises two questions:
- What are the measurable elements of the risks, and what overall measurement system is required to estimate the intrinsic and residual seriousness of the risks?
- What is the best way to do this?

3.3.1 MEASURABLE ELEMENTS AND RISK METRICS

Traditionally, risk is measured based on two parameters:
- The degree of seriousness of the consequences, or "impact",
- The probability of the occurrence, or "likelihood".
Global and direct assessment of these two parameters is usually difficult; as such, it is preferable to use a more analytical approach that breaks these parameters down into multiple levels and individually evaluates:
- The intrinsic impact, excluding all security measures,
- The intrinsic likelihood, excluding all security measures,
- The effect of security measures on these two parameters.
The principles underlying these evaluations are described below.

3.3.1.1 INTRINSIC IMPACT

The intrinsic impact of a risk is defined by the maximum level of consequence the organization may incur, in the absence of any security measure designed specifically to reduce these consequences.

Complementary considerations to take into account

Two other points should also be considered:
- Once an incident has occurred, the organization will have "natural" defence reactions that, even without "organized" and planned measures, will make it possible to minimize the consequences of the incident,
- There may also be measures that limit the consequences and cannot be called into question because they are external or tied to a permanent context.
In these specific cases, and only in these cases, these security measures may be taken into account
when evaluating the intrinsic impact of a risk.

3.3.1.2 INTRINSIC LIKELIHOOD

The intrinsic likelihood is defined as the maximum probability that the risk will occur, in the absence of any security measure designed specifically to reduce this probability.
It is possible to evaluate the level of likelihood directly while taking into account security measures. However, as with the intrinsic impact, evaluating the intrinsic likelihood is preferable for the simple reason that it is easier to do, as

well as for the two other complementary reasons already mentioned:
- Measures taken or envisaged to reduce the probability of the risk occurring may end up not lasting or being inoperable, and the intrinsic likelihood makes it possible to evaluate the probability in such a case,
- Managers sometimes tend to underestimate risks by overestimating the effect of existing security measures; they will be better able to judge the risk situation and its probability if they first examine the position under the assumption that there are no security measures.

More precisely, if the intrinsic likelihood of a risk scenario is significant, the question of the quality and effectiveness of the means used to reduce the likelihood that it will occur will inevitably be raised, whereas if the residual likelihood was evaluated directly only the existence of relevant means would be evoked.

The actors and conditions in which the risk occur will be important when taking into account the security measures (the effectiveness of these measures depends on those factors), but measures already implemented should not be considered for the intrinsic likelihood because, by definition, no security measure is to be considered at this stage.

Description

The activities of each organization, as well as factors such as economic, social and geographic context, all influence the extent to which each organization is exposed to different types of risk, independently of any measures implemented:
- A market-leading high-tech company is more exposed to hacking and industrial espionage than others,
- A company located 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, and therefore to the event triggering that risk, must therefore be examined.

The intrinsic likelihood of an event can depend on a number of factors:
- Where the organization is located and its environment, for natural risks, - The potential stakes, for the perpetrator, of a voluntary act such as theft, embezzlement and intellectual satisfaction,
- The probability that a voluntary act will specifically target the organization (inversely proportional to the number of potential targets: idea of targeting).

3.3.1.3 THE EFFECT OF SECURITY MEASURES: RISK REDUCTION FACTORS

The security measures implemented may act as risk reduction factors. To manage risks, it is necessary to understand how, in what way and to what degree these measures reduce the risk level. Certain measures influence the likelihood, while others affect the consequence level (or impact); in both cases, they work in several ways that must be identified.

Likelihood reduction factors

Suitable measures can reduce risk likelihood through diverse mechanisms that may act independently or cumulatively and do not all apply to the same actors.

It is possible to identify different kinds of measures, for example those that:
- completely prevent an event from occurring;
- may or may not prevent an event from occurring, depending on the severity of the event;
- make it more difficult to carry out a malicious act (thereby making that act feasible by fewer people);
- forbid human actions;
- forbid and check;
- forbid, check and severely punish violation of a rule.

The above measures can be divided into two types:
- Dissuasive measures, which target human actions and aim at making it less likely that an actor will actually perform the action
- Preventive measures, which aim at making it less likely that any action, whether by a human or not, leads to the occurrence of the risk.

