METHODS

MEHARI www.mehari.info

MEHARI 2010

Risk analysis and treatment Guide

August 2010

CLUSIF

Methods Commission

Please post your questions and comments on the forum:

http://mehari.info/

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11, rue de Mogador, 75009 PARIS
Tél.: +33 1 53 25 08 80 – Fax: +33 1 53 25 08 88 – e-mail: clusif@clusif.asso.fr
Web: http://www.clusif.asso.fr

Contents

Acknowledgments

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

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

1 Introduction

This guide is for managers who want to begin a process of risk management in a business or organization, with the help of MEHARI.

MEHARI is notable for the fact that it enables direct, individual management of each risk, in contrast to management methods that are global and provide less differentiation between risks.

1.1 *Direct and individual management or global management?*

There are effectively two major types of risk management:

— The first type of management consists of identifying all risk situations, analyzing each risk situation identified, and taking specific decisions tailored to each one, with strong involvement of senior management in risk management.

— The second type of management, in contrast, is based on a more general analysis that identifies the security goals and regulations specific to a global reduction of risks, without direct and individual management of risks, and probably with less involvement from senior management.

A detailed analysis of these types of management is presented in the document "*Risk Management, Concepts and Methods*", published in 2009 and available from the CLUSIF web site.

The table below presents a comparison of the two types of management.

	Direct and individual management of risks	Global and indirect management of risks
Advantages	Identification and analysis of all risk situations Precise evaluation of the level of risk for each risk situation Precise evaluation of the effect of security measures on the risk level for each risk situation	Simple presentation of risks Easy to understand the concepts Easy to communicate the risks Easy to connect the risks to the measures to put in place
Disadvantages	Requires a complete model presenting all risks Requires that every risk situation is presented in all its complexity	Opens to ignore potentially serious risk situations Lacks assessment of the seriousness level of risks Over cost or under evaluation in the treatment of risks

MEHARI is clearly positioned as a methodical framework for direct management of risks in businesses and organizations, and the approaches introduced below are strictly within this framework.

1.2 Review of the general principles of MEHARI

Choosing the option of direct management of risks leads to the definition of a number of principles and specifications, which are described in the document *"MEHARI 2010 – Fundamental concepts and functional specifications"*.

The key elements are the following:

Risks must be identified and described by scenarios containing a certain number of specific and precise elements.

Each risk scenario can be evaluated quantitatively (that is, the risk can be measured) and this evaluation takes into account:

- ➢ The intrinsic impact of the risk scenario, which reflects the level of consequence of the scenario occurring, in the absence of any security measures,
- ➢ The intrinsic likelihood of the scenario (or natural exposure to the scenario), which reflects the probability of the scenario occurring, in the absence of any security measures,
- ➢ Risk reduction factors based on the security measures, categorized by the type of effect they have on the impact or likelihood of risk measures and the quality of these measures.

The procedure for evaluating each risk scenario enables security measures to be selected, with qualitative goals for each measure such that the risk can be held below an acceptable to level.

To present the MEHARI approach, we adopt the organization described in the ISO/IEC 27005 standard, which is shown in the diagram below.

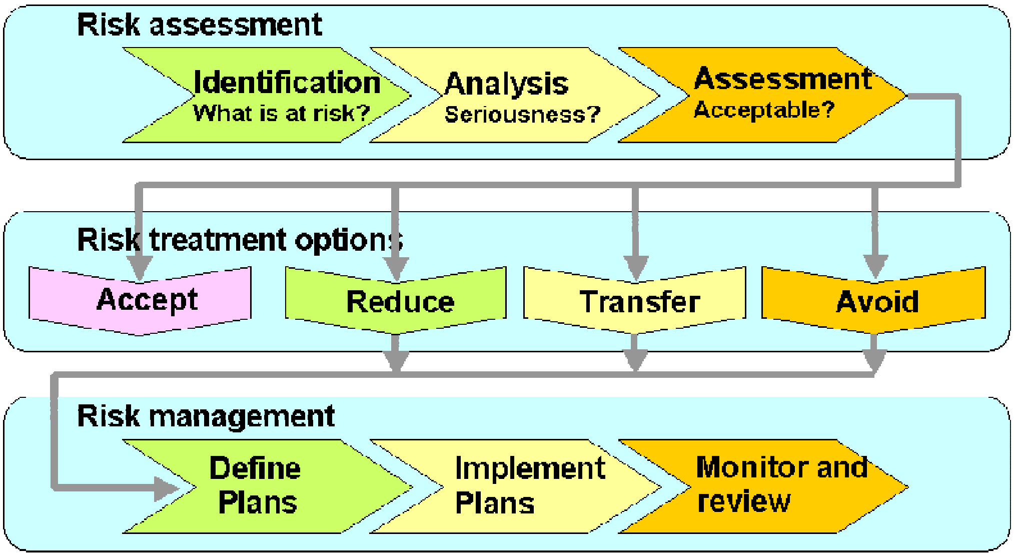

Figure 1: Phases in risk management

This diagram presents three risk management main phases. The first two phases are the evaluation of risks and options for treating them, and correspond to the Plan phase of ISO/IEC 27001 standard. The management phase integrates the deployment (Do), monitoring (Check), and improvement (Act) phases.

