

METHODS



## **MEHARI 2010**

### **Processing guide for risk analysis and management**

Version 2: April 2011



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

Tel.: +33 1 53 25 08 80 – Fax: +33 1 53 25 08 88 – e-mail: [clusif@clusif.asso.fr](mailto:clusif@clusif.asso.fr)

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

MEHARI is a registered trademark of CLUSIF.

The French law of March 11th, 1957 only permits "copies or reproductions strictly reserved for individual private – not public – use", or analyses and short quotations used as examples or illustrations (Article 41, paragraphs 2 and 3). Therefore, "any representation or reproduction, whether partial or complete, made without the approval of the author, of entitled parties or of the legal successors is prohibited" (Article 40, paragraph 1).

Any form of representation or reproduction would therefore constitute an infringement of copyright, an offence punishable under Article 425 et seq. of the French Penal code.

# Table of contents

Table of contents.....	3
Acknowledgments.....	4
Introduction.....	5
1. Preparatory phase.....	6
1.1 Evaluating context.....	7
1.1.1 Evaluating the strategic context.....	7
1.1.2 Evaluating the technical context.....	8
1.1.3 Evaluating the organizational context.....	9
1.2 Setting the scope and boundaries of the risk analysis and treatment operation.....	10
1.2.1 Technical perimeter of risk analysis and treatment.....	10
1.2.2 Organizational perimeter of risk analysis and treatment.....	11
1.2.3 Oversight structure of the operation.....	12
1.3 Establishing the technical parameters of the risk analysis.....	13
1.3.1 Establishing the risk acceptability table.....	13
1.3.2 Establishing the natural exposure table.....	14
1.3.3 Establishing evaluation tables for residual potentiality and impacts.....	15
2. Risk analysis – operational phase.....	16
2.1 Stakes analysis and asset classification.....	17
2.1.1 Malfunction value scale.....	17
2.1.2 Asset classification.....	18
2.1.3 Intrinsic impact table.....	19
2.2 Assessing security service quality.....	20
2.2.1 Establishing the audit schema.....	20
2.2.2 Evaluating security service quality.....	21
2.3 Risk assessment.....	22
2.3.1 Selecting risk scenarios.....	22
2.3.2 Risk assessment.....	23
3. Risk treatment and planning phase.....	24
3.1 Planning of immediate measures.....	25
3.1.1 Selecting risks for immediate treatment.....	25
3.1.2 Selecting measures for immediate implementation.....	26
3.2 Planning of context-specific measures.....	27
3.2.1 Treatment strategy and priority setting.....	27
3.2.2 Selecting measures and planning.....	28
3.3 Implementation of risk treatment oversight.....	29
3.3.1 Oversight planning.....	29
3.3.2 Selecting indicators, dashboards and trend chart.....	30

## Acknowledgments

The CLUSIF would like to thank the members of the Methods working group for their contributions and specially Jean-Philippe Jouas for his outstanding contributions.

Jean-Louis Roule has managed the English translation of this document.