Dissuasive measures

Dissuasion is based on three principles:
- The fact that an action can be attributed to the perpetrator (the actor), which brings into play measurable technical and organizational mechanisms (e.g. existence of traces, user authentication, strength of evidence),
- The existence of penalties, the severity of which may also be measured,

- Awareness on the part of the actor that their actions may be attributed to them and of the penalties incurred in such a case.

The effectiveness of dissuasive measures may therefore be evaluated and quantified by referring to a scale that each organization should define or at least validate, as discussed later in this document.

Preventive measures

Prevention depends, of course, on the events that the organization is trying to avert. Most often, prevention involves technical measures and monitoring mechanisms whose effectiveness and robustness may be evaluated.

The effectiveness of preventive measures may therefore be evaluated and quantified by referring to a scale that each organization should define or at least validate, as discussed later in this document.

Impact reduction factors

Suitable measures can reduce risk impact (the level of its consequences) through diverse mechanisms that may act independently or cumulatively and do not all apply to the same types of consequences.

It is possible to identify different kinds of measures, for example those that:

- Limit, in absolute terms, the maximum direct impact possible,
- Prevent the propagation of an initial incident,
- Anticipate reparation of equipment following a material incident,
- Anticipate restoration of the original state following an immaterial incident,
- Anticipate backup facilities.

The above measures can be divided into two types:

- Confinement measures, which aim to limit the magnitude of direct consequences,
- Palliative measures, which aim to minimize the indirect consequences of a risk by anticipating crisis management.

Confinement measures

Confinement is based on several types of mechanisms that all impose limits on the consequences of a risk:

- Setting limits on events that can be propagated, such as physical limits on certain types of incidents (e.g. firewalls),
- Determining intermediary checkpoints in processes to prevent the propagation of errors or faults,
- Monitoring process execution to limit the consequences of a mishap that may lead to more severe consequences,
- Setting limits on parameter variations allowed (e.g. limits on amounts transferred or on differences between two states, with control procedures being triggered when these limits are exceeded).

The effectiveness of confinement measures may be evaluated and quantified by referring to a scale that each organization should define or at least validate, as discussed later in this document.

Palliative measures

These measures, sometimes called *palliation*, do not in any way change the direct consequences, which is to say the incident itself, but may minimize the indirect consequences of the incident.

These measures are based on different types of mechanisms:

- Hardware or software maintenance plans,
- Data restoration and backup plans,
- Activity continuity and recovery plans,
- Crisis management and communication plans.

The effectiveness of palliative measures may be evaluated and quantified by referring to a scale that each organization should define or at least validate, as discussed later in this document.

3.3.1.4 INFLUENCE OF THE QUALITY OF EXISTING SECURITY MEASURES

It is clear that these risk reduction factors do not solely depend on the type of existing security measures, but also on their quality. Certain implementations may include mechanisms that are more effective than others, and this must be taken into account.

3.3.1.5 USING A RISK KNOWLEDGE BASE

If risks are identified using a knowledge base of typical risks, as described in section 3.2.2.3, this knowledge base may be completed to include, besides the simple description of the characteristic elements of each risk, information on the relevant security measures for each type of risk, the criteria used to evaluate the quality of these measures and the relationship between the quality of these measures and the effectiveness of risk reduction factors.

MEHARI and its knowledge base include all these elements and, in particular:

- A specification of the "security services" including criteria for evaluating quality and a measurement system for evaluating the measures
- A security services reference manual,
- An expert knowledge base of questionnaires for diagnosing the quality of security services,
- The reference, for each risk reduction factor for each risk in the knowledge base, of relevant security services and formulas for evaluating the combined effects of these services.

3.3.2 THE RISK ESTIMATION PROCESS

The process for estimating risks involves two phases:
- A phase that could be considered "strategic" in that it involves setting up evaluation references and knowledge bases,
- A more operational phase that involves actually estimating the risks using the knowledge bases and references put into place in the first phase.

3.3.2.1 DEVELOPING REFERENCE MATERIAL

This involves defining the levels that will be used to evaluate the various parameters of each risk, as previously mentioned, and defining in particular:
- The impact scale,
- The likelihood scale,
- Effectiveness scales for the different risk reduction factors.

