



MEHARI 2007

Overview



Methods Commission

Mehari is a trademark registered by the Clusif

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

30, rue Pierre Semard, 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>

Acknowledgements

The CLUSIF would like to thank Jean-Philippe Jouas and Jean-Louis Roule, authors of this overview of the MEHARI security management methodology, who have allowed its publication by the CLUSIF.

Please send your questions or comments to: mehari@clusif.asso.fr

Contents

1.	Introduction.....	3
2.	Uses of Mehari.....	5
2.1.	Security assessments.....	5
2.1.1	The vulnerability review, an element of risk analysis.....	6
2.1.2	Security plans based on vulnerability reviews.....	6
2.1.3	Support provided by the knowledge bases in creating a security reference framework.....	6
2.1.4	Domains covered by the assessment module.....	7
2.1.5	Overview of the assessment module.....	7
2.2.	Analyzing the stakes.....	7
2.2.1	Analyzing the stakes, the basis for a risk analysis.....	8
2.2.2	The security stakes analysis: the cornerstone of any strategic action planning.....	8
2.2.3	Classification: an element essential to security policy.....	8
2.2.4	Security stakes analysis: the basis of security planning.....	9
2.3.	Risk analysis.....	9
2.3.1	Risk analysis: an aid to strategic planning.....	9
2.3.2	Systematic analysis of risk situations.....	10
2.3.3	Spontaneous analysis of risk situations.....	10
2.3.4	Risk analysis in new projects.....	10
2.4.	General overview of the uses of Mehari.....	10
3.	Mehari and international standards.....	11
3.1.	The respective goals of ISO 17799, ISO/IEC 27001 and MEHARI.....	11
3.1.1	Goals of the ISO/IEC 17799:2005 standard.....	11
3.1.2	Goals of ISO/IEC 27001.....	12
3.1.3	Goals of MEHARI.....	12
3.1.4	Comparison of the goals of MEHARI and the ISO 17799 and ISO/IEC 27001 standards.....	12
3.2.	Compatibility between these approaches.....	13
3.2.1	Compatibility with the ISO 17799 standard.....	13
3.2.2	Compatibility with the ISO 27001 standard.....	13

1. INTRODUCTION

MEHARI was originally designed to assist Chief Information Security Officers (CISOs) in their information system security management tasks. It is in continuous evolution; to meet the evolving nature of the business environment.

This overview is aimed principally at CISOs, but is also intended for auditors or risk managers who share largely the same or similar challenges.

The main aim of this document is to briefly describe how MEHARI can be used. A more detailed description of the methodology and associated tools is provided in other documents available from the Clusif, in particular:

- *MEHARI: Concepts and Mechanisms,*
- *MEHARI: Stakes analysis and classification Guide*
- *MEHARI: Evaluation Guide for security services*
- *MEHARI: Risk Analysis Guide,*
- MEHARI knowledge bases and Reference manuals (security services and risk scenarios).

MEHARI aims to provide a set of tools specifically designed for security management, which comprises a set of managerial actions, each of which has a specific goal.

Some examples of these are:

- Developing security plans, or strategic plans,
- Implementing security policies or rules, which will be grouped together under the term “security reference framework”,
- Running light or detailed assessments of the state of security,
- Risk evaluation and management
- Ensuring the inclusion of security in the management of development projects,
- Security awareness and training sessions,
- Operational security management and the control/monitoring of committed actions.

These, and similar, managerial actions can be performed either in parallel or in series, by specific groups or by the same group, depending on permanent or specific requirements. Equally, these actions may be performed either independently or as a constituent part of an overall program.

The same managerial actions can be performed in different ways, depending on a number of factors:

- The maturity, in terms of security, of the organization and its staff,
- The level of management implication in information security decision making,
- The enterprise’s culture: hierarchical and technocratic (rules exist and are applied), or, on the contrary, decentralized and empowered.

Given these differences, the major requirement of a methodology is to come with an accompanying set of tools; appropriate to each situation, consistent and complementary among

themselves, allowing movement from one to the other without duplication of tasks or extra workload.

MEHARI provides a consistent methodology, with appropriate knowledge databases, to aid Chief Information Security Officers (CISOs), general managers, and security managers, or other people implicated in risk reduction, in their different tasks and actions.