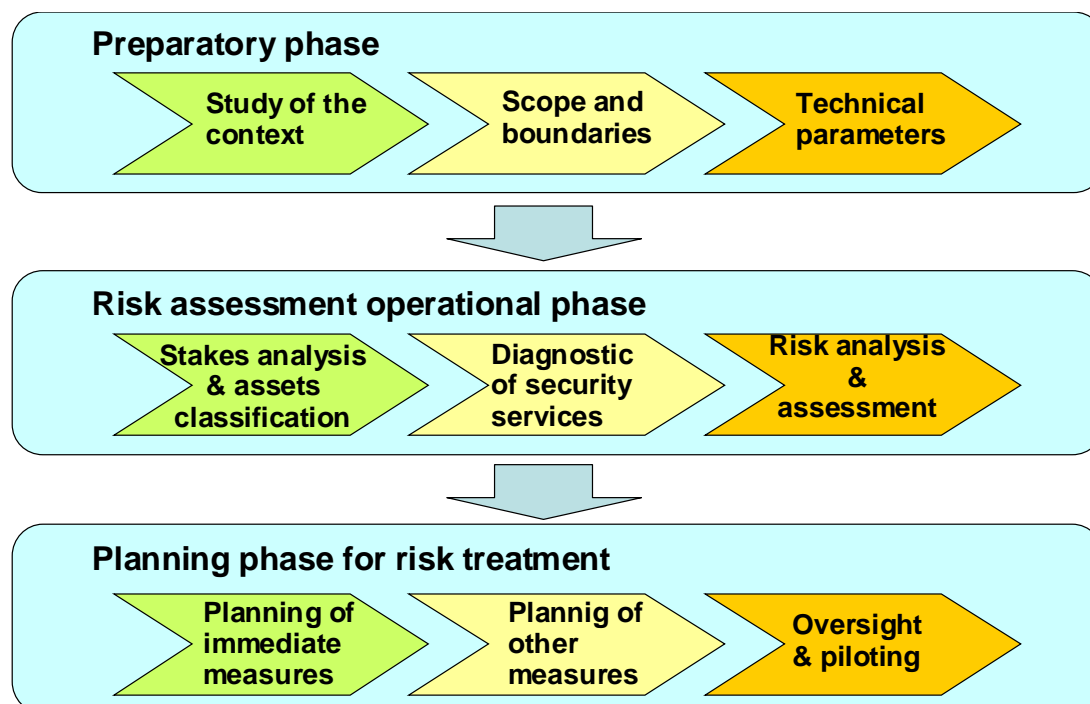
## Introduction

This guide presents MEHARI overall processing for risk analysis and treatment and describes the different steps involved.

It is based on the use of MEHARI 2010 knowledge base.

### General presentation of the overall process

The MEHARI approach involves three phases, as illustrated in the diagram below.



These phases are explained in the following sections and chapters.

### Mehari and compliance to ISO/IEC 27001:2005 standard.

Mehari follows a complete process of risk assessment and management compliant to the continuous improvement model provided by the ISO/IEC 27001:2005 standard; additionally, Mehari answers to the guidelines set forth by ISO/IEC 27005:2008.

The presentation of the phases in this guide can be compared to the one proposed by ISO/IEC 27003 standard, with the benefit that it is directly usable by any organization seeking to manage risks or an ISMS with the support of Mehari.

Note also that the knowledge bases contain a questionnaire domain “14 Ism” which, in the scope of an ISMS, allows stating the level of compliance of the audited organization.

The knowledge bases file, as downloaded from CLUSIF, cannot anticipate the effective operations and responsibilities during the risk assessment itself; several of the deliverables mentioned in this document can contribute to the creation of a folder attached to the activities and decisions taken during the process and to record the customization of the method by the organization undertaking a Mehari based project.

# 1. Preparatory phase

The preparatory phase is subdivided into three main steps. Ideally they should be carried out one after the other, but this is not absolutely necessary.

The steps are:

- 1.1 Evaluating context
  - 1.1.1 Strategic context
  - 1.1.2 Technical context
  - 1.1.3 Structural context
- 1.2 Determining the scope and boundaries for the risk analysis and treatment operation
  - 1.2.1 Technical perimeter
  - 1.2.2 Organizational perimeter
  - 1.2.3 Piloting structure
- 1.3 Establishing the main risk analysis parameters
  - 1.3.1 Risk acceptability table
  - 1.3.2 Natural exposure table
  - 1.3.3 Risk evaluation tables

## ***1.1 Evaluating context***

### ***1.1.1 Evaluating the strategic context***

#### ***Objectives***

To establish a number of points that should be clarified and taken into account for risk analysis and treatment.

The following elements should be considered:

- Strategic positioning of the entity on its market (for commercial entities) or its structure in a political context (for public organizations and services):
  - Market position (dominant or not),
  - Competitive nature of the activity,
  - Critical thresholds of services provided,
  - Media focus on incidents and malfunctions,
  - Etc.
- Constraints weighing on the operation and structure of the entity
  - Legal constraints,
  - Regulatory constraints,
  - Rules to be followed.
- Information security policy
  - Security goals (if they exist),
  - Role of risk analysis and treatment in security policy,
  - Entity requesting risk analysis and treatment,
  - Management support.

#### ***Prerequisites***

To begin this task, it is important that mission orders for the risk analysis and treatment operation be already established.

#### ***Participants and stakeholders***

The organizer of this task is the person responsible of the risk analysis and treatment operation.

Stakeholders are:

- Business managers,
- General management,
- The legal department (legal constraints),
- The CISO.

#### ***Deliverable***

The deliverable is a document that synthesizes the various stated objectives.

#### ***Process – implementation guidelines***

The process involves the following:

- Collection of elements available on the stated objectives,
- Creation of a summary,
- Approval by the Management Committee or directly by General Management.

### ***1.1.2 Evaluating the technical context***

#### ***Objectives***

To collect and establish data and technical information that will be necessary for risk analysis and treatment.

The following elements should be considered:

- The information system architecture
  - Network architecture,
  - Systems architecture,
  - Application architecture,
  - Overall cartography.
- Plans for (or likelihood of) technical evolutions in the short, medium and long term
  - Development plans,
  - Durability of operational solutions.
- Crucial external suppliers and providers
  - Structural service providers (network access and services, facility management, etc.),
  - Software providers,
  - Occasional service providers (maintenance, assistance, etc.).