The main difference carried by the implementation of direct and individual management of risks is essentially in the planning phase and concerns the way for evaluating each risk and defining the relevant action plan.

1.3 Overview of risk treatment planning

Figure 2 shows the steps in the risk evaluation and action planning phases.

Each of the phases is described in the aforementioned document *"MEHARI 2010 – Fundamental concepts and functional specifications"*.

Steps and Requirements bases and actions Specific application Final result

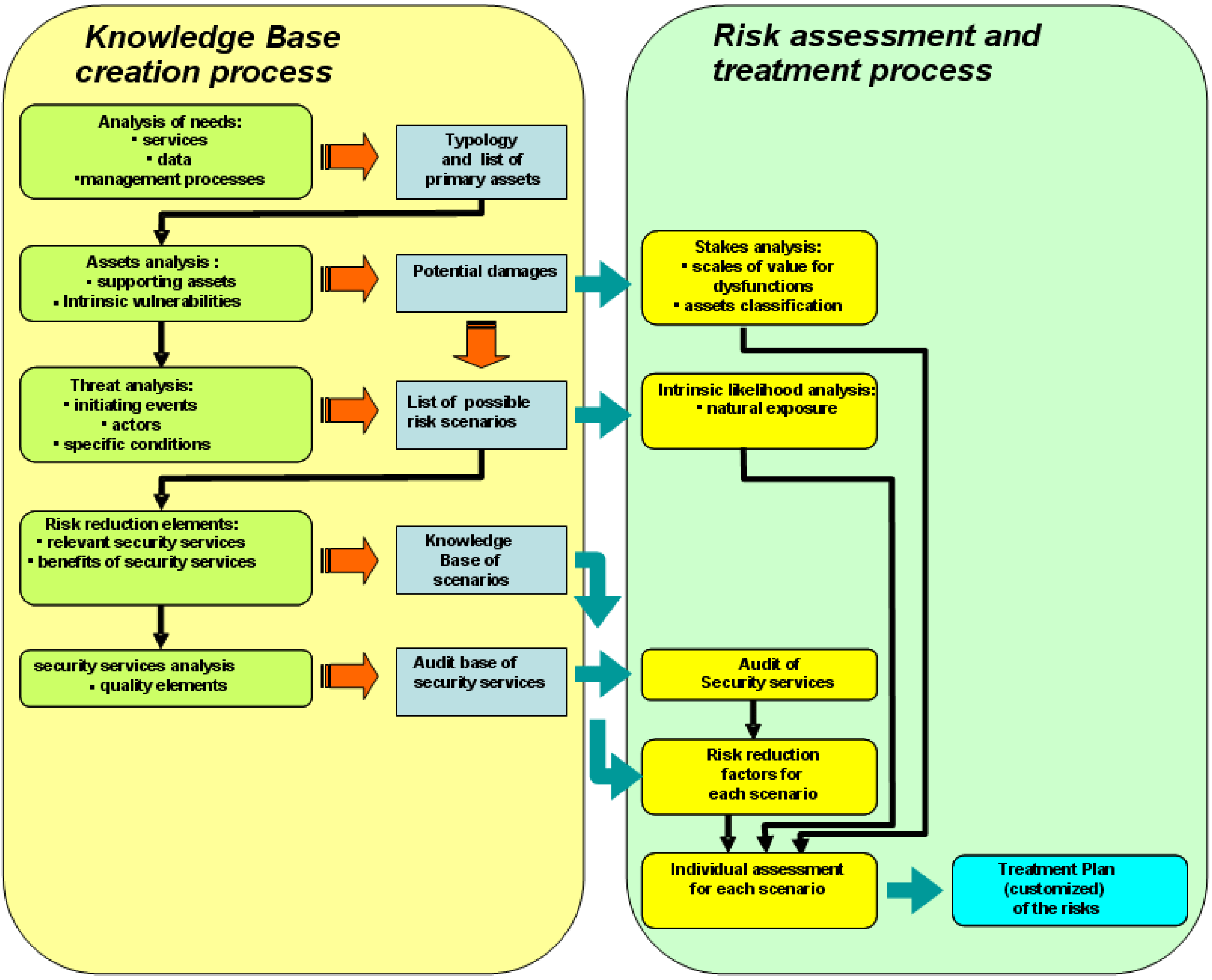
Knowledge Base creation process
Analysis of needs: • services • data •management processes
Typology and list of primary assets
Assets analysis : • supporting assets • Intrinsic vulnerabilities
Potential damages
Threat analysis: • initiating events • actors • specific conditions
List of possible risk scenarios
Risk reduction elements: • relevant security services • benefits of security services
Knowledge Base of scenarios
security services analysis • quality elements
Audit base of security services
Risk assessment and treatment process
Stakes analysis: • scales of value for dysfunctions • assets classification
Intrinsic likelihood analysis: • natural exposure
Audit of Security services
Risk reduction factors for each scenario
Individual assessment for each scenario
Treatment Plan (customized) of the risks

Figure 2: Overview of planning for risk assessment

This diagram shows that the requirements and the analysis steps are common to a number of entities and enable an approach to be constructed, together with bases and tools that can later be applied to each individual environment. This leads to the conclusion that the first two columns correspond, in fact, to a knowledge base, and that it is therefore convenient to consider separately two types of activity:

- — Creation of a knowledge base for risk assessment
- — Analysis and treatment of the risks with the aid of this knowledge base

This document covers the management of risks (analysis and creation of action plans) using the MEHARI knowledge base. Guidelines for constructing a knowledge base will be given in another document (to be provided).

