MEHARI 2010

Overview

April 2010

Methods working group

Please post your questions and comments on the forum:
http://mehari.info/

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

30 rue Pierre Sémard, 75009 PARIS
Tel.: +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

ACKNOWLEDGMENTS

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

Jean-Philippe	Jouas	Responsible of Methods commission Responsible for the Work Group Principles, Mechanisms & Knowledge Bases for MEHARI
Jean-Louis	Roule	Responsible for the Work Group MEHARI Documentation
Dominique	Buc	BUC S.A.
Olivier	Corbier	Docapost
Martine	Gagné	HydroQuébec
Moïse	Hazzan	Ministère des Services Gouvernementaux du Québec
Gérard	Molines	Molines Consultants
Chantale	Pineault	AGRM
Luc	Poulin	CRIM
Pierre	Sasseville	Ministère des Services Gouvernementaux du Québec
Claude	Taillon	Ministère de l'Éducation, du Loisir et du Sport du Québec
Marc	Touboul	BULL SA

CONTENTS

1. INTRODUCTION

MEHARI methodology has been originally designed and is continuously updated to assist Chief Information Security Officers (CISOs) in their management of information security tasks.
This overview is aimed principally at them, but is also intended for auditors, CIOs or risk managers who share largely the same or similar challenges.

The main aim of this document is to 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 Functional specifications,
- MEHARI Guides: for
    - stakes analysis and classification,
    - evaluation of security services and
    - risk analysis,
- MEHARI Reference manual of security services,
- MEHARI knowledge base.

MEHARI first objective is to provide a risk assessment and management method, specifically in the domain of information security, compliant to ISO/IEC 27005:2008 requirements and providing the set of tools and elements required for its implementation[1].

Additional objectives are:

To allow a direct and individual analysis of risk situations described by scenarios,

To provide a complete set of tools specifically designed for short, middle and long term security management, adaptable to various maturity levels and types of actions considered.

Indeed, 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.

MEHARI's relationship to ISO/IEC 27000 standards is described at the end of the document.

[1] The tools and associated means, provided by MEHARI in addition to the standard, are described and justified in *MEHARI: Concepts and Functional specifications*

2. USES OF MEHARI

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

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

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

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

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

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

MEHARI is founded on the principle that the tools required at each stage of security development must be consistent. By this, it should be understood that any results generated at one stage must be reusable by other tools later or elsewhere in the organization.

The various tools and modules of the MEHARI methodology set, designed to accompany a direct and individual risk analysis, can be used separately from each other at any step of security development, using different management approaches, and guarantee a consistency of the resulting decisions.

All these tools and modules - briefly described below – compose a consistent risk assessment method with the required supporting tools and modules for analyzing the stakes and auditing the quality of security measures, etc.

2.1. Risk analysis or assessment

Risk analysis is mentioned in nearly every publication concerning security, as being the driving force to express security requirements and this is stated again by ISO/IEC standards. However, most fail to discuss what methods should be used.

For more than 15 years, MEHARI has provided a structured approach to evaluating risk[2], 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.

In fact, the security stakes analysis is necessary 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.

MEHARI enables qualitative and quantitative evaluation of these factors, and assists in evaluating the risk levels as a result. In so doing, MEHARI integrates tools (such as criteria for assessment, formulas, etc.) and knowledge bases (particularly for diagnosing security measures), which are essential complements to the minimum frame proposed by ISO/IEC 27005.

2.1.1 Systematic analysis of risk situations

In order to answer to the question « what are the risks above an organization and are they acceptable or not? », a structured approach is needed to identify all potential risk situations, to analyze individually the most critical of them, and then to identify actions to reduce the risk to an acceptable level.

The approach provided by MEHARI is based on a risk situation knowledge base and automated procedures for the evaluation of factors characterizing each risk and that allow assessing its level. In addition, the method provides assistance for the selection of appropriate treatment plans.

In order to assess the risk, two main options are proposed:

- Either use a set of functions of the knowledge base (for Microsoft Excel or Open Office) allowing to integrate the results of MEHARI modules (e.g. asset classification from the stakes analysis, diagnostics of security). From these functions, it is possible to assess the current level of risks and to propose additional measures for risk reduction.
- Or a software application, (such as RISICARE[3]) which provides a richer user interface and which allows for simulations, visualizations and further optimizations).

[2] A detailed description of the risk model is provided in *MEHARI Fundamental Principles and Functional specifications.*

[3] From BUC S.A. software editor

2.1.2 Spontaneous analysis of risk situations

The same set of tools can be used at any moment in other security management approaches.

In some modes of piloting of security, where risk management is not the main objective and where security is managed through audits or security reference frameworks, there will often be specific cases where the rules cannot be applied. Spontaneous risk analysis can be used to decide how best to proceed.

2.1.3 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.

2.2. Security assessments

MEHARI integrates thorough diagnostic questionnaires of the security controls in place, allowing assessing the quality level of the mechanisms and solutions aimed at reducing risk[4]

2.2.1 The vulnerability review, an element of risk analysis

MEHARI provides a structured risk model which takes into account "risk reduction factors", in the shape of security services.