The impact scale
The impact scale is designed to organize the consequence levels into a hierarchy.
Rationale
As impact is a key factor in estimating risks, it is essential that this scale be defined as clearly and unambiguously as possible.
Description
The level cannot be "measured", per se, only estimated; consequently, it would be misleading to include too many impact levels. Defining four levels is a reasonable compromise.
The likelihood scale
The likelihood scale is designed to organize the probability levels into a hierarchy.
Rationale
As risk likelihood is a key factor in estimating risks, it is essential that this scale be defined as clearly and unambiguously as possible.
Description
Likelihood cannot be "measured", per se, only estimated; consequently, it would be misleading to include too many likelihood levels. Defining four levels is reasonable in this case as well.
Defining effectiveness scales for the different risk reduction factors
Each risk reduction factor may be evaluated according to an effectiveness scale that must be defined in advance.
As for the impact and likelihood scales, defining four levels is a good compromise between excessive and insufficient precision. The most important point is that each level be defined such that it is easy to choose between one level and another.

3.3.2.2 ESTIMATING RISKS

Estimating risks, which relies on references defined in advanced as described above, includes evaluating the following for each risk:
- Intrinsic impact and intrinsic likelihood,
- Risk reduction factors,
- Impact and likelihood, taking into account the existence and value of these reduction factors.

Evaluating intrinsic impact and intrinsic likelihood
These characteristics should both be evaluated based on the definitions of the different levels, disregarding all security measures, as specified above.
For MEHARI, the corresponding processes are described in detail in the stakes analysis guide and the risk analysis and treatment guide.

Evaluating risk reduction factors
Each risk reduction factor should be evaluated using the following process:
- Look for security measures (or services) relevant to each risk scenario,
- Determine the effects (dissuasive, preventive, confinement, palliative) resulting from each security measure or service,
- Determine the level for each effect and each measure using the scales previously defined,
- For each effect, determine the maximum level for all measures selected as relevant to this risk,
- These maximum levels are what determine the level of each risk reduction factor (for the risk analyzed).

For this process, it is highly recommended, if not necessary, to use a risk knowledge base such as the one mentioned in section 3.3.1.5. Arguments

supporting the use of such a knowledge base include:

- Identifying relevant security measures capable of reducing the number of risk reduction factors must take into account a precautionary principle: only those measures that are guaranteed to have an effect should be taken into account. To this end, obtaining assistance from the experts that developed a knowledge base of security measures and associated audit questionnaires would be useful,
- The way in which multiple security measures may be combined, complement each other or depend on each other is a question for experts, who are not necessarily on hand during the evaluation of risk reduction factors,
- Taking into account the quality of the security measures (or the contextual vulnerability levels) requires questionnaires capable of evaluating these levels, the creation of which is not part of an evaluation process,
- The relationship between the levels of the security measures and of the risk reduction factors is also a question for the experts.

To take into account all of these aspects, MEHARI makes use of a knowledge base that includes a section on "security services", questionnaires for evaluating the quality of these services, and formulas that can be used to evaluate the risk reduction factors based on results from a contextual vulnerability audit of the security services.

As such, using the MEHARI knowledge base after assessing the quality of the security services makes it possible to evaluate the level of the risk reduction factors for each risk scenario presented in the knowledge base.

Evaluating the residual impact and likelihood of risks

Evaluating residual risk impact and residual risk likelihood is based on evaluations of the intrinsic impact, intrinsic likelihood and risk reduction factors.

Evaluating likelihood

This evaluation determines the likelihood of a risk given the risk scenario factors, and basically asks one question:

Given the intrinsic likelihood (or natural exposure to the risk), the effectiveness of dissuasive measures (for a human action) and the effectiveness of preventive measures, what is the actual likelihood of this risk?

This evaluation comes down to simply deciding, but it is recommended that the decision tables (that should have been created during the strategic phase, with the four-level scales) be used so that the corresponding assessments may be reproduced.

Such tables should be based on the type of scenario: accident, error or voluntary human action.

Evaluating impact

This evaluation determines the impact of a risk given the risk scenario factors, and basically asks one question:

Given the intrinsic impact, the effectiveness of confinement measures (for scenarios that can be confined) and the effectiveness of palliative measures, what is the actual impact of this risk?

This evaluation comes down to simply deciding, but it is recommended that the decision tables (that should have been created during the strategic phase, with the four-level scales) be used so that the corresponding assessments may be reproduced.

In this case, such tables should be based on the type of scenario: affecting availability, confidentiality or integrity. They may need to include a special case for scenarios where the impact can be limited but palliative measures are not possible.