2 Risk assessment

A risk assessment includes:

- Risk Identification
- Risk Analysis
- Risk Assessment

2.1 Risk identification

Identification of risks is a process that can largely be achieved using a knowledge base. Effectively, other than few risks are specific to a business or organization, the set of risk situations that all businesses and organizations face is relatively stable.

MEHARI proposes a knowledge base of risk scenarios that can be used by the vast majority of organizations. It is of course possible to develop variations, to supplement the knowledge base, or to create new knowledge bases, with the help of a specific guide.

This document assumes that MEHARI 2010 knowledge base is used.

2.1.1 Risk scenarios in the knowledge base

The standard risk situations are described by risk scenarios, organized by type of primary asset and criterion (family), that contain the following elements:

- An identifier for the classification in the family of scenarios
- The type of primary asset,
- The type of vulnerability, including:
  - The type of secondary asset considered,
  - The type of damage,
  - The criterion concerned (AIC or E))
- The type of threat, including:
  - The type of the triggering event,
  - The possible circumstances of the trigger,
  - The type of possible actor
- A description of the scenario, in text form

The rationale for these various elements is given in the document "*MEHARI 2010 - Fundamental concepts and functional specifications*"

MEHARI 2010 knowledge base contains approximately 800 standard risk scenarios.

Among all these scenarios, there may be some that are critical and require a detailed examination and other that are not relevant to the business or organization and can be ignored. It is therefore useful to select the relevant subset of scenarios.

2.1.2 Selecting risk scenarios

It is often desirable to select the relevant subset of risk scenarios before beginning a detailed estimation of their severity and their treatment.

The criteria for selecting relevant criteria could be:

- — The intrinsic seriousness of the scenario,
- — Particular forms of asset,
- — Particular types of event,
- — Particular types of circumstances or of actors.

Practical advice with MEHARI knowledge base

The column “O” of the tab “scenarios” provides filtering capabilities.

Possible selection process is the following:

- Using formulas from the spreadsheet, select parameter(s), like locations, actors, etc. to be used for a (positive or negative) filtering action

2.2 Assessing the risks identified

The introduction to this document presented a global picture of risks assessment, which is defined and explained in detail in the document “*MEHARI 2010 - Fundamental concepts and functional specifications”:*

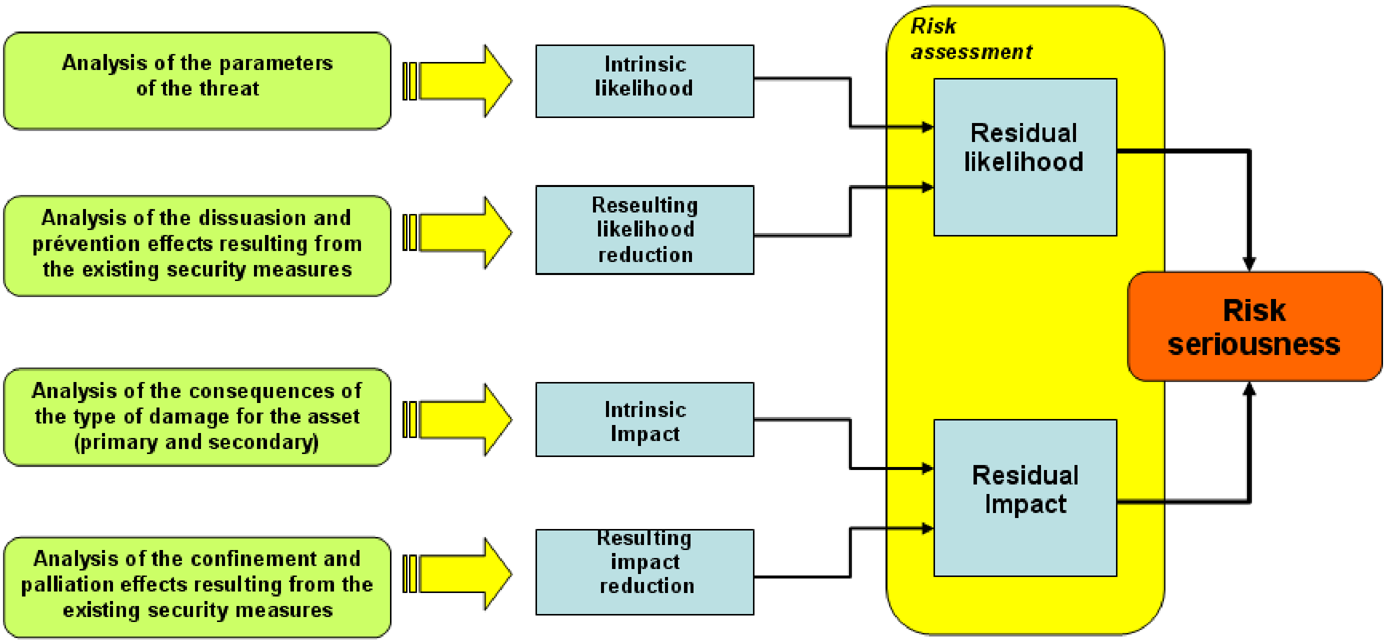
Analysis of the parameters of the threat
Intrinsic likelihood
Analysis of the dissuasion and prévention effects resulting from the existing security measures
Reseulting likelihood reduction
Analysis of the consequences of the type of damage for the asset (primary and secondary)
Intrinsic Impact
Analysis of the confinement and palliation effects resulting from the existing security measures
Resulting impact reduction
Risk assessment
Residual likelihood
Residual Impact
Risk seriousness

