PECB

When Recognition Matters

WHITEPAPER

MEHARI

RISK ASSESSMENT WITH MEHARI METHOD

CONTENT

PRINCIPAL AUTHOR
Eric LACHAPELLE, PECB
Bardha AJVAZI, PECB

INTRODUCTION

It is acknowledged that every Chief Information Security Officer (CISO), when taking up a new job task, is usually confronted with the following two challenges:

1. What are the organization's security management goals?
2. What methodologies and tools currently exist to fulfill these security management goals?

The second challenge is commonly the most complicated to deal with, since there are various available options of risk evaluation and tools to choose from.

Based on Figure 1 (displayed aside), unacceptability is presented in a way that permits us understand that the goal of security management is to prevent valuable assets of the organization from being highly vulnerable.

Therefore, among many risk assessment and management methods, MEHARI, otherwise stated as the Method for Harmonized Analysis of Risk, was originally developed by CLUSIF (Club de la Sécurité de l'Information Français), in 1996, with the purpose of assisting executives in managing their information security, IT resources and consequently reducing the related risks. This methodology is also designed to assist in the implementation of ISO/IEC 27005 - Information security risk management standard.

Other than a methodology, MEHARI is also a set of tools that ensures that an appropriate security management solution can be designed, whatever approach is used.

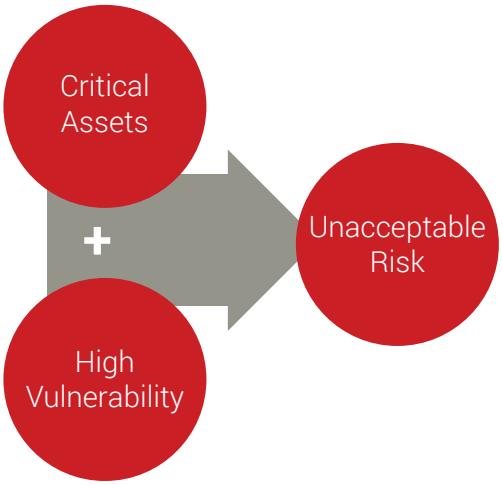


Figure 1: Critical assets + High vulnerability -> Unacceptable risk

MEHARI conforms to the ISO 13335 Risk Management standard and is suitable for the Information Security Management System (ISMS) process elaborated in ISO 27001. In addition, it allows the stakeholder to develop security plans, based on a list of vulnerability control points and an accurate monitoring process to achieve a continual improvement cycle.

Some of the main objectives of the MEHARI methodology are:

- To provide a risk assessment and management method specifically in the domain of information security,
- To provide a set of tools and elements that are required for its successful implementation,
- To allow a direct and individual analysis of risk situations described in various cases, and
- To deliver a complete set of tools particularly for short, middle and long term security management that is compliant to many maturity levels and actions.

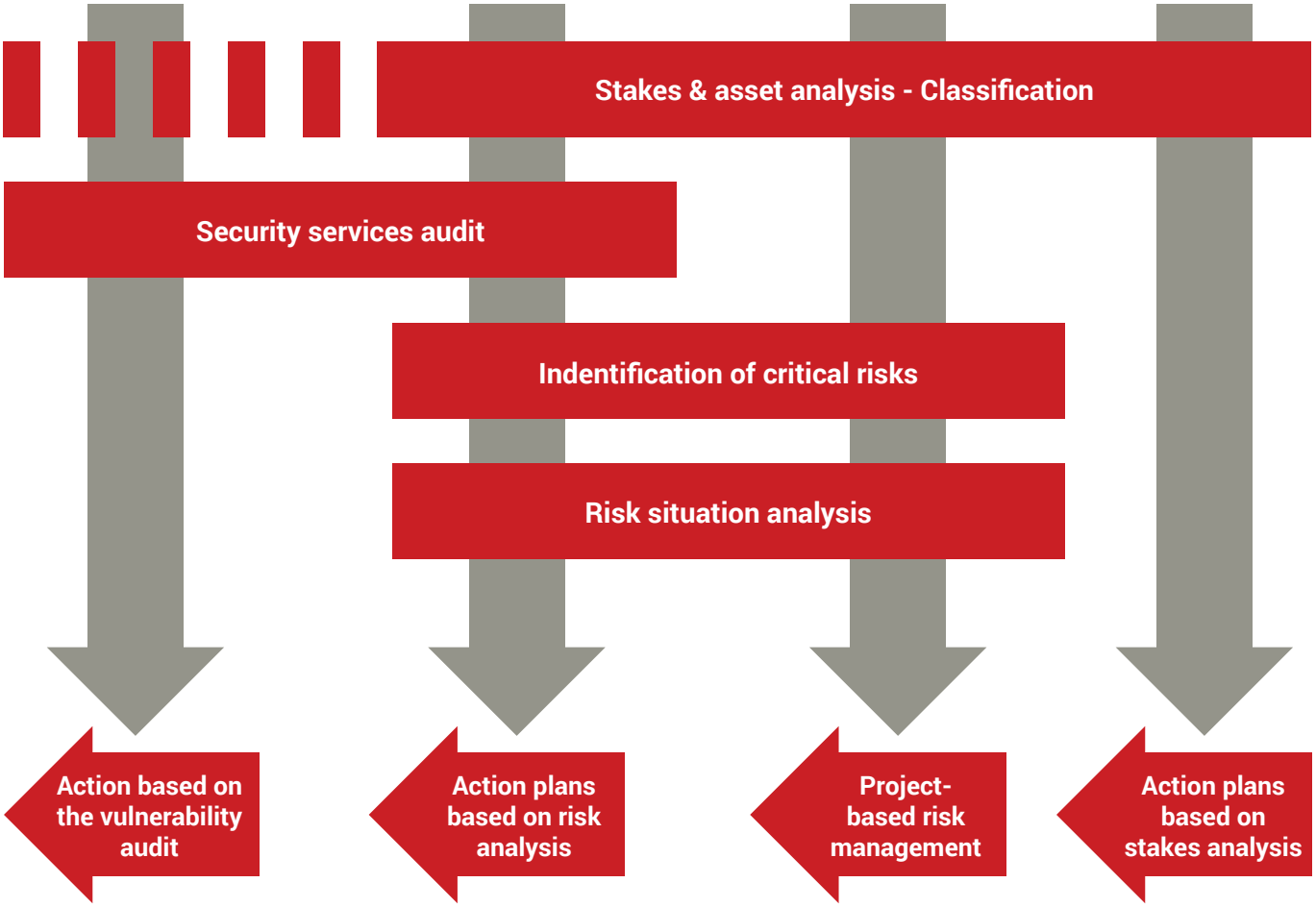
Moreover, the decision to implement security measures in an organization may be at times quite difficult depending on the current situation of that particular organization. However, such decisions should be made using a structured and well thought out approach, such as MEHARI, which addresses the organization's involved risks and assures that their levels are acceptable.

