MEHARI 2010

Reference Manual of MEHARI knowledge base

Base Excel : DB-Mehari_2010_Exc_En_2-20.xls
Base OpenOffice (release 3.1 minimum) : DB-Mehari_2010_Ooo_En_2-20.ods

4 April 2011

Methods working group

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
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

1 Foreword

Mehari 2010 workbook is intended to assist the risk audit team in the information risk assessment and management processes, which require a thorough accompanying work, mainly for the business stakes analysis and threat likelihood for the organization.

Also, the risk treatment phase shall be an opportunity to propose options and additional controls or security measures to the stakeholders in a way that corresponds to their demands in the same terms they expressed during the stakes analysis.

It is expected that the risk assessment, instead of being a one shot activity, be a permanent action possibly included into an ISMS process.

The worksheets contained in the workbook distributed by CLUSIF are organized in this order:

- General purpose worksheets:
  - Intro
  - Nav
  - License: Mehari is an Open Source method
- Worksheets relative to the results of the stakes analysis and assets classification:
  - T1, T2 and T3: security requirements of business and transverse processes
  - Classif: recap from the three above worksheets for data, services and management processes
- Worksheets relative to the diagnostic of the security services
  - 01 Org to 14 ISM: worksheets of diagnostic questionnaires
  - Services: a summary of the results from above questionnaires
  - Themes: recapitulation ordered by security theme
  - ISO 27002: results of the diagnostic distributed according to ISO 27001/27002
- Worksheets relative to the risk assessment
  - Expo: evaluation of the "natural exposure" to the list of threats (events)
  - Scenarios: description of the risk scenarios
  - Risk%asset and Risk%event: recapitulations of the seriousness of the scenarios
- Worksheets relative to the preparation of the action plans,
  - Action Plan: Recap of the scenarios by family and of possible action plans
  - Obj_PA: Recapitulation of the security objectives for action plans
  - Obj_Projects: objectives for risk reduction projects
- Worksheets containing permanent elements and parameters of the method
  - Vulnerabilities: lists of vulnerabilities for assets
  - Seriousness: valuation of the seriousness based on impact and potentiality
  - IP_Grids: Impact and Potentiality tables depending on the security measures
  - Codes (masked): used for the description of the scenarios

2 Description of the worksheets

Conventions for this document:

— Normal text is usually descriptive of the worksheet,

— Each possibility to enter data by the risk management team is provided in yellow boxes,

— Additional possibilities, for experienced auditors, are written in red boxes.

2.1 *Naming and protection of the worksheets*

Warning: the name of the worksheets is used in the formulas and macros included in the workbook. Their change would impact the automatic calculations of the method.

Nevertheless, it is possible to add worksheets that may be used during MEHARI risk analysis, e.g. to describe additional elements such as description of the actions, names of the managers and stakeholders, milestones, list of security documents and policies.

Mehari makes no assumption on the name of the workbook itself.

The worksheets are protected, except for the cells that may be used to input the results of the risk study, explanations and comments. By convention, a cell is designed by a couple "(number of the row)<comma>(letter for the column)". Ex. 21,D.

2.2 *Worksheet Intro*

Intro lists the other worksheets of the book and gives a first level of indications on the use of the knowledge base.

It allows also masking the worksheets that are not used during a given phase of the risk analysis (stakes and asset classification, diagnostic, risk treatment, parameters).

Nota: Within certain organizations the use of Office macros is forbidden and the audit team may not be in a position to use this capability. It is still possible, though, to mask/unmask individually the worksheets in a classical way.

