MEHARI 2010

Evaluation Guide
for security services

May 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

Contents

Acknowledgments

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

The English translation has been managed by:
Jean-Louis Roule and Jean-Philippe Jouas

1. Introduction

"*MEHARI: Fundamental Concepts and Functional specifications*" document, which presents the fundamental principle of MEHARI 2010, states the requirements for the proper use of a knowledge base of security services including:

- Definition of security services,
- Definition of criteria for the evaluation of quality levels : parameters to be considered and quality levels definition,
- The constitution of the knowledge base itself, including a list of security services and questionnaires allowing assessment of their quality level.
- Definition of a metrology for the assessment of the quality of the security services.

We start with the explanation of the above definitions prior to examining the assessment of security services itself.

2. Definitions

2.1. Security services

A **security service** is an answer to a security need, expressed in general and functional terms, which describes the purpose of the service, usually in reference to certain types of threats.

A security service ensures a security function.

This function is **independent from the actual mechanisms and solutions** used to effectively provide the service.

Example: the "Access control" service, the purpose or function of which, as the name implies, is to control access; in other words, only let authorized people 'in'.

2.1.1 Security services and sub-services

The function of a security service can itself require several components, which can be considered 'sub-services'. In the example above, access control requires knowledge of who is authorized, which implies an authorization function, the recognition of a person, which in turn implies an authentication function, and access filtering, which then implies a third filtering function.

A security service can itself be made up of several other security services to meet a specific need or purpose. ***Each component is a security sub-service*** of the service in question, although with respect to an individual function, it retains the characteristics of a service as defined above.

2.1.2 Security mechanisms and solutions

A "**mechanism**" is a particular mean to ensure, totally or partially, a function for a service or sub-service. It may consist of a specific procedure, algorithm, technology, etc.

For the user authentication sub-service (e.g. to an operating system) above mentioned, possible mechanisms may be passwords, tokens, smart cards, biometric systems, etc.

For a given sub-service, several mechanisms are generally possible; whose selection has often a direct consequence on the quality that the sub-service will attain.

A **security solution** is the concrete realization of a security mechanism and may be composed of hardware, software, procedures and operational support, together with the necessary organizational structures required.

2.1.3 Security services typology

Some services may be considered as "general measures" and others as technical services:

- General measures are definitely useful, even mandatory, for information systems security, though their benefit is more effective at the level of the organization, the management of security or awareness rather than on risk situations themselves.
- Technical measures have a clear role, a direct purpose and a direct effect on several risk situations that may be specified.

2.2. Criteria for evaluating security service quality

Security services may vary in performance. They will be more or less efficient in their function, and more or less robust in their ability to resist direct attacks, depending on the mechanisms used and organizational aspects.

2.2.1 Mandatory parameters

To measure security service performance, a number of parameters must be taken into account:

- Efficiency,
- Robustness,
- Permanence.

Security service efficiency

For services of a technical nature, efficiency is a measure of their ability to effectively ensure the required function faced with more or less competent personnel or more or less usual circumstances.

Let us take, as an example, the sub-service "Information system access authorization management", which involves the attribution of users' access rights. The function of this service is to ensure that only those people who have their management's authorization actually get the appropriate information system access. In practice, the efficiency of the service depends on the strictness of the controls on the authenticity of the request, and on the correlation of the hierarchical relationship between the requestor and the new user. If all that is required is a simple mail, without any signature or certificate, anybody who knows a little about the authorization process would be able to unduly allocate themselves access rights, and the quality of the sub-service would be considered poor.

The efficiency of a service that manages human actions is thereby the measure of the competence required to let someone pass through the checks in place, or even to abuse them.

For those services that treat natural events *(such as fire detection, fire extinction.),* the efficiency is a measure of the "strength" of the event for which their intervention remains effective.

If this concerns, for example, a dam that is intended to prevent a river from overflowing due to heavy rains, the efficiency is directly linked to the height of the water (the flood's strength) which it resists to. ***In practice, the strength will often be measured as a function of the exceptional character of the event.***

Services providing general coverage cannot, in principle, be evaluated on the basis of their direct effect, but only on their indirect role.

