MEHARI functional modules

Information risk management requires coordination between the concerned stakeholders of the enterprise,

MEHARI combines 4 modules in an “application like” frame named knowledge base

1- The stakes analysis and assets classification

The stakes analysis is a mandatory step for any risk management process and constitutes the first module of MEHARI.

The 2 main outputs of the stakes analysis are the establishment of :

- the scale of values of the dysfunctions ;
- the classification of the assets around the information systems, including the intrinsic impact table used by the knowledge bases of MEHARI for the assessment of the risk scenarios.

MEHARI process consists then in an analysis of the activities and thus of the processes of the enterprise or the organization, to deduce the feared dysfunctions, and then to assess how and to which level of seriousness prior to evaluating the classification of the assets contributing to the treatment of information.

The workflow is described in details in the “stakes analysis and classification guide” http://meharipedia.x10host.com/wp/wp-content/uploads/2016/12/MEHARI-2010-Stakes-Analysis-and-Classification-Guide.pdf

2- The diagnostic of the efficiency of the security services

The quality and efficiency of the security measures in place are obviously parameters that cannot be ignored in the assessment of risks faced by the company or organization.

With MEHARI, the security measures are defined within “security services” providing an answer to security requirements, expressed in generic and functional terms the purpose of each service independently of concrete solutions and mechanisms allowing its actual realization.
The security services may have very different levels of performance according to the mechanisms used. They will be more or less efficient in their function and more or less robust in their capacity to resist to a direct attack.

One of the foundations of MEHARI is that it is possible to evaluate this global quality (efficiency and robustness) thanks to adapted questionnaires and to use that result for the quantitative evaluation of the risks.

MEHARI diagnosis module is composed of a series of questionnaires included in each knowledge base [1];

The associated workflow and detailed diagnosis processes are described in the « Evaluation Guide for security services »

1 3 MEHARI knowledge bases are available in French (Expert, Standard and Pro), Expert (the most detailed) has been translated to English and provides complete links with ISO 27002:2013 controls so as to be also integrated into an ISO 27001 ISMS.

http://meharipedia.x10host.com/wp/wp-content/uploads/2016/12/MEHARI-2010-Evaluation-guide.pdf

3- Risk analysis and assessment

MEHARI specific value is to allow a direct and individual management of risks leaned on the following principles:

* Risks can be identified and described by scenarios or situations containing precise elements.

* Each risk scenario can be assessed quantitatively by taking into account:

- The maximal intrinsic impact level of the consequences of the scenario, in the absence of any security measure, thus deduced from the stakes analysis module;
- The intrinsic likelihood of the scenario (aka its natural exposure) reflecting the level of potentiality of its occurrence, in the absence of any security measure, as provided directly in the knowledge bases ;
- Risk reduction factors, differentiated by their type of effect on the impact or the likelihood function on the security measures and their quality level as evaluated from the diagnosis of the module of the security services (above) .

The knowledge bases of MEHARI contain the descriptions of the risk scenarios and the whole of the management processes and algorithms used as explained in the “Risk Analysis and treatment guide”:

http://meharipedia.x10host.com/wp/wp-content/uploads/2016/12/MEHARI-2010-Processing-Guide.pdf

4- The treatment of the risks

The treatment of the risks consists of analyzing each risk scenario and taking specific decisions such as:

* decreasing the residual seriousness through measures for reducing the risk’s likelihood or impact or both;

* avoiding the risk situation through structural or organizational measures;

* transferring or sharing the risk, e.g. via insurance;

* even accepting the risk as it is.

Practically, MEHARI proposes organizing the work in a structured way, starting with the reduction of a maximum of risks to an acceptable level and then analyzing the remaining high risks and selecting risk reduction “action plans” or “projects” as proposed in each knowledge base.

A project or plan is composed of one or several security services, with an objective of quality level for the selected services.