Worksheet	Objective			
Intro	Description and pointers within the worksheets of the file. If the security policy of your organisation forbids the use of macros, it will not be possible to use the masks below.			
License	Reminder of the public licence of MEHARI			
Stakes analysis and asset classification module.		Classification tables: T1, T2, T3 & Classif	Mask ➔	☐
T1, T2 and T3	Classification tables			
Classif	Asset classification			
Security services diagnostic module (or Audit)		Questionnaires: from 01Org to 14 ISM + Themes & ISO 27002 scoring	Mask ➔	☐
Domain 01 Org to 14 ISM	Questionnaires relative to MEHARI security domains (01 to 14)			
Services	Recap of the quality of the security services			
Themes	MEHARI security themes			
ISO 27002	ISO 27002 scoring table following the diagnostic of MEHARI security services			
Risk analysis module (identification, assessment and classification of risks)		Risk analysis: Events, scenarios, Risks per asset or event	Mask ➔	☐
Expo	Table of natural likelihood of threats (or natural exposure)			
Scenarios	Table of risk scenarios including formulas for risk assessment			
Risk%Asset	Display of seriousness for the scenarios based on the asset involved			
Risk%event	Display fo the seriousness of scenarios based on the origin or event considered			
Risk treatment : options, risk reduction plans and follow on		Risk treatment: ActionPlans, Obj_PA, Obj_Projects	Mask ➔	☐
Action_plans	Risk reduction plans selected			
Obj_PA	Tab used for the selection of risk reduction plans			
Obj_Projects	Tab used for the selection of risk reduction projects			
Parameters and permanent elements of the method		Grids for risk acceptability, Impact and Likelyhood evaluation	Mask ➔	☐
Vulnerabilities	This tab and the following are provided by the method			
Seriousness	Seriousness Table function on Impact and Likelihood			
IP Grids	Impact and Likelihood tables for the scenarios			

2.3 *Worksheet License*

MEHARI 2010 is distributed under the principles of Open Source as stated in this worksheet.

The use of MEHARI is free but the redistribution and the enhancements of the knowledge base shall mention that the origin is Mehari from CLUSIF.

2.4 *Worksheets T1, T2 and T3*

These worksheets are used to report the results of the stakes analysis and asset classification phase (refer to the corresponding guide) for each asset type and security criterion.

Row 3 indicates the security criteria A (Availability), I (Integrity), C (Confidentiality) or E (Efficiency).

Row 4 contains the code name of the asset designated on row 2.

Row 17 (Classification) is automatically filled by the method with the highest value of the cells above. Depending on the value, the cells are colored in green (2), yellow (3) or red (4).

The cells of rows 5 to 16 shall contain the name of the business processes and their functions (columns A and B) and the classification value (from 1 to 4) of the security criteria, resulting from the stakes analysis, for each of the assets and security criterion applicable.

If more business processes (or domains) need to be reported, it is necessary to remove the protection of the worksheet, insert rows and then reactivate the protection.

2.5 *Worksheet Classif*

It contains synthetic results automatically copied from T1, T2 and T3 "classification" rows for each asset type and criterion.

These values are used later as the (maximum) intrinsic impact for the evaluation of the risk scenarios.

The grey cells mean that there is no security criterion of this type (A, I, C or E) for this asset.

Column F is filled with Ones by default, it is possible to deselect an asset type from the scenarios and the results of the risk analysis by changing the figure to a zero (0). Then, there will be no result for this asset type in the scenarios, Action_Plans, etc. worksheets.

2.6 *Worksheets for the diagnostic of the security services*

These worksheets are organized by domain and numbered from 01 Org to 14 ISM.

They all have the same organization for the columns:

- A: identifier of the services, the sub-services or questions.
- B: designation of the service, sub-service or question
- C (R-V1) to F (R-V4): shall contain the answer to the question for up to 4 variants within the domain as decided in the audit schema. **The number of variants (1 to 4, or void meaning 1) for each security domain shall be indicated in the cell 1,C.**
  The answer for each question may be 1 (Yes), 0 (No) or X (Irrelevant). An empty cell is considered as a 0.
  It is possible to declare a sub-service globally as irrelevant for the analysis by entering an X in the cell attached to the name of the sub-service and the variant (this statement is copied automatically in the Services worksheet), an example for servers may be to audit separately Windows and midframe systems for the domain 08 Sop.
- G to I: Weight, Max and Min parameters used by the method to calculate the level of quality of the service (refer to the *evaluation guide for security services*)
- J: parameter mentioning the type of contribution to the quality of the sub-service and allowing the selection of questions depending for example on the maturity level of the organization. E states for Efficiency, R for Robustness and C for Continuity.
- K: Reference to the section(s) of ISO/IEC 27002:2005 whose "control" is pertinent for the question
- L: dedicated for the collection of comments from the auditor during the diagnostic.