The efficiency of general measures is the result of their ability to create action plans or significant behavioral changes.

How robust is a security service?

The robustness of a security service measures its ability to resist an action that is intended to short-circuit the service, or to restrict its efficiency.

Robustness only concerns those services that are considered technical.

In the preceding example (access management), the robustness of the sub-service depends – in particular – on how easy it is to directly access the user access rights table, and thereby allow someone to attribute themselves access rights without need to follow the normal control processes.

When we are dealing with services for managing accidents or natural events (such as fire detection, automatic fire extinction, and so on), their robustness will also cover their ability to avoid being short-circuited or bypassed (whether accidentally, or on purpose).

Permanence

The global quality of a security service requires that the service be guaranteed over time.

For this, any service interruption must be detected and palliative measures applied. Everything depends, therefore, on the speed of detection and the capacity to react.

For general measures, surveillance of the solutions themselves is important to show that they can be really measured, in terms of implementation and effectiveness, but also that there are effective quality of service indicators and control points in place.

2.2.2 Definition of quality levels for security services

The quality of a security service measures its efficiency, how robust it is, and the existence of regular controls. Globally, therefore, the quality of a security service is its ability to resist any attack on its defenses – although no castle can be considered to be totally defensible.

Security service quality is scored on a scale between 0 and 4. This scale reflects the competency or determination that is required to break through the defenses, to short-circuit them, or to inhibit or render useless the detection of the service's neutralization.

While this scale of values allows for fractional values, we feel that it is useful to give some indication of the integer values for a security service.

Evaluated service quality level of 1

This service has a minimum level. It could be totally inefficient (or not resist) faced with an ordinary user, without any particular qualification, or slightly learned. In natural events, it is likely to be of no use in day-to-day problems. Generally, it will have little or no effect on the behavior or efficiency of the organization.

Evaluated service quality level of 2

The service is generally efficient and remains resistant to the average or slightly competent hacker. However, it is certainly insufficient when faced with an experienced professional in the specific domain (this could be an IT professional, a well equipped burglar, or an expert in physical break-ins). As far as natural events are concerned, it is rarely sufficient to cover serious events – though these are rare. Generally, such services would only improve day-to-day situations.

Evaluated service quality level of 3

The service is more efficient and resists against attacks and events described above, but could be insufficient against specialized attacks (well equipped and experienced hackers, specialized system engineers, particularly if they have tools or expertise applied to the domain, professional spies, and so on), or really exceptional natural disasters. A generalized solution would have some effect across a large number of circumstances. However, it would certainly not provide any guarantees for very serious problems or attacks.

Evaluated service quality level of 4

This is the highest level, and the security service will remain active and efficient in the face of all aggressions described above. It could however be breached in exceptional circumstances: the world's best code breakers with the world's best code breaking tools (which is possible if some countries want it to happen) or an exceptional combination of exceptional circumstances.

The security service quality evaluation process used by MEHARI was built to provide quality evaluations corresponding to the above definitions.

2.3. MEHARI knowledge base of the security services

MEHARI comprises a knowledge base of security services made up of questionnaires, organized by responsibility domains, for the vulnerability review.

That organization allows limiting the questions asked to each interlocutor met during the review phase.

MEHARI 2010 domains of responsibility cover:

- Organization
- Site security
- Premises security
- Architecture and service continuity of inter-site extended networks
- Architecture and service continuity of local area networks
- Network operation
- Systems architecture and logical security
- IT systems operation
- Application security
- IT projects and development security
- Management of users workstations
- Telecommunications operations
- Management processes
- Information security Management (ISM)

2.4. Security service quality evaluation

The quality evaluation system comprises a set of **questions for which a yes/no answer is required**, with an associated scoring and weighting system that we shall examine later in this document.

Below is an example, taken from the questionnaire, showing questions concerning the "systems architecture" domain.