#### ***Prerequisites***

Pre-existing cartography, or at least an up-to-date inventory of IT equipment, systems and applications.

#### ***Participants and stakeholders***

The organizer of this task is the person responsible of the risk analysis and treatment operation, possibly delegated to a member of his/her team.

Stakeholders are:

- The CIO (Chief Information Officer),
- The chief networks officer (if different from the CIO).

#### ***Deliverable***

The deliverable is a cartography (complete or summarized) and related lists (equipment, applications, etc.).

#### ***Process – implementation guidelines***

The process involves the following:

- Collection of the various technical elements available,
- Creation of a summary,
- Approval by the CIO.



### ***1.1.3 Evaluating the organizational context***

#### ***Objectives***

To collect and establish data and information about the entity's structure that will be needed for risk analysis and treatment.

The following elements should be considered:

- The complete organization chart of the entity
  - Hierarchical relationships,
  - Functional links and relationships.
- Distribution of responsibilities for security matters
  - Job descriptions and associated memos,
  - Division of responsibilities among site managers, activity managers, the CIO and CISO.
- Oversight structure
  - Existing process for proposing and approving action plans,
  - Setting-up and operating modes of oversight structures.

#### ***Prerequisites***

Pre-existing complete and detailed organization chart and notes defining functions.

#### ***Participants and stakeholders***

The organizer of this task is the person responsible of the risk analysis and treatment operation, possibly delegated to a member of his/her team.

Stakeholders are:

- HRM (Human Resources Manager) or management of the organization (where applicable),
- Financial and administrative officer,
- CISO.

#### ***Deliverable***

The deliverable is a summary of the entity's structure and the distribution of responsibilities in terms of information security and implementation of corrective action plans.

#### ***Process – implementation guidelines***

The process involves the following:

- Collection of the various technical elements available,
- Creation of a summary,
- Approval by general management.

## ***1.2 Setting the scope and boundaries of the risk analysis and treatment operation***

### ***1.2.1 Technical perimeter of risk analysis and treatment***

#### ***Objectives***

To formally establish the technical scope for the initiating operation of risk analysis and treatment.

The following elements should be considered:

- Geographical perimeter
  - Sites/locations,
  - Countries, if required.
- Information systems concerned
  - General information systems,
  - Exclusion (or not) of industrial process management systems,
  - Exclusion (or not) of computer-assisted design systems,
  - Etc.
- Types of information media concerned
  - Digital media,
  - Printed and written media,
  - Voice and audio media.

#### ***Prerequisites***

Pre-existing summary of information system cartography.

#### ***Participants and stakeholders***

The organizer of this task is the person responsible of the risk analysis and treatment operation.

Stakeholders are:

- General management or client ordering the mission,
- CISO.

#### ***Deliverable***

The deliverable is a summary of the technical scope of the risk analysis and treatment operation.

#### ***Process – implementation guidelines***

The process involves the following:

- Collection of the various options and client's choices,
- Creation of a summary
- Approval by general management

## ***1.2.2 Organizational perimeter of risk analysis and treatment***

### ***Objectives***

To formally establish the organizational scope of risk analysis and treatment for the planned operation.

The following elements should be considered:

- Activity perimeter
  - Activities concerned,
  - Subsidiaries, units or services, where applicable.
- Types of risks included in the operation
  - All information related risks,
  - Limitation to one or several types of risk (disclosure or fraud, for example).

### ***Prerequisites***

Pre-existing summary of the entity's structure.

### ***Participants and stakeholders***

The organizer of this task is the person responsible of the risk analysis and treatment operation.

Stakeholders are:

- General management or the client
- CISO

### ***Deliverable***

The deliverable is a summary of the structural scope of the risk analysis and treatment operation.

### ***Process – implementation guidelines***

The process involves the following:

- A survey of the various options and client's choices.
- Creation of a summary
- Approval by general management

### ***1.2.3 Oversight structure of the operation***

#### ***Objectives***

To formally establish the oversight structure of the operation and the relationship between the risk analysis and treatment team and the client and general management.

The following elements should be considered:

- Structure and operating modes of the Oversight Committee for the operation
  - Participants
  - Meeting schedule
- Types of deliverables and approval methods

#### ***Prerequisites***

Pre-existing summary of the entity's structure.

#### ***Participants and stakeholders***

The organizer of this task is the person responsible of the risk analysis and treatment operation.

Stakeholders are:

- General management or the client,
- CISO

#### ***Deliverable***

The deliverable is a summary of the oversight structure of the risk analysis and treatment operation. An initial meeting with the Oversight Committee should be organized.