3.3.3 SUMMARY OF RISK SCENARIO ASSESSMENT

Each risk scenario is assessed in multiple stages, each of which contributes to independently evaluating the likelihood and the impact of each risk scenario, as illustrated in the diagram below.

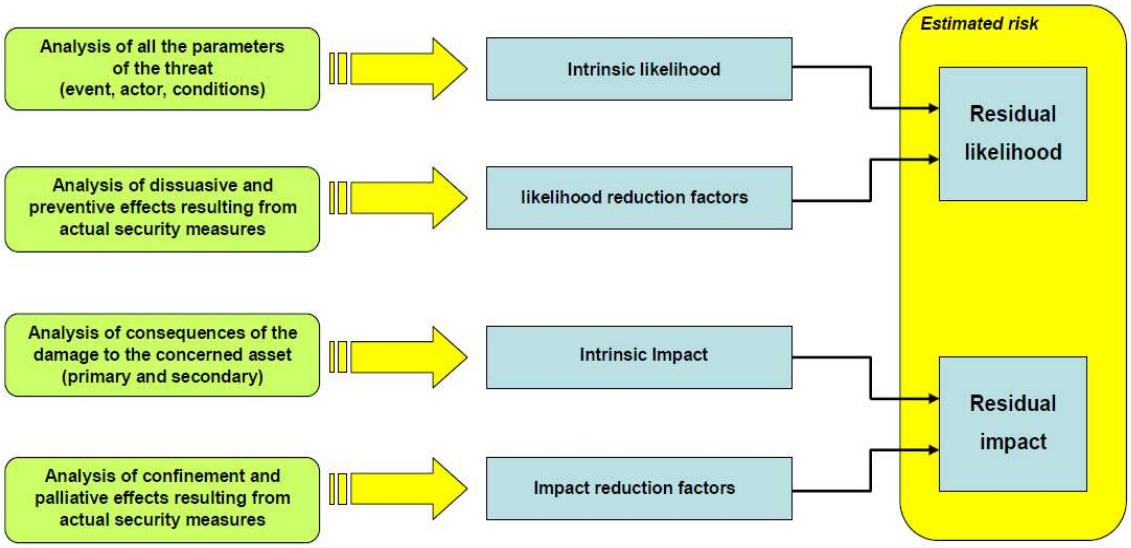

Figure 5. Risk scenario assessment
Source: Mehari 2010

3.4 EVALUATING RISKS

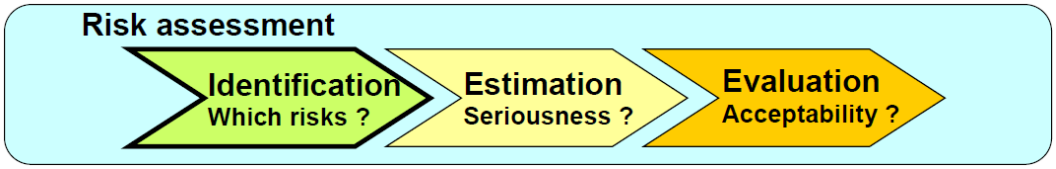

Figure 6. Risk Assessment
Source: Mehari 2010

The seriousness of each risk scenario or situation is a function of its residual likelihood and impact. That said, it is not a simple mathematical calculation based on these two values, but rather a judgment on the acceptability (or unacceptability) of the situation.
Based on the likelihood and impact of the risk analyzed, the only question that needs to be asked is:
Is this risk situation acceptable as it stands or, if not, what should be done?
The decision to accept a risk or deem it unacceptable should be made using a process that ensures reliability of the decision.
To this end, developing a decision table that will guarantee consistency across decisions made at different times or by different people is essential.
These decision tables can be represented using a "risk acceptability" table that indicates, according to the estimated impact and likelihood, whether the risk is acceptable or not.

As an example, three categories of risk can be defined:
- Intolerable risks, which require emergency measures outside of normal budget cycles,
- Inadmissible risks, which must be reduced or eliminated at some point in time. This should be integrated into a planning cycle (security plan),
- Accepted risks.

The first two categories correspond to what had previously been called unacceptable risks.
The standard risk acceptability table from MEHARI 2010 is provided below. In this example, S is the global seriousness evaluated as a function of the impact (I) and likelihood (L). Level 4 corresponds to an intolerable risk, level 3 to an inadmissible risk and the lower levels to acceptable risks.