This document gives an overview of how MEHARI can be used. Applicable international standards, and MEHARI's relationship to them, are briefly described at the end of the document.

2. USES OF MEHARI

MEHARI is above all a method for risk analysis and risk management.

In practice, this means that MEHARI and its associated knowledge bases have been designed for precise risk analysis, when necessary, although without imposing risk analysis as a management policy priority.

In day-to-day terms, security management is a function or activity that evolves over time. Managerial 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, or include the concept of risk, although this is not mandatory. 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.

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 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.

All these tools and modules - briefly described below - comprise tools for security status assessment, a module for analyzing the stakes, and a risk analysis method with supporting tools.

2.1. Security assessments

Two assessment modules exist in the MEHARI set:

- A rapid assessment module¹
- A more detailed assessment module

¹ This module is currently under development.

In each case, the goal is to evaluate the level of security. In practice, the assessment will judge the security services. Clearly, the results will depend on the depth of the assessment: if rapid, less precise; if detailed, more reliable.

The first module should be used for a rapid assessment of the main weaknesses, or “vulnerability review”. The security services that are examined are the same as those for the detailed assessment, or audit, but the questions are aimed at finding out whether the security function has been implemented without validating it for weaknesses. In this sense, any weaknesses identified are certainly weaknesses, but potential strengths may not be strengths.

The detailed assessment module seeks, in detail, the possible weaknesses of each security service individually. It thereby constitutes an expertise base, usable for risk analysis.

The consistency between these two modules allows the first approach to be used as a starting point, and then to iterate in depth at any time, and for any point that might require assurance.

The assessment modules can be used in a variety of ways².

2.1.1 The vulnerability review, an element of risk analysis

MEHARI provides a structured risk analysis method that will be explained later. At this point, it should suffice to know that the risk model takes into account “risk reduction factors”, in the shape of security services.

The detailed assessment will therefore be an important input for risk analysis in ensuring that the security services really fulfill their role - an essential point for the credibility of the risk analysis.

2.1.2 Security plans based on vulnerability reviews

A relatively popular approach is to build action plans directly as a result of the assessment of the state of the security services.

The security management process following this approach is extremely simple: run an assessment and decide to improve all those services that do not have a sufficient quality level.

The use of a preliminary analysis of the security stakes is also planned for, thus providing a link to this module of MEHARI (described later in this document).

The different stages and advice for implementing this form of management are described in the *MEHARI - Evaluation Guide for security services*.

2.1.3 Support provided by the knowledge bases in creating a security reference framework

The detailed assessment module makes use of the security services knowledge base (documented in the *MEHARI - security services reference manual*³). This describes, for each service, what it is for, what it is used against, the mechanisms and solutions supporting the service, and those elements that should be considered when evaluating the quality of the service.

This unique knowledge base can be used directly to create a security reference framework (or security policies) that will contain, and describe, the set of security rules and instructions that the enterprise or organization will follow.

This approach is often used in organizations or enterprises with a number of independent operational units or sites. This would typically be the case for large multinational companies with a number of affiliates; but just as easily applies to medium sized companies with a large number of regional branches or agencies. In such cases, it is effectively difficult to perform numerous assessments or risk analyses.

² Vulnerability reviews are described in the *MEHARI - Evaluation Guide for security services*.

³ The *Security services reference manual* is part of the Mehari knowledge bases.

Building the security reference framework

Assessment questionnaires and, above all, the *security services reference manual* with the additional explanations it provides are a good working basis for security managers to decide what should be applied in their organization.

Managing exceptions from the rules

The creation of a set of rules, through a security reference framework, often comes up against local implementation difficulties; so, waivers and exceptions from the rules must be managed.

Using a coherent knowledge base, with a consistent set of tools and analytical methodology, enables local divergences to be managed. Requests for exceptions can be covered by a specific risk analysis focused on the identified difficulty.

2.1.4 Domains covered by the assessment module

From a risk analysis point of view, in terms of identifying all risk situations and the desire to cover all unacceptable risks, MEHARI is not restricted simply to the IT domain.