MEHARI is generally beneficial for operating managers, risk managers, auditors, Chief Information Security Officers (CISO) and Chief Information Officers (CIO).

MORE ABOUT MEHARI METHODOLOGY

MEHARI is an efficient way to manage Information Security for all types of organizations, through the provision of a methodological framework (see figure below), which consists of the following phases:

1. Analysis and classification of stakes,
2. Evaluation of security services,
3. Risk analysis, and
4. Definition of security plans.



- PHASE 1: the aim of the stakes analysis is to identify the direct and indirect consequences that may result in a lack of availability, integrity or confidentiality.

  The stakes analysis is critical since it assists in the selection of the implemented measures and prevents expenses where the stakes are less important. It avoids unnecessary constrains and sets priorities.

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

  The stakes analysis has two main outcomes:
  1. The malfunction value scale – reference document that focuses on the impacts of business.
  2. The classification of assets – classification of the information system assets.

- PHASE 2: the purpose of the security services evaluation is to ensure that the identification of weaknesses and defects in security measures are in place.

The key elements of the security services evaluation are:
- The effectiveness of the security services,
- Their firmness, and
- Their stability over time.

In addition, this phase aims at:
- Verifying that there is no unacceptable weak point, or else immediate action plans are established,
- Evaluating the efficiency and reality of the security measures, by using a professional checklist, and
- Comparing the organization to best practices, to evaluate the conformance to a standard and its importance on the level of expertise of the audit base used.

- PHASE 3: the risk analysis of the MEHARI methodology includes the following processes:
  - Identifying situations that may delay expected results,
  - Estimating the probability of such situations, the possible consequences, and criteria to reduce, transfer or preserve the risk, and
  - Bringing upfront the relevant security measures.

Risk
comes from the fact that an entity, company or organization owns "values", material or not, which can sustain damages causing consequences on the entity.

The figure below presents the Risk Model used for the MEHARI methodology.