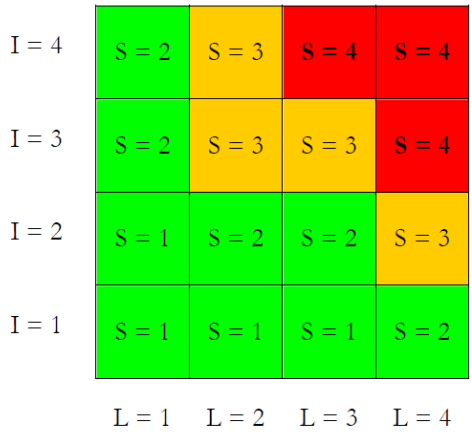

Figure 7. Risk acceptability table
Source: Mehari 2010

4. RISK TREATMENT

Different options are available for treating risks once they have been identified, listed and evaluated, which is to say once each risk has been deemed acceptable or not.
These options are not described in detail here, the goal being instead to highlight what each option may require in terms of management methodologies for information risks, in order to specify what each of these methodologies must contain to be able to directly and individually manage risks.
This section will look at the four main options available for treating risks, which are described in the ISO/IEC 27005 standard and represented in the diagram below. These options are:
- Retaining the risk,
- Reducing the risk,
- Transferring the risk,
- Avoiding the risk.

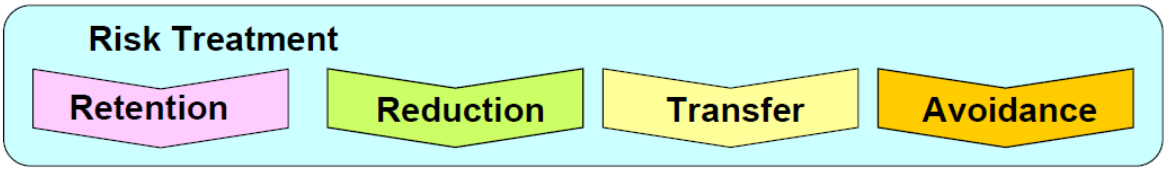

Figure 8. Risk Treatment
Source: Mehari 2010

4.1 RETAINING THE RISK

Retaining a risk means accepting the risk situation described by the risk scenario, as explained earlier in this document.
It would be more correct and more general to say that it means the company or organization accepts to not do anything to change the situation.
This option may be chosen for two reasons:
- It covers all cases where the risk was evaluated as acceptable in terms of the risk acceptability table because its combined impact/likelihood was deemed acceptable,
- It also covers the case where, though theoretically unacceptable, it was deemed impossible to attenuate the risk with a different solution or all other solutions were rejected for economic reasons.

In all cases, and especially the second, there must be a consensus to accept the risk, and acceptance must be communicated.
However, this communication does not require anything more than a detailed description of the risk situation, which is already provided by the specifications described in the preceding chapters. Consequently, there are no additional requirements for accepting a risk except, most

likely, setting up monitoring indicators to ensure that any conditions for accepting this risk remain valid over time.

4.2 REDUCING THE RISK

Reducing a risk means reducing one of the two characteristic parameters of that risk, likelihood or impact, or both simultaneously using specific actions. Such actions are determined for each risk identified as unacceptable.
These actions basically aim to improve certain risk reduction factors by implementing suitable security measures.
Directly choosing concrete solutions would be inappropriate for the risk-reduction decision making process because it would make the relevance of the solution dependent on technological evolution. At this point, then, it is important to specify a functional need with regard to both the targeted purposes and the desired level of performance. This leads to the idea of "security services", which is a fundamental concept in risk treatment.

4.2.1 CHOOSING WHICH SECURITY SERVICE TO IMPLEMENT TO INCREASE CERTAIN RISK REDUCTION FACTORS

4.2.1.1 SECURITY SERVICES RELEVANT OR ADAPTED TO A GIVEN RISK

The first step in the decision-making process used in relation to reducing risks is choosing the security services suitable for both the risk scenario in question and the risk reduction factor that is to be improved.
To do this, decision-makers have to be able to rely on a knowledge base of security services that should include at least:
- A list of the security services,
- The purpose (or objectives) of each service,
- The technical and organizational mechanisms that may be envisaged for implementing the service.