2.7 *Worksheet Services*

The worksheet Services collects automatically the results of the diagnostics allowing measuring the quality of the security services. Each sub-service obtains a quality level, from 0 to 4, for each variant of the audit schema. The worksheet is fully protected.
The organization of the columns for this worksheet is:

- A: number (from 01 to 14) identifying the domain
- B and C: number and description of the security services and sub-services
- D: reference of the security theme to which the service is associated
- E to H: Indicate the quality level (from 0 to 4) of the security services, for the variants, depending on the audit schema.
  This is based on as many diagnostic enquiry sessions of the same service as the number of variants.

As the answers for each variant have been entered in separate columns, the quality level of the sub-services for each potential variant (V1 to V4) is given in these columns.
Irrelevant questions (marked X) do not participate to the weighting, but if answers are partial for a sub-service, or a variant thereof, the level is calculated only for the questions that have received an answer (0 or 1) but the weight of all the questions is still considered.

— I (Min): contains the lowest current value of the service quality for the variants. This minimum is used by the method for the risk assessment (precaution principle).

— J (Obj): contains an automatic copy of the quality objective retained by the action plans or the projects considered in the risk treatment phase (see below worksheets Obj_PA and Obj_projects) as these plans or projects may fix a higher target value for the security services.
Same here, if a sub-service is considered by several improvement decisions, the highest value will be copied in the corresponding cell.
The cell 2,J, is automatically filled with "1" if the decision to consider the target values is introduced in the worksheet "Action_Plans".

— K (Fin): this column is used for simulating the residual risks.
Depending on the option retained, the column will display either the current quality of the sub-service or the objective set for it (more exactly the maximum value of the current and objective values).

2.8 *Worksheet Themes*

This worksheet lists several "security themes" and, for each theme, the services and sub-services of MEHARI that should be considered for the assessment of the "quality" for this theme. The worksheet is fully protected.
Depending on the value of the parameter setting the consideration of the objectives (in the Action_Plans worksheet), the results (from 0 to 4), are given, using the average value of the mentioned services, either with the current value (following the results of the diagnostic of the security services) or the future values (taking into account the expected objectives).

2.9 *Worksheet ISO 27002*

This worksheet permits evaluating a "scoring" value (from 0 o 10) of the completion of the controls listed by the ISO/IEC 27002:2005 standard based on the "Yes" answers to the questionnaires of MEHARI.
The value, in Column F, represents the number of positive answers divided by the total number of questions and multiplied by 10. The worksheet is fully protected.

The score value is established for the first variant (V1) only.

2.10 *Worksheet Expo*

The worksheet Expo contains the list and description of the originating events (or threats) for the scenarios and the "intrinsic potentiality" of their occurrence for the organization.

The organization of the columns for this worksheet is:

— A to D: description of the threats, grouped by types, and corresponding codes.

— E: natural exposition, "standard" value, from 1 to 4, proposed by CLUSIF,

— F: the organization may decide another natural exposure value for each threat, due to its specific situations and environment. Note that this value is not definitive and may have to be changed over time.

— G: contains the standard value unless a value has been entered in F, then the latter is taken into account.

— H: by default, the method considers all the types of threats (1 in column H) but allows deselecting the scenarios referencing any originating event (threat) by setting the value to 0.

— I: allows commenting the decision for each threat.

2.11 *Worksheet Scenarios*

The worksheet Scenarios is the cornerstone of the risk assessment and management and describes all the risk scenarios of the knowledge base.

The organization of the columns for this worksheet is:

— A: code of each family of scenarios, it is composed of the primary asset code followed by the security criterion (A, I, C or E). The same codes are also used as entries in the Action- Plans worksheet.

— B: specific code used for the description of the scenario.

— C: Code for the primary asset type considered (see Classif).

— D to G: Elements of the vulnerability exploited such as criterion (AICE), secondary asset, type of damage and code representing the vulnerability or requirement of compliance.

— H to N: Elements of the threat originating the risk, such as a type and sub-type of event, the circumstances (place, time, type of access and of process) and the type of actor.
All these elements are detailed in the worksheet codes.

— O: description of the scenario. Note that it is based on a formula taking into a sentence all the previous elements (apologies for sometimes in an uneasy form dictated by the automatic translation).