The assessment module covers, apart from the information system, the overall organization, and site protection in general, as well as the work environment and legal and regulatory aspects.

2.1.5 Overview of the assessment module

The one thing to bear in mind about the assessment module is that it provides a broad and consistent view of security. This can be used in a variety of approaches, evolutive in depth and granularity of analysis, and can be used at all stages of maturity of the enterprise's security awareness and organization.

2.2. Analyzing the stakes

Security is about protecting assets. Whatever the security policy orientations, there is one principle upon which all managers agree; that there must be a just balance between investments in security on the one hand and the importance of the security stakes themselves.

This means that a proper understanding of the security stakes is fundamental, and that analysis of the security stakes deserves a high priority level and a strict and structured method of evaluation.

The goal of a security stakes analysis is to answer the double question:

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

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

MEHARI provides a stakes analysis module, described in *MEHARI: Stakes analysis and classification*, which produces two types of results:

- A malfunction value scale
- A classification of information and of IT assets

The malfunction value scale

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

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

This set of results constitutes a malfunction value scale.

Classification of information and assets

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

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

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

Expressing security stakes

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

The former is more detailed and provides more information for CISOs. The latter is more global and more useful for awareness campaigns and communication, but is less granular.

2.2.1 Analyzing the stakes, the basis for a risk analysis

Clearly, this module is key in risk analysis. Without a common agreement on the consequences of potential malfunctions, no judgment on risk levels will be possible.

2.2.2 The security stakes analysis: the cornerstone of any strategic action planning

As described in the introduction, analyzing the stakes is very often required for implementing any form of security plan. Effectively, whatever approach is used, at some point, assets will have to be allocated to implement the action plans, and inevitably, the justification for such investment will be questioned.

The assets and funds that will be allocated to security are, as for insurance policies, in direct proportion to the risk. If there is no common agreement on the potential malfunctions, then it is very unlikely that any budgets will be allocated.

2.2.3 Classification: an element essential to security policy

Security reference frameworks, security policies, and the associated approach to security management have already been mentioned in this document.

In practice, companies that manage security through a set of rules are obliged to differentiate, in the rules themselves, between actions to be performed as a function of the sensitivity of the

information being processed. It is usual to refer to a classification of information and IT system assets.

MEHARI's security stakes analysis module provides the means to perform this classification.

2.2.4 Security stakes analysis: the basis of security planning

The very process of security stakes analysis, which obviously requires the contribution of operational managers, very often leads to the need for immediate action.

Experience shows that, when top level operational management have been interviewed, whatever the size of the organization, and they have explained their view and estimation of serious malfunctions, this leads to security needs that they had not previously considered and which require rapid responses.

Action plans can then be directly created, using a light and direct approach based on the combination of two sets of expertise: that of the profession itself, provided by the operational management, and that of security solutions, provided by security experts.

2.3. Risk analysis

Risk analysis is mentioned in nearly every publication concerning security, as being the driving force in security. However, most fail to discuss what methods should be used.

For more than ten years, MEHARI has provided a structured approach to evaluating risk⁴, based on few simple principles.

A risk situation can be characterized by various factors:

- Structural (or organizational) factors, which do not depend on security measures, but on the core activity of the organization, its environment, and its context.
- Risk reduction factors that are a direct function of implemented security measures.

MEHARI enables qualitative and quantitative evaluation of these factors, and assists in evaluating the risk levels as a result.

In fact, the security stakes analysis is used to determine the maximum seriousness level of the consequences of a risk situation. This is typically a structural factor, while the security assessment will be used to evaluate the risk reduction factors.

2.3.1 Risk analysis: an aid to strategic planning

The identification of risk reduction factors, themselves a function of security measures, provides a methodological basis for building a security plan or the strategic master plan. To assist in this, MEHARI provides a structured and organized approach for security planning.

The approach is based on a risk situation knowledge base and automated procedures for the evaluation of risk reduction factors. In support of the approach, a software tool⁵ alleviates the user from having to make calculations, and also provides simulations and optimizations.

This use of MEHARI focuses on global optimization of security measures with a view to risk reduction.

⁴ A detailed description of the risk model is provided in *MEHARI General Concepts and Principal Mechanisms*.