Given that this knowledge base exists, decision-makers simply have to choose the risk reduction factors and relevant services to meet this requirement.
The corresponding process is not unique, and there may be several different ways to present the main strategic options. This document is not intended to specify a specific process for choosing.

4.2.1.2 CHOOSING THE TARGET QUALITY LEVEL FOR THE SECURITY SERVICE TO BE IMPLEMENTED

There is no doubt, however, that the degree to which the risk reduction factors in question are improved is highly dependent on the performance of the security services selected, which means it is necessary to define the quality level of the security services.
The best way to do this is to define a quality scale, similar to the scales established for the different risk parameters.

4.2.1.3 EVALUATING THE COMBINED EFFECT OF MULTIPLE SECURITY SERVICE

Evaluating the combined effect of multiple security services, whether anticipated or already existent, remains an important step in choosing which services to implement for risk management.
This requires the provision of aids, which is the goal of a risk knowledge base such as the one discussed in sections 1.2.2.3, 1.3.1.5 and 1.3.2.2.

4.2.1.4 DECISION MAKING FOR REDUCING RISKS

The decision-making process for reducing risks involves:
- Selecting suitable security services,
- Selecting a target level for these services,
- Deducing new values for the risk reduction factors,
- Verifying that these new values reduce the risk to an acceptable level of seriousness.

4.2.2 USING STRUCTURAL MEASURES

Certain measures, called "structural" measures for the purposes of this document, can influence the intrinsic likelihood or the intrinsic impact of a risk. These measures "structurally" change certain aspects of the company's context or of its relationship to its surroundings. Two examples can help illustrate this idea:
A given company may be exposed to environmental risks such as floods or

earthquakes. It may reduce these risks by implementing suitable security measures, or it may simply decide to move. This would constitute a "structural" measure because it can "structurally" change the nature or level of the risk.
A bank may be exposed to the risk of a hold-up. It can limit this risk with suitable security services, but it may also use the structural measure of limiting the amount of cash available.

4.3 TRANSFERRING THE RISK

Transferring a risk means, in practical terms, looking at the risk from a financial standpoint and transferring part of the financial burden incurred, should the risk materialize, to a third party. In most cases, this means obtaining insurance, but it can also mean transferring the burden to a third party (the one responsible) through legal proceedings.
This decision, while not calling on the same evaluation mechanisms, still requires that specific security measures be implemented (especially in terms of collecting evidence).
All that precedes this section still applies, and there are no additional requirements.

4.4 AVOIDING THE RISK

Avoiding a risk is similar to reducing a risk through structural measures.
The difference lies in the fact that, rather than changing the relationship between a company or organization and its surroundings, internal processes are changed so that the risk no longer exists at all.

5. RISK MANAGEMENT

Managing risks involves all the processes that facilitate implementing the decisions previously made regarding the treatment of risks, monitoring the effect of these decisions, and improving them if necessary.
In light of the purpose of this document, the question here becomes whether these processes call for any specific requirements that must be detailed to guarantee effective management of information risks.
This section analyzes the requirements of each phase of the overall process illustrated in the diagram first presented at the beginning of this document and recalled below.

Figure 9. Risk management
Source: Mehari 2010

5.1 DEVELOPING ACTION PLANS

After analyzing the risks and making decisions on how to treat these risks, the company or organization decided to go ahead with a certain number of actions that, according to the type of treatment chosen, are based on:
- Implementing security services, each with a quality level objective,
- Structural measures designed to reduce the exposure to certain risks,
- Organizational measures designed to avoid certain risks.

That said, it should be obvious that not all of these actions will be carried out simultaneously, nor will they all be implemented immediately, for various reasons such as limited budgets or lack of available human resources.
As such, action plans should be developed according to the following steps:
- Choose priority objectives in terms of security services to implement, and optimize this choice,
- Transform the choice(s) of security services into concrete action plans,
- Choose potential structural measures and risk avoidance measures,
- Validate the preceding decisions.

5.1.1 CHOOSING PRIORITY OBJECTS AND OPTIMIZATION

If it is impossible to deploy all actions simultaneously, due to economic reasons, lack of available resources or any other reason, a choice must be made as to which measures should be implemented first.
To establish the order of priority for these actions, certain factors should be taken into account:
- The seriousness of the risks that the priority measures are designed to reduce (more serious risks should be treated first),
- The number of risks that will be treated, and the number of risks that will have to be treated at a later date,
- The speed with which the first results will be observed,
- The effects of these choices on personnel awareness,

Depending on the importance attributed to the different criteria, optimization tools may prove useful.
MEHARI 2010 proposes an optimization algorithm for prioritizing the measures.