#### ***Process – implementation guidelines***

The process involves the following:

- A survey of the client's various options and choices,
- Creation of a summary,
- Approval by general management.

### ***1.3 Establishing the technical parameters of the risk analysis***

Prior to actually analyzing risks, the following parameters need to be established:

- The risk acceptability table,
- The natural exposure (or intrinsic likelihood) table,
- The risk evaluation tables.

#### ***1.3.1 Establishing the risk acceptability table***

##### ***Objectives***

To formally establish the risk acceptability table, used afterwards to determine whether a risk scenario is tolerable or not.

This table is presented in the “*Mehari 2010: risk analysis and treatment guide*”.

##### ***Prerequisites***

Pre-existing summary of the oversight structure for risk analysis and treatment.

In addition, the Oversight Committee, which is a key stakeholder in this task, must have a prior, thorough understanding of the Mehari risk model.

##### ***Participants and stakeholders***

The organizer of this task is the person responsible of the risk analysis and treatment operation.

Stakeholders are:

- General management or the client,
- Oversight Committee for the operation,
- CISO

##### ***Deliverable***

The deliverable is the risk acceptability table and any terminology associated with each risk category.

##### ***Process – implementation guidelines***

The process involves the following:

- Drafting of a risk acceptability table,
- Approval by general management.

Note: this draft can be built from the table presented in the Mehari knowledge base and provided as an example in the “*Mehari 2010: Risk analysis and treatment guide*”. Approval by general management is necessary.

### ***1.3.2 Establishing the natural exposure table***

#### ***Objectives***

To formally establish the natural exposure table or intrinsic likelihood table used afterwards to establish the intrinsic potentiality of the risk scenarios in the knowledge base.

This table is presented in “*Mehari 2010 risk analysis and treatment guide*” and in “*Mehari 2010 Fundamental concepts and functional specifications*”.

#### ***Prerequisites***

The Oversight Committee, which is a key stakeholder in this task, must have a prior, thorough understanding of the Mehari risk model.

#### ***Participants and stakeholders***

The organizer of this task is the person responsible of the risk analysis and treatment operation.

Stakeholders are:

- The Oversight Committee for the operation,
- The CISO

#### ***Deliverable***

The deliverable is the risk acceptability table and any terminology associated with each risk category.

#### ***Process – implementation guidelines***

The process involves the following:

- Drafting of the natural exposure table,
- Approval by Oversight Committee.

Note: this draft can be the basic natural exposure table presented in the Mehari knowledge base and provided as an example in the “*Mehari 2010: Risk analysis and treatment guide*”. Approval by the Oversight Committee is necessary.

### ***1.3.3 Establishing evaluation tables for residual potentiality and impacts***

#### ***Objectives***

To formally establish tables allowing evaluating residual potentiality and impact based on both intrinsic potentiality/impact and risk reduction factors in each knowledge base scenario.

These tables are presented in “*Mehari 2010: risk analysis and treatment guide*” and in “*Mehari 2010 – Fundamental concepts and functional specifications*”.

#### ***Prerequisites***

In addition, the Oversight Committee, which is a key stakeholder in this task, must have a prior, thorough understanding of the Mehari risk model.

#### ***Participants and stakeholders***

The organizer of this task is the person responsible of the risk analysis and treatment operation.

Stakeholders are:

- the Oversight Committee for the operation,
- the CISO

#### ***Deliverable***

The deliverable is the series of risk evaluation tables.

#### ***Process – implementation guidelines***

The process involves the following:

- Drafting of tables (3 to evaluate residual potentiality and 4 to evaluate residual impact).
- Approval by Oversight Committee

Note: these drafts can use the basic tables presented in the Mehari knowledge base and provided as an example in “*Mehari 2010: Risk analysis and treatment guide*”.

Approval by the Oversight Committee is recommended.

## **2. Risk analysis – operational phase**

The risk analysis phase itself includes three main steps.

These are:

- 2.1 Stakes analysis and asset classification
  - 2.1.1 Malfunction value scale
  - 2.1.2 Asset classification
  - 2.1.3 Intrinsic impact table
- 2.2 Assessment of security services quality
  - 2.2.1 Establishing an audit schema
  - 2.2.2 Assessing security services quality
- 2.3 Risk assessment
  - 2.3.1 Selecting risk scenarios for analysis
  - 2.3.2 Assessing risk scenarios



## ***2.1 Stakes analysis and asset classification***

### ***2.1.1 Malfunction value scale***

#### ***Objectives***

To formally establish the security stakes for each of the entity's activities, to be used afterwards for classifying assets.

The purpose and objectives of the malfunction value scale are described in "*Mebari 2010 - Stakes Analysis and Classification guide*".