Figure 3: Risk assessment procedure

MEHARI offers, by means of its knowledge base, several forms of assistance in assessing risks:

- Assistance in evaluating the intrinsic likelihood,
- A generic table of intrinsic impacts that can be extended following a classification or based on a scale of values of dysfunction.
- Mechanisms for assessing risk reduction factors (deterrence, prevention, protection, palliation) depending on the quality of the security services, if this has been assessed by a MEHARI audit.

- Mechanisms for calculating the residual likelihood and impact, depending on the intrinsic likelihood, the intrinsic impact, and risk mitigation factors.
- Assistance in evaluating the resulting seriousness of the risks.

2.2.1 Assessment of the intrinsic likelihood

The "intrinsic likelihood" is an assessment of the probability that a threat occurs when no security measures are in place.

This factor is also designated, perhaps more intuitively, as the "natural exposure" **of the business or organization** to the threat.

The intrinsic likelihood of a threat is not a constant and can vary between organizations, and within an organization depending on other coincident factors.

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

2.2.1.1 Standard natural exposure (or intrinsic likelihood)

Each scenario of MEHARI knowledge base refers to a specific threat. A threat is defined by an event type and by an accompanying description of the circumstances and participants (see the explanation of the various parameters in the document "*MEHARI 2010 - Fundamental concepts and functional specifications".)*

The intrinsic likelihood or natural exposure (a value from 1 to 4) essentially depends on the event type, whether accident, error, deliberate act (malicious or not) for which there is an *a priori* assessment of the exposure.

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

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

Each scenario refers to an event type, for which a standard likelihood (potentiality) value is proposed in the knowledge base.

2.2.1.2 Enterprise-specific natural exposure for a given risk

It should be made clear that the standard evaluation provided is only a default evaluation, and that the specific evaluation of the exposure of the enterprise to the risk situation under analysis is preferable by far. For such an evaluation, refer to the definitions of levels of exposure given in the document «"*MEHARI 2010 –Fundamental concepts and functional specifications*". These are resumed in Appendix 2.

NOTE:

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

Practical realization with MEHARI knowledge base

The person in charge of risk management shall validate these values or change them in order to correspond to the correct value for the entity.

The process is then:

Open the knowledge base spreadsheet,

Select the “mask” leaf and check whether the parameter “typical events” is not masked,

Select the “typical events” leaf,

Enter the new values in the column” decided natural exposure” (this is useless if the standard value is accepted).

2.2.2 Evaluation of intrinsic impact

The intrinsic impact of a scenario is the evaluation of the consequences of the risk event actually happening, independently of any security measures.

For each of the scenarios defined in the MEHARI knowledge base, a target asset is mentioned (an asset that will be deteriorated or affected by the scenario). Each scenario clearly mentions the type of primary and supporting asset (refer to “*MEHARI 2010 –Fundamental concepts and functional specifications”* for the definition of the primary and supporting assets).

The intrinsic impact depends fundamentally on the primary asset type.

The scenario also indicates the type of damage inflicted.

This could be a type of data that is stolen, a type of service that is rendered unavailable, or a type of data that is altered, depending on whether it is a scenario involving the confidentiality, availability, or integrity of an asset, which are the three criteria taken into account by MEHARI as standard. An additional criterion, effectiveness, is considered for assets of type “management process”.

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

The classification approach used by MEHARI enables the creation of a generic classification table. This table shows the kinds of assets specifically identified through the knowledge base scenarios. The classification approach is described in the document “*MEHARI 2010 – Fundamental concepts and functional specifications*” and in the “*Security Stakes Analysis and Classification Guide*”.

2.2.2.1 *The intrinsic impact table*

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

Intrinsic impact table			
Data and information type of assets	A	I	C
D01 Data files or application databases			
D07 Electronic Mail			
…/…			
Service type of asset			
S01 Mainframes, application servers,			

This table is automatically completed (with a value from 0 to 4) for the level of the consequence or impact on availability, integrity or confidentiality for each type of identified asset. However, certain entries will not be filled, for example that for confidentiality of some services.

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

At the worst, it can be done directly, but the classification approach defined in the above guide, is undoubtedly better.

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

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

2.2.2.2 *Extending the intrinsic impact table*

The standard MEHARI table only refers to three standard criteria: availability, integrity and confidentiality. Other criteria can, of course, be used. The table can be extended to include such criteria as proof, trace-ability, audit-ability, and so on.