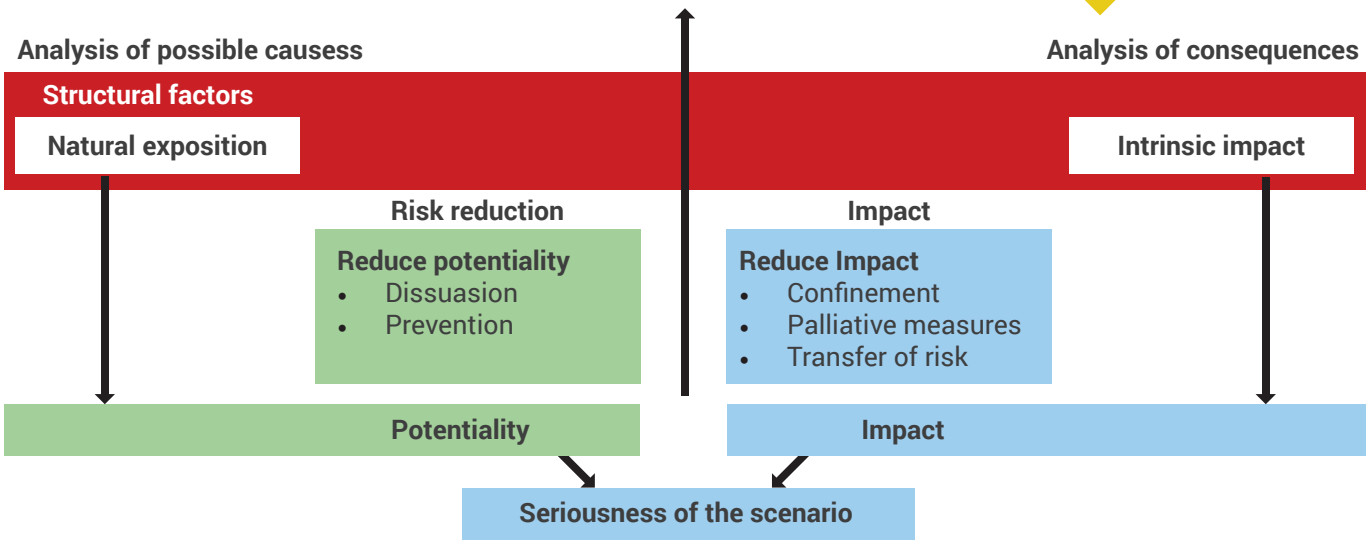


Figure 3: MEHARI Risk Model

- PHASE 4: the definition of risk situations is obviously an important stage for which tools are the most critical sources.

There are two main ways to define and identify risks, by using:
1. **A direct approach**, through the malfunction value scale, and
2. **An organized and systematic approach**, through an automated evaluation using the scenario base provided by MEHARI.

The first approach highlights the scenarios that are closest to the organization's core activities and to the manager's concerns, so they are more relevant to users.

Whereas, it is known that the second approach, using the risk acceptability table (see example aside), is applied more commonly to highlight the scenarios that are of lesser impact but higher potentiality that might otherwise pass as unseen in using the direct approach. Thus, these scenarios could have an unacceptable seriousness (generally 3 and above).

I = 4	S = 3	S = 3	S = 4	S = 4
I = 3	S = 2	S = 3	S = 3	S = 4
I = 2	S = 1	S = 2	S = 3	S = 3
I =1	S = 1	S = 1	S = 1	S = 3
	P = 1	P = 2	P = 3	P = 4

Figure 4: Acceptability table: Seriousness function of Potentiality and Impact

ABOUT MEHARI 2010 BASIC TOOL

The worksheet of the methodology covers several formulas allowing to display step-by-step the results of the Risk Assessment and Risk Management activities and to propose additional controls for risk reduction. This tool is built in Microsoft Excel, as a supporting document following MEHARI methodology, and can be downloaded by clicking on the following link: http://www.clusif.asso.fr/en/production/mehari/download.asp http://www.clusif.asso.fr/en/production/mehari/download.asp

WHY IS PECB A WORTHY CHOICE?

Not like most of the other risk assessment methodologies, MEHARI is fully compatible with all ISO Information Security standards, and contains extensive knowledge base through the Microsoft Excel format. MEHARI is used in combination with dedicated software and spreadsheets.
After completing the PECB MEHARI Risk Manager Training course, the candidate will be able to:

- Develop the necessary skills to conduct a risk assessment with MEHARI method,
- Master the steps to conduct a risk assessment with MEHARI method,
- Understand the concepts, approaches, methods and techniques allowing an effective management of risk according to MEHARI,
- Interpret the requirements of ISO 27001 on Information Security Risk Management, and
- Understand the relationship between the information security risk management, the security controls and the compliance with the other requirements.

HOW TO BECOME A PECB CERTIFIED MEHARI RISK MANAGER?

To ensure that organizations and individuals achieve planned and desired results in information security, the following steps will serve as guidance on how to become certified as a MEHARI Risk Manager through PECB scheme.

1. Participate in the training course,
2. Register for the certification exam,
3. Sit for the certification exam,

4. Apply for the certification scheme upon successful exam completion and fulfillment of application requirements (stated on our website), and finally
5. Obtain the certification.

The PECB "Risk Assessment with MEHARI method" training and exam are both labeled by CLUSIF.

Moreover, after successfully completing the exam, participants can apply for the credentials of MEHARI Provisional Risk Manager or MEHARI Risk Manager, depending on their level of experience.

The table below states the requirements for the corresponding certification schemes:

Credential	Exam	Professional Experience	MEHARI Audit Experience	MEHARI Project Experience	Other Requirements
MEHARI Provisional Risk Manager	MEHARI Risk Manager Exam	None	None	None	Signing the PECB Code of Ethics
MEHARI Risk Manager	MEHARI Risk Manager Exam	**Two years** One year of MEHARI work experience	None	Project activities totaling 200 hours	Signing the PECB Code of Ethics

For further details relating the types of trainings and certifications that PECB offers, please visit our website: www.pecb.com

PECB

+1-844-426-7322

customer@pecb.com

Customer Service