5.1.2 CHOOSING SOLUTIONS: ORGANIZATIONAL AND TECHNICAL MECHANISMS

Choosing concrete solutions to deploy, whether they are based on organizational or technical mechanisms, is the responsibility of specialized teams such as the IT department, network managers, physical security managers and CISOs.
Nevertheless, the fact remains that transferring responsibilities between the risk management managers who selected the security services to implement at a certain quality level and the managers in charge of defining and deploying the mechanisms is highly dependent on the degree of precision with which the security services were defined.
A security services reference manual should be developed for these definitions.
The security services reference manual
A security services reference manual should describe, for each security service:
- The purpose of the service,
- The results expected from implementing the service,
- A description of the mechanisms associated with the service, including both organizational and technical aspects,
- The elements that can be used to evaluate the quality of the service according to the three assessment criteria: efficiency, robustness and permanence over time.

5.1.3 CHOOSING STRUCTURAL MEASURES AND RISK AVOIDANCE MEASURES

These choices essentially based on the specific details of situations or operating processes, do not entail any particular requirements in terms of risk management methodologies, and have no direct impact on MEHARI knowledge bases or principles.

5.1.4 APPROVAL AND DECISION-MAKING

The different choices described above must be quantified and integrated into a planning cycle before being presented to the decision-makers for approval. This step is not specific to direct management of risks, and does not entail any particular requirements in terms of the risk management methodology.

5.2 IMPLEMENTING ACTION PLANS

Implementing the action plans may pose application challenges in specific contexts.
In this case, it is important to be able to refer to the risks that each action plan was supposed to reduce in order to determine the best response.

5.3 MONITORING AND STEERING DIRECT MANAGEMENT OF RISKS

Numerous verifications must be carried out to steer the direct management of risks, as illustrated in the diagram below.
The first level of monitoring involves verifying that the security solutions and mechanisms planned and selected do indeed correspond to the service quality levels chosen during the risk treatment phase.
The second verification is related to implementation compliance.

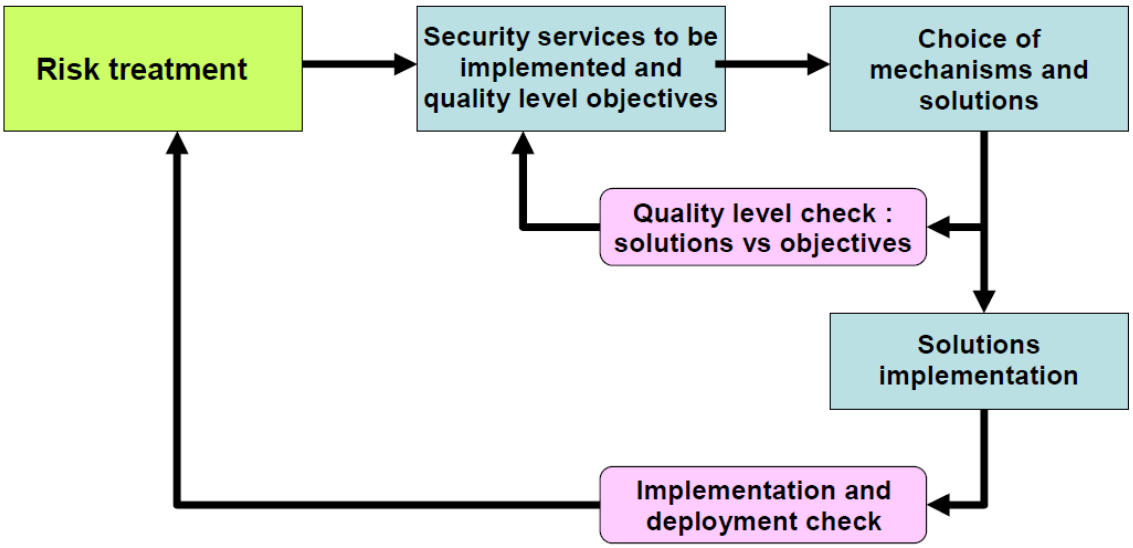

Figure 10. Risk Management Diagram
Source: Mehari 2010

5.3.1 SERVICE QUALITY VERIFICATION

More often than not, this should be self-imposed. This raises the question of knowing how technical personnel responsible for defining the mechanisms and solutions to implement will be able to do so with sufficient knowledge as to the impact their decisions will have on the service quality level ultimately obtained.
Furthermore, post-control testing will be necessary, and will have to be performed by personnel who are not necessarily senior, experienced technicians.
Consequently, it is necessary to have a knowledge base of expertise or security services audit knowledge base that will facilitate making suitable choices when defining the mechanisms and solutions to implement, as well as post-control testing.