For each activity, the malfunction value scale is used to highlight:

- Dreaded malfunctions,
- Qualitative or quantitative criteria for evaluating the seriousness of these malfunctions on a scale of one to four.

#### ***Prerequisites***

To begin this task, it is important to have established a work order for the stakes analysis operation.

It is recommended that this task be preceded by an initial meeting to identify the procedure and the expectations of management.

#### ***Participants and stakeholders***

The organizer of this task is the person responsible of the risk analysis and treatment operation.

Stakeholders are:

- Activity managers,
- General management,
- the CISO.

#### ***Deliverable***

The deliverable is the malfunction value scale for the entity.

#### ***Process – implementation guidelines***

Described at length in the "*Security Stakes Analysis and Classification guide*", the process involves the following:

- An initial meeting,
- Meetings with activity managers to highlight potential malfunctions and criteria for evaluating how serious they are,
- Summary for each activity,
- Overall summary for the entity,
- Approval by Management Committee or directly by General Management.

## **2.1.2 Asset classification**

### **Objectives**

To classify each set of assets based on how sensitive they are.

The asset sets used in the MEHARI 2010 knowledge base are activity-related categories of primary assets, as defined in “*Mebari 2010 – Fundamental concepts and functional specifications*”.

Assets should be classified according to Availability, Integrity and Confidentiality.

Classification is used to complete classification tables – T1, T2 and T3 – as indicated in “*Mebari 2010 - Security Stakes Analysis and Classification*”. Each cell in the T1 and T2 tables should indicate the highest level of seriousness inherent in a type of damage (unavailability, loss of integrity or confidentiality) for each type of asset and activity involved (specified in each line of the table).

T3 cells indicate the required level of efficiency of the management processes regarding compliance to laws and regulations.

### **Prerequisites**

It is strongly recommended, if not essential, that the malfunction value scale be established beforehand. Directly classifying assets can skew the risk analysis process.

### **Participants and stakeholders**

The organizer of this task is the person responsible of the risk analysis and treatment operation.

Stakeholders are:

- Activity managers,
- The CIO,
- The CISO.

### **Deliverables**

The deliverables are the T1 to T3 classification tables.

### **Process – implementation guidelines**

The process, which is described in the “*stakes analysis and classification guide*”, includes the following:

- Finalizing of the T1 to T3 tables by indicating the lines that correspond to the various fields of activity included in the malfunction value scale.
- Filling in of the tables by field of activity and cell by cell:
  - Each cell in the table indicates a type of damage (unavailability, loss of integrity of confidentiality) by asset class (the title of the column) and by activity (listed in each line of the table). It is necessary to determine:
    - Whether this damage can lead to one or several of the malfunctions listed in the malfunction value scale.
    - If it can, what is the highest possible level of seriousness feared? The highest level will be the classification entered into the table cell.
    - If not, a '1' (lowest level of seriousness) may be entered into the table cell.
- Filling in, using the same method, of the line which indicates the management or CIO's overall view (this can indicate a higher level of overall need than the summary of needs for each activity)
- Approval by the Management Committee

### ***2.1.3 Intrinsic impact table***

#### ***Objectives***

To fill in the intrinsic impact table, used afterwards to assess the risk situations of the knowledge base.

The MEHARI knowledge base (see “*MEHARI Risk analysis and treatment guide*”) contains scenarios (over 800 in the 2010 base) that specifically refer to types of assets and their intrinsic impacts.

The intrinsic impact values of the risk scenario knowledge base are contained in the intrinsic impact table.

#### ***Prerequisites***

The T1 to T3 classification tables must be filled in beforehand (see preceding paragraph).

#### ***Participants and stakeholders***

The organizer of this task is the person responsible of the risk analysis and treatment operation, possibly delegated to a member of his/her team.

Stakeholders are:

- Activity managers,
- The legal department,
- The communication department,
- The CISO

#### ***Deliverables***

The deliverable is the intrinsic impact table (see “Classif” tab in the knowledge base).

#### ***Process – implementation guidelines***

The basic option, described below, involves filling in the standard intrinsic impact table. The process involves the following:

- The lines in the first two sections of the intrinsic impact table (service-/data-related assets) correspond to a type of asset and there are three impact values (A, I and C) to fill in. Each value is the highest one possible for each of the columns of either the T1 or T2 table (each column contains a given type of damage for a given type of asset). The automatic calculation feature of Mehari 2010 can be used to automatically fill in the table based on T1 and T2.
- For the last section, which contains only one column, it evaluates the impact of a non-compliance involving each of the listed management processes. This should be done with the activity managers and the assistance of the legal and communication departments.
- Approval by the Management Committee.