— P: Direct selection of the scenarios to be considered (1) or not (0) by the risk analysis may be decided by the auditor.
This column is filled with ones by default; so all scenarios are evaluated and taken into account in the final risk results and plans.

— Q (Type AEM) and R (Type AICE): display the codes allowing differentiating the cause of the scenario (A for accident, E for Error, M for Malevolence, V for voluntary action, but not necessarily malevolent) and the criterion consequently attained (A for Availability, I for Integrity, C for Confidentiality, E for Efficiency of the management process). These indications are used by the formulas of the knowledge base in its automatic operations.

— S (Impact) and T (Exposure): are the automatic carry forward of the intrinsic impact (from columns C and D) and natural exposure (intrinsic likelihood from columns H and I) of the scenario.

— U (Seriousness): value (from 1 to 4) of the intrinsic seriousness of the scenario, determined, without consideration of the possible risk reduction factors, by the Seriousness

worksheet.

— V to Y (Dissuasion, Prevention, Confining, Palliation): valuation of the risk reduction elements based on the quality level of the security services associated to the scenario. Note that the lowest value of the possible variants is taken into account for the valuation of the risk reduction elements.

— Z (Capacity to confine (or confinability)): If a cell of this column is set to 1, this means that confining measures, referenced in the column AJ, are used to reduce the impact (established with a maximum value of the damage).
If the value is 0 (or the cell is void), the confining measures for the scenario are not selected. This allows considering the consequences of not being able to detect and limit the expansion of the attack or event.

— AA (Impact) and AB (likelihood): decided values for Impact and Likelihood (Potentiality). This allows checking directly the consequences of a value different from the ones resulting from the stakes analysis and set in Expo (Natural Exposure) classifications.

— AC and AD *(Impact and Likelihood*): I and P calculated values for the scenario, based on the intrinsic impact, natural exposure and risk reduction elements (security services).

— AE (*Seriousness*): level of the seriousness resulting from the values of I and P (columns AB and AC) introduced into the grid of the seriousness worksheet.

Note: it is possible to decide dynamically in the Action_Plans worksheet (cells N,1 and N,2) to edit here either the intrinsic, current or expected (at a given date) seriousness value.

— AF (*Accept or Transfer*): by entering A or T, it is possible to mention that the scenario is accepted (despite its level) or that a transfer (using insurance for example) decision is taken. Then the scenario is not ranked among those needing treatment in the Action_Plans, Risk%asset and Risk%event worksheets.

— AG: the cell is a copy of the seriousness value (column AE) or is empty if the scenario is accepted or transferred (in column AF).

— AH to AK: contain the reference to the security services used by the method for the assessment of risk reduction.

— AL to AS: locked columns used as working areas by the method.

2.12 ***Worksheet Risk%asset***

This worksheet contains a summary statement for each type of asset of the number of scenarios, ordered by security criterion (A, I, C or E) and seriousness level (from 1 to 4).

This synthetic view allows to work directly, in the action plans worksheet on the corresponding family of scenarios through the hypertext links provided by the “>” sign.

The worksheet is fully protected.

2.13 ***Worksheet Risk%event***

This worksheet contains a summary statement for each type of event (threat) of the number of scenarios, ordered by seriousness level (from 1 to 4).

The worksheet is fully protected.

2.14 *Worksheet Action_Plans*

This worksheet contains information about the action plans allowing a reduction of the risk level for a family of scenarios, a family applies to a type of primary asset and a security criteria.

At the top of the worksheet, it is possible to select dynamically one display option:

- Indicate the intrinsic seriousness of the scenarios, that is prior to considering any possible security controls in place (using 0 both in cells 1,N and 2,N),
- Indicate the current seriousness level of the scenarios, taking into account the reduction already provided by the controls and the quality level of the security services assessed from the diagnostic (set cell 1,N to 1 and 2,N to 0).
- Anticipated seriousness based on the actions decided, the seriousness displayed takes into account the expected quality levels of the security services (set cell 2,N to 1)

The organization of the columns for this worksheet is:

- A: asset name and security criterion identifying the family name of the scenarios,
- B to F: number of scenarios, ordered by seriousness level, followed by the total number of scenarios.
  If there is no scenario, the cell remains blank otherwise the color refers to the seriousness level.
- G: type of effect provided by the action plan described in the following columns, if it is selected.
- H: indication of the "efficiency" of the action plan, based on the percentage of the scenarios in the family enhanced by the action plan.
- I (Decision): if set to 1, the action plan based on the security services of the row is considered in the expectation of risk reduction, otherwise set to 0 or blank.
  The number of scenarios whose seriousness level is reduced by the security services of the row is automatically updated.
- J, M, P, S, V, Y, AB, AE, AH and AK: services included in the plan.
- K, N, Q, T, W, AC, AF, AI and AL: current value of the quality level of the security service (as established from the diagnostic phase).
- L, O, R, U, AD, AG, AJ and AM: desired (target) quality level for the service, the proposed value may be modified by the auditor willing to check another option.
  If the risk auditor wants to exclude any of the services of a selected row (1 in column I), it is sufficient to set the target level to 1.

Setting of the objective levels for the security services

The pertinent security services for a family of scenarios are listed on several rows by homogeneous sets and by type of effect (dissuasion, prevention, confining, palliation). For each service, the current quality level is put in front of the desired target level for reducing the risk.

The tuning capabilities above allow to simulate the consequences of several options and to decide the most efficient plans.

2.15 *Worksheet Obj_PA*

This worksheet recaps the quality level objectives assigned to the security services by the actions plans selected in Action_Plans.

The organization of the columns for this worksheet is:

— A to C: recap of the columns A to C from the Services worksheet, one row per sub-service.

— D: recap of the target quality level resulting from the action plans selected, it is also copied into the security objectives of the Services worksheet (column J).

— E to BC: the columns are used by the method resulting from the selected action plans.

2.16 *Worksheet Obj_Projects*

This worksheet permits defining up to 40 projects together with the target value of the enhanced security services at the completion date of each project.

The organization of the columns for this worksheet is:

— A to C: recap of the columns A to C from the Services worksheet, one row per sub-service.

— D to H: hidden columns, used by the method for the evaluation of the "needed value for the security service" by the scenarios referencing it.

— I: synthetic value expressing the importance of this need by the scenarios considered (or blank).

— J: Highest quality level expected for this service from the projects completed at or before the **reference date** provided in cell J,4.

— Cell J,4 is used to enter a **reference date**. It may be modified if alternate dates need to be considered during the risk assessment.

— K to AX: The expected quality level for each service mentioned from each project shall be entered in the corresponding cell.
Row 3 of each column is a short description of the project.
Row 4 of each project contains its planned achievement date (yy mm).
Note: if the completion date of a project is void, it is considered by the method as being completed before the reference date.

2.17 *Worksheet Vulnerabilities*

The worksheet Vulnerabilities contains the list, for each type of supporting asset, of the potential damages and vulnerabilities usable by an exploit.

The organization of the columns for this worksheet is:

— A: Asser category.

— B: type of supporting asset.

— C: type of damage.

— D: type of vulnerability.

— E: security criterion or criteria affected.

— F: code name of the vulnerability

— G: by default, it contains "ones" and the scenarios of the method consider the vulnerability.
Note: the risk auditor may set "0" for a vulnerability in order to exclude the scenarios referencing it from the assessment, the scenarios will then show a seriousness level of 0 and not be counted among those listed in the Action_Plan.

2.18 *Worksheet IP_Grids*

The worksheet IP_Grids contains the decision tables used by the method to evaluate the impact and likelihood values based on their intrinsic values and the risk reduction factors in place or anticipated (see "*Mehari 2010 risk analysis and treatment guide*").

The worksheet is fully protected.

It may be possible for experienced users to change the values in the grids once the protection is reset.

2.19 *Worksheet Seriousness*

The worksheet Seriousness contains the standard table, proposed by CLUSIF, establishing the seriousness level of risks as a function of the impact and likelihood. The same table applies for the intrinsic, current and planned values.

The worksheet is fully protected.

The experienced organization may decide other values in the table, if needed and once the protection is reset.

2.20 *Worksheet Codes*

The worksheet Codes is masked, it contains several tables used for the centralized description of the scenarios, mostly for the purpose of facilitating the maintenance and the translation of the base.

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11, rue de Mogador
75009 Paris
✆ 01 53 25 08 80
clusif@clusif.asso.fr

You can download CLUSIF productions from

www.clusif.asso.fr