5.3.2 VERIFYING IMPLEMENTATION OF THE SECURITY SERVICES

For obvious reasons, it is crucial to verify the actual implementation of the security services previously defined.
Often, security services are only partially deployed, or implemented in a way that does not completely comply with decisions previously made.
In terms of risk management, the response(s) to such situations must be defined.
Specification
How to respond to and report on incomplete deployment of security services, as well as how to incorporate this into the risk management system, shall be specified.

5.3.3 OVERALL STEERING FOR DIRECT MANAGEMENT OF RISKS

Overall steering of the direct management of risks is similar to all project steering, and includes:
- Indicators and a scoreboard,
- A reporting system,
- A system for periodic reviews and decision-making regarding necessary corrective actions.

REFERENCES

[1] Champlain J., *Auditing Information Systems*, Second Edition, Editura Wiley USA, 2003.

[2] Davis R., *Information Systems Auditing: The IS Audit Testing Process* , USA, 2011.

[3] Nastase P, Stanciu V, Eden A., Auditul si controlul sistemelor informationale ,Editura ECONOMICA , Bucuresti, 2007.

[4] Weber R., Information Systems Control and Audit, Editura Prentice Hall, USA, 1998.

[5] ***, MEHARI et le management de la sécurité – 2002.

[6] *** MEHARI 2010

Appendix A1
MEHARI 2010 knowledge base classification of primary Assets

Data and information assets		**A**	**I**	**C**
Data and information				
D01	Data files and data bases accessed by applications			
D02	Shared office files and data			
D03	Personal office files (on user work stations and equipments)			
D04	Written or printed information and data kept by users and personal archives			
D05	Listings or printed documents			
D06	Exchanged messages, screen views, data individually sensitive			
D07	electronic mailing			
D08	(Post) Mails and faxes			
D09	Patrimonial archives or documents used as proofs			
D10	IT related Archives			
D11	Data and information published on public or internal sites			
Service assets		**A**	**I**	**C**
General Services				
G01	User workspace and environment			
G02	Telecommunication Services (voice, fax, audio & videoconferencing, etc.)			
IT and Networking Services				
R01	Extended Network Service			
R02	Local Area Network Service			
S01	Services provided by applications			
S02	Shared Office Services (servers, document management, shared printers, etc.)			
S03	Users' disposal of Equipments (workstations, local printers, peripherals, specific interfaces, etc.) **Nota : Applies to a massive loss of these services, not for one or few users.**			
S04	Common Services, working environment: messaging, archiving, print, editing, etc.			
S05	Web editing Service (internal or public)			
Management process type of assets		**E**		
Management Processes for compliance to law or regulations				
C01	Compliance to law or regulations relative to personal information protection			
C02	Compliance to law or regulations relative to financial communication			
C03	Compliance to law or regulations relative to digital accounting control			
C04	Compliance to law or regulations relative to intellectual property			
C05	Compliance to law or regulations relative to the protection information systems			
C06	Compliance to law or regulations relative to people safety and protection of environment			

Appendix A2
Mehari 2010 knowledge base classification of supporting assets

The following table presents the list of MEHARI 2010 knowledge base supporting (or secondary) asset types by category of primary asset.

SECONDARY ASSET TYPES
Asset category: Services
Service support hardware equipment
Software configurations
Software support media
Accounts and means necessary to access the service
Security services associated with the service
Ancillary means necessary for the service
Premises
Personnel and service providers necessary for the service (internal and external)

Asset category: Data
Logical entities: files or databases
Logical entities: transiting data packets or messages
Physical entities: media and devices
Means for accessing data: keys and other means, physical or logical, required to access the data

Asset category: Management processes
Internal guidelines and procedures (organizational tools)
Physical resources necessary for management processes
Personnel and service providers necessary for management processes