## ***2.2 Assessing security service quality***

### ***2.2.1 Establishing the audit schema***

#### ***Objectives***

Security services are features which can involve different types of equipment and implementation strategies within the same company. These differences must therefore be considered parts of the same service, requiring differentiated assessment.

The purpose of this step is to identify the different variants requiring separate assessment.

#### ***Prerequisites***

A clear picture of the technical and organizational context beforehand (steps 1.1.2 and 1.1.3) is needed.

#### ***Participants and stakeholders***

The organizer of this task is the person responsible of the risk analysis and treatment operation, possibly delegated to a member of his/her team.

Stakeholders are:

- the client,
- the general services manager,
- the CIO,
- the CISO

#### ***Deliverables***

The deliverable is an audit schema that lists the different variants per security domain.

#### ***Process – implementation guidelines***

Points to consider and advice on making the audit schema are described in “*Mebari 2010 – Evaluation Guide for Security Services*”.

The process involves the following:

- For each security domain, an analysis of the number of variants needed.
- Approval of the complete audit schema with the person responsible of the risk analysis operation.

## ***2.2.2 Evaluating security service quality***

### ***Objectives***

To conduct a review of the quality level of each variant of the security services. This overall assessment is used to evaluate risk reduction factors during the risk analysis and assessment steps.

### ***Prerequisites***

A clear picture of the technical and structural context beforehand (steps 1.1.2 and 1.1.3) is needed. The audit schema must already be completed.

### ***Participants and stakeholders***

The organizer of this task is the person responsible of the risk analysis and treatment operation.

Stakeholders are:

- Managers in technical departments (general services, IS, networks, telecommunications, user equipment pools, application security, application development, etc.) or managers in administrative departments (legal, organizational, etc.),
- The CIO,
- The CISO

### ***Deliverables***

The deliverable is a set of diagnostic files (one per security domain and per category variant) based on the *Mebari* knowledge base (the 2010 edition contains 14 assessment categories).

These files may be accompanied by summaries for communication purposes (radar views, for example).

### ***Process – implementation guidelines***

Points to consider during the assessment process are provided in “*Mebari 2010 – Evaluation Guide for Security Services*”.

The process involves the following:

- An assessment of each variant of each security domain with the manager in charge
- Any necessary corrections and adjustment with managers from different departments
- Creation of summaries
- Approval by the Management Committee

## **2.3 Risk assessment**

### **2.3.1 Selecting risk scenarios**

#### **Objectives**

To select a series of risk scenarios in order to focus analysis to situations that could be critical.

#### **Prerequisites**

The steps of the preparatory phase and the classification of assets must have been completed beforehand.

#### **Participants and stakeholders**

The organizer of this task is the person responsible of the risk analysis and treatment operation.

Stakeholders are:

- Activity managers
- the CISO

#### **Deliverables**

The deliverable is a summary of the options selected and a list of scenarios to be analyzed in detail (in practice, this involves filling in the "selection" column of the "Scenarios" spreadsheet in the MEHARI 2010 knowledge base.)

#### **Process – implementation guidelines**

Guidelines for selecting the scenarios can be found in “*Mehari 2010 - Risk analysis and treatment guide*”.

The process involves the following:

- Determining a selection strategy:
  - Scenarios with an intrinsic impact over a certain limit (3, for example)
  - Scenarios with a level of intrinsic seriousness over a certain limit (idem)
  - Scenarios which affect specific types of assets
- Approval by the Management Committee
- Effective selection of scenarios in the base

### **2.3.2 Risk assessment**

#### **Objectives**

To review how serious the selected risk scenarios are, in relation to the state of security services quality and the risk reduction factors that result.

#### **Prerequisites**

All preceding steps described above must have been completed beforehand.

#### **Participants and stakeholders**

The organizer of this task is the person responsible of the risk analysis and treatment operation.

The stakeholder is:

- the CISO

#### **Deliverables**

The main deliverable is the completed Mehari knowledge base, which has been filled in and finalized.

This base contains summaries organized by asset type and incident type

Additional presentations can be included, such as cartography of risks, for example (in an I, P plan), or any other type of summary.

#### **Process – implementation guidelines**

Guidelines for estimating risks are provided in “*Mehari 2010 - Risk analysis and treatment guide*”.

The process involves the following:

- Incorporating the results of the security service quality assessment (if they have not been directly entered into the base beforehand).
- Analyzing the scenarios and, if necessary, correcting risk reduction factors if any anomalies are detected.
- Creation of summaries
- Presentation to the Management Committee

### **3. Risk treatment and planning phase**

The risk planning and treatment phase is composed of three main steps.