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

The RISICARE[1] software package enables up to eight criteria to be taken into account.

[1] Registered trademark of BUC S.A.

2.2.2.3 Evaluating intrinsic impact of scenarios

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

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

2.2.2.4 Cartographic decomposition

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

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

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

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

This capability is not directly usable with the knowledge base spreadsheet but may be realized with RISICARE^{TM} software.

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

2.2.3 Evaluating risk reduction factors through a MEHARI security audit

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

Risk reduction factors are dissuasion and prevention for likelihood; protection and palliation for impact.

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

This automated evaluation is carried out in two steps:

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

2.2.3.1 *Efficiency indicators for security services by scenario and risk reduction measure*

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

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

EFF-DISS for the efficiency of *dissuasive measures*

EFF-PREV for the efficiency of *preventive measures*

EFF-PROT for the efficiency of *protective measures*

EFF-PALL for the efficiency of *palliative measures*

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

The formulae provided in the MEHARI knowledge base call on:

- Either a security service directly, by its identifier[2], when the service is the only one to have this type of effect on the scenario;
- Or formulae that contain functions: MIN(arg1 ; arg2 ; …) or MAX(arg1 ; arg2 ; …), the parameters (arg1 ; arg2, …) are being identifiers of security services of the MEHARI knowledge base.

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

EFF-PALL = 06B01

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

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

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

NOTE:

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

The MAX function signifies that the services called as parameters are alternatives. If one of the services is of a high quality level, so the whole will be of a high quality level. An example of such a case, depending on certain scenarios, is in data access control and the encryption of the data itself.

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

The formulas are integrated into MEHARI 2010 knowledge base.

[2] the identifier of a sub-service is composed of a domain number, a letter indicating the service to which it is attached, and a sub-service number (e.g.: 06B01)

2.2.3.2 "Calculated" risk reduction factors

Clearly, the efficiency coefficients evaluated above EFF-XXXX are calculated on the basis of service quality values, which have no reason to be integer values, and the efficiency coefficients are not themselves integer values either. To make the final evaluation of likelihood and impact easier, MEHARI transforms them into integer values, using the closest integer value.

MEHARI knowledge base gives a calculated value (from 0 to 4) for the risk reduction factors by using the quality of service value indicated in the "service" tab.

When a domain of services exhibits several "variants" in the audit schema (as explained in "*MEHARI 2010 - Evaluation guide for security services*"), the formulas of the knowledge base retain, for the risk reduction calculation, the minimum value of the variants (note that Risicare allows to treat more precisely the audit schema).

Practical realization with MEHARI knowledge base

The value of the risk reduction factors is given in the columns "dissuasion", "prevention", "confining" and "palliative" of the "scenarios" tab.

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

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

Whenever one disagrees with the values, it is not advised to change the values directly in the "scenarios" tab as this would definitely suppress the formulas of the knowledge base, but to enter the preferred values in the "I decided" and "P decided" columns of the "scenarios" tab.

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

2.2.4 Evaluation of residual likelihood and impact

2.2.4.1 Automated likelihood evaluation: STATUS-P

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

MEHARI evaluates the "residual likelihood" under the denomination STATUS-P. This is deduced directly from the- natural exposure and STATUS-DISS and STATUS-PREV by the evaluation tables.

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

- — Natural event or accident,
- — Human error,

— Voluntary action (malicious or not),

These standard tables can be modified if required.

Note:

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

2.2.4.2 Automated impact evaluation: STATUS-I

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

MEHARI knowledge base contains 4 standard tables allowing to assess the residual impact (STATUS-I), depending on the type of criterion associated with the scenario:

— Availability,

— Integrity,

— Confidentiality or disclosure,

— “Limitable”[3]

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

These standard tables can also be modified if required, by an expert of the method.

Note:

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

2.2.4.3 Evaluation table construction principles

In practice, standard tables, whether for likelihood or impact, are built using a certain number of principles. It is possible to modify these tables, based on a new set of principles.

Standard evaluation tables are documented in Appendix 5.

[3] This type of scenario generally corresponds with the case where integrity is hit, for which there is no palliation measure applicable, but whose impact may be limited thanks to specific confining measures.

2.2.4.4 Evaluating likelihood and impact

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

These automatic procedures and formulas give values for the residual likelihood and impact, under the form of STATUS-P and STATUS-I.

A final judgment should be made, as a general rule, on the pertinence of the levels of likelihood P and impact I.

Practical realization with MEHARI knowledge base

In Practice, the calculated values of residual likelihood and Impact (that is using the quality of the security services) are transferred into the columns “I computed” and “I computed” of the “scenarios” tab..

It is possible to set different values in the columns “I decided” and “P decided”. Then these decided values will be taken into account for the calculation of the (residual) “computed seriousness”

2.3 Evaluating the seriousness of a scenario

The seriousness of a scenario will be deduced from the evaluations of residual likelihood and impact, STATUS-P and STATUS-I.

This corresponds to a judgment about the character acceptable or not of each risk scenario as it has been presented in “*MEHARI 2010 –Fundamental concepts and functional specifications*”.