⁵ Risicare, a software tool, trademark of BUC SA

2.3.2 Systematic analysis of risk situations

On the same methodological basis, a slightly different approach is: to identify all potential risk situations, analyze the most critical of them, and identify actions to reduce the risk to an acceptable level. MEHARI, supported by its knowledge bases, provides for this approach.

This use of MEHARI focuses on ensuring that each critical risk situation has been identified and is covered by an action plan.

2.3.3 Spontaneous analysis of risk situations

The same set of tools can be used at any moment in other security management approaches. In the cases already described, where security is managed through audits or security reference frameworks, there will always be specific cases where the rules cannot be applied. Spontaneous risk analysis can be used to decide how best to proceed.

2.3.4 Risk analysis in new projects

The risk analysis model and mechanisms can be used in project management; to plan against risk and decide what measures should be used as a result.

2.4. General overview of the uses of MEHARI

Clearly, the main orientation of MEHARI is risk analysis and reduction. Its knowledge bases, mechanisms and tools were created for that purpose.

Also, in the minds of the designers of the methodology set, the need for a structured method for risk analysis and reduction can be, depending on the organization:

- A permanent working method - the guidelines for a specialized group,
- A working method used in parallel with other security management practices,
- A working method occasionally used to complement regular practices.

With this in mind, MEHARI provides a set of approaches and tools that enable risk analysis to be made when needed.

The MEHARI methodology, comprising the knowledge bases, the manuals and the guides that describe the different modules (stakes, risks, vulnerabilities), is here to assist people implicated in security management (CISOs, risk managers, auditors, CIOs, ..), in their different tasks and actions.

3. MEHARI AND INTERNATIONAL STANDARDS

A question that is often asked is: how does MEHARI correspond to with international standards - in particular ISO 13335, ISO17799⁶ and ISO/IEC 27001⁷.

Here, MEHARI will not be directly compared with the standards and the tools that they have given rise to. The intent is rather to explain how MEHARI fits with ISO standards, in terms of compatibility of goals.

The ISO 13335 standard includes a risk management model referred to by MEHARI, and with which MEHARI is totally compatible. MEHARI provides a method and tools as required by the standard.

The ISO 17799 and ISO/IEC 27001 will be discussed here with respect to MEHARI.

3.1. The respective goals of ISO 17799, ISO/IEC 27001 and MEHARI

3.1.1 Goals of the ISO/IEC 17799:2005 standard

This standard stipulates that an organization should identify its security requirements using three main sources:

- Risk analysis,
- Legal, statutory, regulatory, or contractual requirements,
- The set of principles, goals, and requirements applying to information processing that the organization has developed to support its operations.

Using this as a basis, control points can be chosen and implemented using the list provided in the section “code of practice for information security management” in the standard or come from any other set of control points (§4.2).

NB: in the scope of 17799: 2005, it is stipulated that the standard provides “guidelines and general principles for initiating, implementing, maintaining and improving information security management”, which means that the ISO standard can be seen as a starting point. However, ISO/IEC 27001 stipulates (§1.2) that any exclusion must be justified and that it is acceptable to add control points (Appendix A - A.1).

The ISO 17799 standard provides a compilation of guidelines, which an organization can use. It notes, however, that the list is not exhaustive, and that complementary measures may be required. However, no methodology is recommended for the creation of a complete security management system.

On the other hand, each part of the best practices guide includes introductions and comments on the intended goals, which can be a very useful aid.

NB: The ISO standard also stipulates in its scope that it can be used to “help build confidence in inter-organizational activities”. This is not included by chance, and brings out an essential aspect that the supporters of the standard promote, which is evaluation (even certification), from an information security point of view, of partners and suppliers.

⁶ ISO/IEC 17799:2005(E)

⁷ ISO/IEC 27001-2005

3.1.2 Goals of ISO/IEC 27001

The clear goal of ISO/IEC 27001 is to “provide a model to create and administer a corporate **information security management system (ISMS)**” and to be “used either internally or by third parties, including certification authorities”.

The evaluation and certification goal puts a strong focus on formal aspects (documentation and registration of decisions, declaration of applicability, registers, etc.) and control (reviews, audits, etc.).