The resulting vulnerability 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 and dependability of the risk analysis.

An essential strength of MEHARI, is its capability to assess the current level of risk as well as its future level(s) based on an expert knowledge base evaluating the quality level of the security measures, either operating or decided.

2.2.2 Security plans based on vulnerability reviews

A possible 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.

MEHARI diagnostic questionnaires may be used in this approach.

A preliminary analysis of the business stakes should also be planned for, thus providing a link to this module of MEHARI The stakes analysis allows to state required quality levels for the relevant security services and, consequently, to ignore the others as part of the assessment.

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

MEHARI 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

[4] Security controls, or measures, are grouped in sub-services, then services and finally in security domains.

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.

Building the security reference framework

MEHARI assessment questionnaires 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.

2.2.4 Domains covered by the vulnerability 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.

2.2.5 Overview of the assessment module

The one thing to bear in mind about the vulnerability 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.

2.3. 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 relevant business stakes.

This means that a proper understanding of the business 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 though other criteria may be used, such as traceability), 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.

2.3.1 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.

MEHARI presents a rigorous method for the assessment of the stakes and the asset classification, which provides objective and rational deliverables.

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

Obviously, analyzing the stakes is required for implementing any form of security plan. Effectively, whatever approach is used, at some point, means will have to be allocated to implement the action plans, and inevitably, the justification for such investment will be questioned.

The means 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.

2.3.3 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.

2.3.4 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.

2.4. General overview of the uses of MEHARI

Clearly, the main orientation of MEHARI is risk assessment 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 ISO/IEC 27000 STANDARDS

A question that is often asked is: how does MEHARI correspond to with international standards - in particular ISO/IEC 27000 series.

The intent here is to explain how MEHARI fits with ISO 27001, 27002 and 27005 standards, in terms of compatibility and goals.

3.1. The respective goals of ISO/IEC 27001, 27002, 27005 and MEHARI

3.1.1 Goals of the ISO/IEC 27002:2005 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 27002: 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 27002 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.

3.1.2 Goals of ISO/IEC 27001:2005

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 the 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 27002:2005", 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 ISO/IEC 27005:2008

The objectives of this standard are not to constitute a risk management method but, rather, to fix a minimal framework and to describe requirements, for the risk assessment process itself, for the identification of the threats and vulnerabilities allowing to estimate the risks, their level and then to be in a position to select a mode of treatment and associated plans and measurements aimed at evaluating and improving the situation.

The standard states that a risk assessment method must be selected in accordance to these requirements in order to avoid the use of inconsistent or simplistic methods, as compared to the intent of the editors of the standard.

3.1.4 Goals of MEHARI

MEHARI is a consistent set of tools and methodological features for security management and associated measurement, based on an accurate risk analysis. The fundamental aspects of MEHARI:

- its risk model (qualitative and quantitative),
- the consideration of the efficiency of the security measures in place or planned,
- the capability to evaluate and simulate the residual risk levels resulting from additional measures,

are mandatory complements to the requirements of the ISO/IEC 27000 standards and particularly of ISO/IEC 27005.

3.1.5 Comparison of the goals of MEHARI and ISO/IEC 27001 and 27002 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 and to evaluate the residual risks once these measures will be operating. This is not the primary 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 ***security services reference manual*** of MEHARI effectively provides detailed elements that can be used to build a security framework and may be compared to ISO/IEC 27002. 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 27002 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 27002 indicators.

MEHARI responds to the need, expressed in both ISO 27001 and 27002 standards, for a risk analysis to define the measures that should be implemented.

3.2.1 Compatibility with the ISO/IEC 27002:2005 standard

The standard control points or *best practices* of ISO are mainly general, behavioral or organizational measures, while MEHARI, in addition to them, stresses the need for measures whose efficiency can be guaranteed.

Despite these differences, Mehari vulnerability review provides correspondence tables to display indicators aligned with the breakdown used in the ISO 27002:2005 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/IEC 27001 standard

Mehari can be easily integrated into the PDCA (Plan – Do – Check – Act) processes as stated by ISO/IEC 27001, 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.

3.2.3 Compatibility with the ISO/IEC 27005:2008 standard

The framework set by this new standard is fully applicable to the way MEHARI allows to manage risks, for example:

- The processes for risk analysis, assessment and treatment (taken up from ISO 13335),
- The identification of the primary and supporting assets plus the classification levels attached to them, following the stakes analysis,
- The identification of threats including their level (natural exposure), for which MEHARI is more precise for the description of risks scenarios,
- The identification and quantification of the efficiency of security measures (or controls) in the reduction of the vulnerabilities,
- The combination of these elements for the assessment of the seriousness level of risk scenarios, on a scale with 4 levels.
- The ability to select directly the security measures required for the risk reduction plans.

Therefore, MEHARI is not only easily integrated into an ISMS process, as promoted by ISO 27001, but fully complies with ISO 27005 requirements for a risk management method.

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

30, rue Pierre Sémard
75009 Paris
✆ 01 53 25 08 80
clusif@clusif.asso.fr

Download CLUSIF productions at:
www.clusif.asso.fr