The process relies over the risk acceptability table, as defined in the above document.

This table is an essential strategic document, which should be defined for each organization. In the absence of a specific thinking, MEHARI knowledge base provides, under “seriousness” tab, a standard table, which, anyway, needs to be understood and accepted.

3 Risk treatment

Risk treatment consists, in theory, of analyzing each risk scenario and taking specific decisions, which could be the following:

- Accept the risk as it is,
- Reduce the risk, by taking measures to diminish the impact or the likelihood (or both), thereby reducing the residual seriousness of the risk,
- Avoid the risk by removing the risk situation using structural or organizational measures,
- Transfer the risk, typically through insurance.

In practice, it is logical to organize this work in a structured way, and several approaches could be adopted, including:

- Work by families of scenarios considering the same types of asset and therefore the same intrinsic impact, and select action plans by family.
- Work by federated projects, each project involving services with similar purposes (for example physical access control, rights management and clearance)
- Work service after service using the idea of "service need"

3.1 Selecting action plans by scenario family

To facilitate this approach, the scenarios in the MEHARI knowledge base are grouped into families corresponding to the same asset type and same type of damage.

For each family, action plans are proposed (on the Action_Plans tab) for each type of effect (deterrence, prevention, confinement or protection, palliation), each plan groups the relevant services for the family of scenarios under consideration, and determines for each service a target level on completion of the action plan.

If the option of taking into account objectives for the risk assessment was chosen, the selection of action plans permits a simulation of the level of seriousness of each risk scenario on completion of the actions plans.

The recommended procedure consists of the following steps:

- For each family, select the most effective plans. To this end, the knowledge base gives each plan an effectiveness indicator that reflects the percentage of scenarios in the family influenced by the implementation of the plan.
- Where appropriate, modify the goals for the services mentioned in the selected plans.
- Validate the set of action plans, by visualizing the resulting risks after implementation.
- For each scenario where the risk is not reduced by the selected plans, choose one of the following:
    - ➢ Select additional measures (repeating the earlier steps)
    - ➢ Accept the risk, at least temporarily

- Avoid the risk
- Transfer the risk

To help with this procedure, the MEHARI knowledge base includes the following:

- A global view of all the risk scenarios by asset type, showing the number of scenarios and their gravity for each type of primary asset and for each of the classification criteria. Hypertext links provide an automatic connection from the global view to the asset types in the "Action_Plans" tab.
- A view of the same scenarios grouped by type of threat.

3.2 Defining and selecting projects

It is also possible to define projects grouping various services, with each project definition indicating:

- The services for which the project should deliver improvements
- The target level of quality for the services at the end of the project
- The completion date for the project

A project is taken into account when assessing the level of risk of the scenarios if this option is selected and if the project completion date is prior to a specified reference date.

This enables simulations to be made using different time frames, and creation of a risk dashboard.

The selection of services and their target levels in each project is completely open, and could be based on the actions plans described in the previous section or on the idea of "service need" described below.

3.3 Service need

A "service need" indicator can be defined, taking into account the number of scenarios that call on a given service, the gravity of the scenarios, and the effectiveness of the plans in which this service is implicated.

This is only an indicator, but it is reasonable to prioritize improvements for those services which show the greatest need.

3.4 Other approaches

Many other approaches are possible, notably that of selecting small subsets of scenarios according to various criteria and of addressing each subset separately.

4 Practical advice

4.1 Spirit of the risk assessment process

In this guide, the automatic features of Mehari are explained so as to assist in the risk assessment.

It must be kept in mind, however that a consensus within the group of persons completing the assessment shall be more reliable than automatisms.

4.2 Composition of the risk assessment group

The process shall be more efficient if the risk assessment is effected by a group representing the stakeholders. So the composition of this group is important. It should include:

- Users of each concerned domain of business at a sufficient level allowing to judge the effective reduction of the risk level that may be provided by the security measures,
- ITC staff able to explain to the risk assessment group the effectiveness of the various security measures and the turnarounds that should be prevented (robustness and control),
- A group leader, well trained about the method and capable about information systems security.

4.3 Control of the automatic calculations

As mentioned above, the automatic calculations should only be considered as facilitators in the assessment process. This implies that a control of the results obtained should be always be done in order for the group to validate each intermediary result, such as:

- Quality level of the security services,
- Risk reduction contributions,
- Assessment of the calculated residual likelihood and impact,
- Calculated residual seriousness of the risk scenarios.

In order to do so, we recommend comparing the results of the calculations for each of the above parameters.