It is clear that the basis of the security approach implies that a risk analysis should be run, to examine the risks to which an organization might be exposed, and to select appropriate measures to reduce the risks to an acceptable level (paragraph 4.2.1).

ISO/IEC 27001 stipulates that a risk analysis method should be used, but this is not a part of the standard, and no specific method is proposed, apart from integrating the PDCA (Plan, Do, Check, Act) recursive process of the model as defined for the creation of the ISMS.

Also, the recommendations or *best practices* that can be used to reduce risk are “aligned on those listed in ISO/IEC 17799:2005”, while an associated list of control points is provided in the appendices.

According to ISO/IEC 27001, the basis of **evaluating the security management system** is not so much the knowledge or verification of whether the decisions that have been made are appropriate and adapted to the organization’s needs, but rather to check that, once the decisions have been made, the management system is really such that an auditor or certifier can be sure that the decisions have really been implemented.

3.1.3 Goals of MEHARI

MEHARI is a consistent set of tools and methods for security management, based on risk analysis. The two fundamental aspects of MEHARI: its risk model (qualitative and quantitative) and the risk analysis based security management models have no equivalent components in either ISO/IEC 27001 or ISO 17799.

3.1.4 Comparison of the goals of MEHARI and the ISO 17799 and ISO/IEC 27001 standards

The goals of MEHARI and of the aforementioned ISO standards are radically different.

- MEHARI aims to provide tools and methods that can be used to choose the most appropriate security measures for a given organization. This is absolutely not the stated goal of either the ISO standards.
- The ISO standards provide a set of best practices, which are certainly very useful, but not necessarily appropriate to what is at stake in the organization, and are useful to cover the aspects of maturity in security, information security planning, independent internal units and partners.

The only point in the MEHARI set that can be compared to ISO 17799 (and Appendix A of ISO/IEC 27001) is the *security services reference manual* of MEHARI. This effectively provides detailed elements that can be used to build a security framework. On this point, it is clear that MEHARI’s coverage is broader than that of ISO, and it covers essential aspects of security beyond only that of the information systems.

3.2. Compatibility between these approaches

The MEHARI approach is totally reconcilable with ISO 17799 because, while they do not have the same stated objectives, it is relatively easy to represent results of a MEHARI analysis in terms of ISO 17799 indicators.

MEHARI responds to the need, expressed in both ISO standards, for a risk analysis to define the measures that should be implemented.

3.2.1 Compatibility with the ISO 17799 standard

The standard control points or *best practices* of ISO are mainly general, behavioral or organizational measures, while MEHARI stresses the need for technical measures whose efficiency can be guaranteed. The results, in terms of security management, will be radically different with these two approaches.

Despite these differences, MEHARI 2007 vulnerability review provides correspondence tables to display indicators aligned with the breakdown used in the ISO 17799:2005 standard, usable for those who need to prove their compliance with that standard.

It is worthwhile mentioning here that the MEHARI audit questionnaires were designed and constituted so as to enable operational managers to efficiently run vulnerability reviews and to deduce the capacity of each security service to reduce these risks.

3.2.2 Compatibility with the ISO 27001 standard

MEHARI can be easily integrated into the ISO/IEC 27001 process, notably the 'PLAN' phase (§4.2.1). MEHARI completely covers the description of the tasks that enable the creation of the ISMS bases.

For the 'DO' phase (§4.2.2), which aims to implement and administer the ISMS, MEHARI provides useful starting elements such as the building of plans for risk management, with prioritization directly linked to risk classification, and progress measurements during their use. For the 'CHECK' phase (§4.2.3), MEHARI provides elements that enable the evaluation of residual risks, and improvements made in the security measures. In addition, any changes to the environment (the stakes, threats, solutions and organization) can easily be re-evaluated by targeted audits that use the results of the initial MEHARI audit. Thus, security plans can be revised and evolve over time.

For the 'ACT' phase (§4.2.4), MEHARI implicitly calls on controls and continuous security improvement; thereby ensuring that the risk reduction goals are met. In these three phases, while MEHARI is not at the heart of the processes, it contributes greatly to their execution and ensures their efficiency.