These are:

- 3.1 Planning of immediate measures
  - 3.1.1 Selection of risks for immediate treatment
  - 3.1.2 Selection of measures for immediate implementation
- 3.2 Planning of context-specific measures
  - 3.2.1 Treatment and priority strategy
  - 3.2.2 Selection of measures and planning
- 3.3 Implementation of risk treatment oversight
  - 3.3.1 Oversight planning
  - 3.3.2 Indicators, dash board and trend chart



## ***3.1 Planning of immediate measures***

### ***3.1.1 Selecting risks for immediate treatment***

#### ***Objectives***

To select high priority risk scenarios to be treated out of the usual decision cycle.

The main selection criterion should be based on the most critical level (level 4), but other criteria can be used.

#### ***Prerequisites***

The steps of the risk analysis phase must have been completed beforehand.

#### ***Participants and stakeholders***

The organizer of this task is the person responsible of the risk analysis and treatment operation.

Stakeholders are:

- Activity and business managers
- the CISO

#### ***Deliverables***

The deliverable is a summary of intolerable risks requiring priority treatment.

#### ***Process – implementation guidelines***

Guidelines for selecting scenarios are provided in “*Mehari 2010 - Risk analysis and treatment guide*”.

The process involves the following:

- Determining a selection strategy:
  - Scenarios which present the highest possible level of intrinsic risk (4)
  - Any other criteria used
- Approval by activity managers
- Effective selection of scenarios in the base

### ***3.1.2 Selecting measures for immediate implementation***

#### ***Objectives***

To offer General Management immediate solutions to reduce risks deemed intolerable. Here, the goal is not necessarily to make residual risks directly tolerable but to move intolerable (level 4) risks to inadmissible (level 3). These might be reduced to level 1 or 2 at a later stage.

#### ***Prerequisites***

The steps of the risk analysis phase must be completed beforehand.

#### ***Participants and stakeholders***

The organizer of this task is the person responsible of the risk analysis and treatment operation.

Stakeholders are:

- Activity managers
- the CISO
- General management

#### ***Deliverables***

The deliverable is a series of action plans: one per intolerable risk to be reduced.

#### ***Process – implementation guidelines***

In the case of highly critical risks, being able to respond quickly is essential.

The process involves the following:

- Determining an action strategy:
  - Avoiding the risk (through structural measures)
  - Reducing the risk (through technical or structural measures)
- Selecting quick measures for implementation.
- Planning and cost budgeting
- Preliminary approval with activity managers
- Approval by Management Committee or by General Management

## ***3.2 Planning of context-specific measures***

### ***3.2.1 Treatment strategy and priority setting***

#### ***Objectives***

To choose between possible treatment strategies and select the criteria for establishing priorities, keeping in mind that it is generally not possible to treat all inadmissible risks simultaneously.

Aside from an initial selection based on the seriousness of the risks (starting with level 3 risks), other considerations can include:

- How quickly additional measures can be implemented (producing quick results and motivating managers)
- Cost effectiveness
- Time effectiveness
- Human resources needed to implement the action plans
- (Positive or negative) impact on users
- The choice of particular themes (continuity of operations, backup, access control, etc.) based on how they raise awareness among users
- Etc.

#### ***Prerequisites***

The steps of the risk analysis phase must be completed beforehand.

#### ***Participants and stakeholders***

The organizer of this task is the person responsible of the risk analysis and treatment operation.

Stakeholders are:

- Activity managers
- the CIO
- the CISO

#### ***Deliverables***

The deliverable is a summary of the treatment strategy and priorities.

#### ***Process – implementation guidelines***

The process involves the following:

- Evaluating the pros and cons of each option
- Preliminary discussions and arbitration with activity managers and stakeholders
- Approval by the Management Committee

### ***3.2.2 Selecting measures and planning***

#### ***Objectives***

To offer the Management Committee action plans (generally multi-year) to reduce or avoid risks deemed inadmissible (level 3).

Here, the goal is not necessarily to treat all inadmissible risks simultaneously but to have an overall and possibly multi-year, plan based on priorities established beforehand.

#### ***Prerequisites***

The steps of the risk analysis phase must have been completed beforehand.

#### ***Participants and stakeholders***

The organizer of this task is the person responsible of the risk analysis and treatment operation.

Stakeholders are:

- Activity managers
- the CIO
- the CISO
- General management

#### ***Deliverables***

The deliverable is a series of action plans, usually grouped together within projects.

#### ***Process – implementation guidelines***

In the case of inadmissible risks, being able to decide which action to take based on the usual decision cycle is essential.