Appendix 1:
Standard table of natural exposure

Family type	***Code type***	***Event description***	***Code***	***Natural exposure (standard CLUSIF)***
Absence of personnel due to an accident	AB.P	Absence of personnel from partner	AB.P.Pep	3
		Absence of internal personnel	AB.P.Per	2
Accidental lack or unavailability of service	AB.S	Absence of service : Power supply	AB.S.Ene	3
		Absence of service : Air conditioning	AB.S.Cli	2
		Absence of service : Impossibility to have access to the premises	AB.S.Loc	2
		Absence or impossibility of application software maintenance	AB.S.Maa	3
		Absence or impossibility of information system maintenance	AB.S.Mas	2
Environmental serious accident	AC.E	Lightning	AC.E.Fou	2
		Fire	AC.E.Inc	2
		Flooding	AC.E.Ino	3
Hardware accident	AC.M	Equipment breakdown	AC.M.Equ	3
		Accessory equipment breakdown	AC.M.Ser	3
Voluntary absence of personnel	AV.P	Social conflict with strike	AV.P.Gre	2
Conceptual error	ER.L	Software blocking or malfunction due to a design or programming error (in-house software)	ER.L.Lin	3
Hardware error or behavioural error by personnel	ER.P	Lost or forgotten document or media	ER.P.Peo	3
		Error of operation or non compliance of a procedure	ER.P.Pro	3
		Typing or data entry error	ER.P.Prs	3
Incident due to environment	IC.E	Damage due to ageing (of equipment)	IC.E.Age	2
		Water damage	IC.E.De	3
		Electrical boosting or over load	IC.E.Se	2
		Pollution damage	IC.E.Pol	2
Logical or functional incident	IF.L	Production incident	IF.L.Exp	3
		Software blocking or malfunction (information system or software package)	IF.L.Lsp	2
		Saturation due to an external cause (worm)	IF.L.Ver	3
		Virus	IF.L.Vir	4
Malevolent action (logical or functional)	MA.L	Deliberate blocking of accounts	MA.L.Blo	2
		Deliberate erasure or massive pollution of system configurations	MA.L.Cfg	2
		Deliberate erasure of files, data bases or media	MA.L.Del	2
		Electromagnetic pick up	MA.L.Ele	3
		Deliberate corruption of data or functions	MA.L.Fal	3
		Forging of messages or data	MA.L.Fau	3
		Fraudulent replay of transaction	MA.L.Rej	2
		Deliberate saturation of IT equipments or networks	MA.L.Sam	3
		Deliberate total erasure of files and backups	MA.L.Tot	2

Family type	***Code type***	***Event description***	***Code***	***Natural exposure (standard CLUSIF)***
		Diversion of files or data (tele-load or copy)	MA.L.Vol	3
Malevolent action (physical)	MA.P	Tampering or falsification of equipment	MA.P.Fal	2
		Terrorism	MA.P.Ter	2
		Vandalism or hooliganism	MA.P.Van	2
		Theft of physcial asset	MA.P.Vol	2
Non compliance to procedures	PR.N	Inadequate procedures	PR.N.Api	2
		Procedures not applied due to lack of resource or means	PR.N.Naa	2
		Procedures not applied due to ignorance	PR.N.Nam	2
		Procedures not applied deliberately	PR.N.Nav	2

Appendix 2: Definition of natural exposure levels

Natural exposure to risk

Level 1: Very low exposure

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

Level 2: Low exposure (hardly exposed).

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

Level 3: Medium exposure (not particularly exposed)

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

Level 4: High exposure: (particularly exposed).

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

Appendix 3: Intrinsic impact table

Intrinsic Impact table

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	0	▨	▨
G02	Telecommunication Services (voice, fax, audio & videoconferencing, etc.)	0	0	▨
IT and Networking Services				
R01	Extended Network Service	0	0	▨
R02	Local Area Network Service	0	0	▨
S01	Services provided by applications	0	0	0
S02	Shared Office Services (servers, document management, shared printers, etc.)	0	0	▨
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.**	0	▨	▨
S04	Common Services, working environment: messaging, archiving, print, editing, etc.	0	0	▨
S05	Web editing Service (internal or public)	0	0	▨
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 of information systems		▨	▨
C06	Compliance to law or regulations relative to people safety and protection of environment		▨	▨
Nota : Grey cells represent those asset security criteria for which, in general, no classification is needed and no scenario exists in the knowledge base.				
Légende :				
A	Availability			
I	Integrity			
C	Confidentiality			
E	Efficiency (of the management process, regarding compliance to law and regulations). For this criteria, the decision grid L will be used for impact reduction.			

Appendix 4:
Definition of risk reduction factor levels

Dissuasive measures

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

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

Level 2: The effect of dissuasive measures is medium.

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

Level 3: The effect of dissuasive measures is high.

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

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

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

Preventive measures

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

Any person in the organization, or close to it, or even someone who knows something about it, is capable of setting this scenario in motion, with the means at their disposal (or easy to obtain).
Perfectly ordinary circumstances can be the cause of this scenario (misuse, error, ordinary unfavorable conditions).

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

A professional can set off the scenario, without the need for special means or tools outside of those available in the profession.
Rare natural circumstances can produce the same result.

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

Only a specialist or a professional with special tools or means, or a group of professionals in collusion and using their collective means and tools could succeed.
This is usually the result of the conjunction of rare or exceptional circumstances.

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

Only a few determined experts, with exceptional means, could succeed.
Only the conjunction of very rare or extremely exceptional circumstances would permit this scenario to happen.

Protective measures or confinement

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

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

The possible protective measures then only have a restricted influence on the level of the direct consequences.

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

Even if the damage and its direct consequences can be limited, the time to detect it is long, or reaction is slow.
The protective measures that are used have a real influence on the result, but the direct consequences are still very big.

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

The event is rapidly detected, with immediate reaction.

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

Level 4: The measures have a very strong effect.

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

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

Palliative measures

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

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

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

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

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

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

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

Normal operations continue without any noticeable interruption.

Appendix 5:
Standard evaluation tables

Grids of evaluation of STATUS-P

1. Scenarios resulting from an Accident

EXPO = 1

D				
I				
S				
S 1	1	1	1	1
	1	2	3	4
	P	R	E	V

EXPO = 2

D				
I				
S				
S 1	2	2	2	1
	1	2	3	4
	P	R	E	V

EXPO = 3

D				
I				
S				
S 1	3	3	2	1
	1	2	3	4
	P	R	E	V

EXPO = 4

D				
I				
S				
S 1	4	4	2	1
	1	2	3	4
	P	R	E	V

2. Scenarios resulting from an Error

EXPO = 1

D				
I				
S				
S 1	1	1	1	1
	1	2	3	4
	P	R	E	V

EXPO = 2

D				
I				
S				
S 1	2	2	2	1
	1	2	3	4
	P	R	E	V

EXPO = 3

D				
I				
S				
S 1	3	3	2	1
	1	2	3	4
	P	R	E	V

EXPO = 4

D				
I				
S				
S 1	4	4	2	1
	1	2	3	4
	P	R	E	V

3. Scenarios resulting from a Volontary action

EXPO = 1

D 4	1	1	1	1
I 3	1	1	1	1
S 2	1	1	1	1
S 1	1	1	1	1
	1	2	3	4
	P	R	E	V

EXPO = 2

D 4	1	1	1	1
I 3	2	2	1	1
S 2	2	2	2	1
S 1	2	2	2	1
	1	2	3	4
	P	R	E	V

EXPO = 3

D 4	2	2	1	1
I 3	2	2	1	1
S 2	3	3	2	1
S 1	3	3	2	1
	1	2	3	4
	P	R	E	V

EXPO = 4

D 4	2	2	2	1
I 3	3	3	2	2
S 2	4	4	3	2
S 1	4	4	3	2
	1	2	3	4
	P	R	E	V

Grids of of evaluation of STATUS-I

The non evolutionary scenarios are represented on the nc line

1. Scenarios affecting Availability

II = 1

C 4	1	1	1	1
O 3	1	1	1	1
N 2	1	1	1	1
F 1	1	1	1	1
nc	1	1	1	1
	1	2	3	4
	P	A	L	L

II = 2

C 4	2	2	1	1
O 3	2	2	1	1
N 2	2	2	2	1
F 1	2	2	2	1
nc	2	2	2	1
	1	2	3	4
	P	A	L	L

II = 3

C 4	2	2	1	1
O 3	3	2	2	1
N 2	3	3	2	1
F 1	3	3	2	1
nc	3	3	2	1
	1	2	3	4
	P	A	L	L

II = 4

C 4	2	2	2	1
O 3	3	3	2	1
N 2	4	3	2	1
F 1	4	3	2	1
nc	4	3	2	1
	1	2	3	4
	P	A	L	L

2. Scenarios affecting Integrity

II = 1

C 4	1	1	1	1
O 3	1	1	1	1
N 2	1	1	1	1
F 1	1	1	1	1
nc	1	1	1	1
	1	2	3	4
	P	A	L	L

II = 2

C 4	1	1	1	1
O 3	2	2	1	1
N 2	2	2	2	1
F 1	2	2	2	1
nc	2	2	2	2
	1	2	3	4
	P	A	L	L

II = 3

C 4	1	1	1	1
O 3	2	2	1	1
N 2	3	3	2	1
F 1	3	3	2	1
nc	3	3	2	2
	1	2	3	4
	P	A	L	L

II = 4

C 4	1	1	1	1
O 3	2	2	2	1
N 2	3	3	2	1
F 1	4	3	2	1
nc	4	4	4	4
	1	2	3	4
	P	A	L	L

3. Scenarios affecting Confidentiality

II = 1

C 4	1			
O 3	1			
N 2	1			
F 1	1			
nc	1			
	1			
	P	A	L	L

II = 2

C 4	2			
O 3	2			
N 2	2			
F 1	2			
nc	2			
	1			
	P	A	L	L

II = 3

C 4	2			
O 3	2			
N 2	3			
F 1	3			
nc	3			
	1			
	P	A	L	L

II = 4

C 4	2			
O 3	2			
N 2	3			
F 1	4			
nc	4			
	1			
	P	A	L	L

4. Type L (limitable) scenarios

II = 1

C 4	1			
O 3	1			
N 2	1			
F 1	1			
	1	2	3	4
	P	A	L	L

II = 2

C 4	1			
O 3	2			
N 2	2			
F 1	2			
	1	2	3	4
	P	A	L	L

II = 3

C 4	1			
O 3	2			
N 2	3			
F 1	3			
	1	2	3	4
	P	A	L	L

II = 4

C 4	1			
O 3	2			
N 2	3			
F 1	4			
	1	2	3	4
	P	A	L	L

THE SPIRIT OF EXCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

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

Load CLUSIF productions from

www.clusif.asso.fr