The process involves the following:

- Selecting measures for implementation (several strategies are possible during this process: see “*risk analysis and treatment guide*”).
- Planning and cost budgeting
- Presentation of goals in terms of risks and how they may evolve over time
- Preliminary approval with activity managers and the CIO
- Approval by the Management Committee (based on the usual arbitration cycle)

### ***3.3 Implementation of risk treatment oversight***

#### ***3.3.1 Oversight planning***

##### ***Objectives***

To organize and implement risk treatment monitoring and oversight, and decide upon:

- Oversight Committee members
- the Chair
- a meeting schedule
- Committee tasks

##### ***Prerequisites***

The steps of the preparatory phase must have been completed beforehand.

##### ***Participants and stakeholders***

The organizer of this task is the person responsible of the risk analysis and treatment operation.

Stakeholders are:

- Activity managers
- the CIO
- the CISO

##### ***Deliverables***

The deliverable is a summary of how risk management is steered.

##### ***Process – implementation guidelines***

The process involves the following:

- Proposed organization developed by the task manager and CISO
- Selection of Oversight Committee members
- Approval by the Management Committee

### ***3.3.2 Selecting indicators, dashboards and trend chart***

#### ***Objectives***

To offer the Oversight Committee a series of indicators and a trend chart with which it can:

- Verify the implementation of measures decided and project progress
- Verify how risk levels evolve
- Decide which corrective measures are needed

#### ***Prerequisites***

The tasks and composition of the Overall Committee must have been defined beforehand.

#### ***Participants and stakeholders***

The organizer of this task is the person responsible of the risk analysis and treatment operation.

Stakeholders are:

- Activity managers
- the CIO
- the CISO

#### ***Deliverables***

The deliverable is a draft trend chart and the list of indicators which will be used.

#### ***Process – implementation guidelines***

Indicators must be selected so as to allow for short time monitoring (progress, problems encountered, budget monitoring, etc.) as well as for overall, medium-term and long-term vision (number of risk situations per level of residual risk, multi-year forecasting, etc.)

The process involves the following:

- Selecting indicators
- Developing dashboards and trend chart
- Preliminary approval with activity managers and the CIO
- Approval by the Management Committee

## Annex A

### Correspondence table: Mehari 2010 - ISO/IEC 27001:2005

Objectives:

- Recall the list of activities during Mehari risk assessment process,
- Establish the relation with the activities listed for an ISO 27001 ISMS.

Mehari 2010 Process		ISO/IEC 27001	
N°	Step	§	PDCA
1	Preparatory phase		
1.1	Evaluating context		
1.1.1	Strategic context	4.2.1.b	P
1.1.2	Technical context	4.2.1.a	P
1.1.3	Structural context	4.2.1.c	P
1.2	Scope and boundaries		
1.2.1	Technical perimeter	4.2.1.a	P
1.2.2	Organizational perimeter	4.2.1.a	P
1.2.3	Piloting structure	5.1	
1.3	Establishing the main parameters		
1.3.1	Risk acceptability table	4.2.1.e	P
1.3.2	Natural exposure table	4.2.1.d	P
1.3.3	Risk evaluation tables	4.2.1.e	P
2	Operational phase		
2.1	Stakes analysis and asset classification		
2.1.1	Malfunction value scale	4.2.1.e	P
2.1.2	Asset classification	4.2.1.d	P
2.1.3	Intrinsic impact table	4.2.1.e	P
2.2	Assessment of security services quality		
2.2.1	Establishing an audit schema	Absent	C
2.2.2	Assessing security services quality	4.2.3.e	C
2.3	Risk assessment		
2.3.1	Selecting risk scenarios for analysis	Absent	P
2.3.2	Assessing risk scenarios	4.2.1.d	P
3	Risk treatment and planning phase		
3.1	Planning of immediate measures		
3.1.1	Selection of risks for immediate treatment	Absent	P
3.1.2	Selection for immediate implementation	4.2.1.f, 4.2.1.g	P
3.2	Planning of context-specific measures		
3.2.1	Treatment and priority strategy	4.2.1.f, 4.2.2 partial	P, D
3.2.2	Selection of measures and planning	4.2.1.g, 4.2.1.i, 4.2.2 partial	P, D
3.3	Implementation of risk treatment oversight		
3.3.1	Oversight planning	4.2.3 partial	C
3.3.2	Indicators, dash board and trend chart	4.2.4 partial	A

Note: the ISMS elements regarding documentation (§ 4.3) and management responsibility (§ 5) are considered during the phases of Mehari (e.g. assessment and diagnostic of security services).



THE SPIRIT OF EXCHANGE

## CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11, rue de Mogador

75009 Paris

☎ + 33 1 53 25 08 80

clusif@clusif.asso.fr

*Download CLUSIF productions at:*

**[www.clusif.asso.fr](http://www.clusif.asso.fr)**