Audit Questionnaire: Domain: Security of Systems Architecture (07) Service A - Control of access to systems and applications Sub-service A02 : Management of access authorizations and privileges (granting, delegation, revocation)	
Quest. Nr	**Question**
07A02-01	Does the procedure of granting access authorization require the formal approval of line management (at a sufficiently high level)?
07A02-02	Are authorizations granted to named individuals only as a function of their profile?
07A02-03	Is the procedure for granting (or changing or revocation) authorization to an individual (either directly or via his profile) strictly controlled?
07A02-04	Is there a systematic process of updating the table of authorizations at the time of departure of personnel or at the end of contract for external personnel or change of function?
07A02-05	Is there a strictly controlled process (as above) which allows to delegate his/her own authorizations, in part or in whole, to a person of choice for a determined period (in case of absence)?
07A02-06	Is it possible to control at any time, for all users, the rights, authorizations and privileges in force?
07A02-07	Is there a regular audit, at least once a year, of the profiles and authorizations granted to all users and of the procedures for management of attributed profiles?

The questionnaires comprise questions of different kinds. These may be questions oriented towards the efficiency of security measures (e.g.: backup frequency, type of physical access control: card reader, digital code, etc., existence of fire detectors, etc.), questions oriented towards the robustness of security measures (e.g.: where backups are stored, and how access is protected, whether there is a double door, and how well built the doors are, how the fire detection system is protected, etc.). Generally, there are also one or two questions on the monitoring, control and audit of the functions expected of the service.

The weighting system

Questions concerning a security service depend on the useful or necessary security measures of that service. However, not all measures have the same role to play, and a distinction must be made between contributive measures, major or sufficient measures, and essential measures.

2.4.1 Contributive measures

Certain questions have to do with measures that have a certain role in contributing to the quality of service, without their full implementation being necessarily required.

In quantitative terms, a classic weighting applied to these measures reflects this idea of contribution. In this case, certain measures – more important than others – would have a different weighting. The MEHARI knowledge base shows the weighting applied to each question.

The table below enhances the earlier example. In it, V1[1] column is reserved for the answers to the questions (1 for yes, 0 for no); the next column shows the weighting applied to the responses.

[1] At this stage, it is considered that there is only one variant for this domain, as expressed by the value "1" on top of column V1.

Audit Questionnaire: Domain: Security of Systems Architecture (07) A - Control of access to systems and applications A02 Management of access authorizations and privileges (granting, delegation, revocation) 1			
Quest. Nr	**Question**	**V1**	**W**
07A02-01	Does the procedure of granting access authorization require the formal approval of line management (at a sufficiently high level)?	0	4
07A02-02	Are authorizations granted to named individuals only as a function of their profile?	1	2
07A02-03	Is the procedure for granting (or changing or revocation) authorization to an individual (either directly or via his profile) strictly controlled?	1	4
07A02-04	Is there a systematic process of updating the table of authorizations at the time of departure of personnel or at the end of contract for external personnel or change of function?	0	2
07A02-05	Is there a strictly controlled process (as above) which allows to delegate his/her own authorizations, in part or in whole, to a person of choice for a determined period (in case of absence)?	0	4
07A02-06	Is it possible to control at any time, for all users, the rights, authorizations and privileges in force?	1	1
07A02-07	Is there a regular audit, at least once a year, of the profiles and authorizations granted to all users and of the procedures for management of attributed profiles?	0	1

The weighted mean value is simply the sum of the weighted active measures (those whose answer is "1" for "yes"), over the sum of the possible weight, with the result being normalized on a scale of 0 to 4.

So, if $V1_{ii}$ contains the response to question i, W_i is the weighting of i and Mw the weighted mean value:

$$Mw = 4 * \Sigma R_i * W_i \ / \ \Sigma W_i$$

So, for the answers shown in the example questionnaire above, the weighted mean value is:

$Mw = 4 * 7/18 = 1,6$

And the service quality, $Q = Mw = 1,6$

2.4.2 Major or "sufficient" measures

Some measures could be considered sufficient to ensure a certain level of quality of service. For example, a fire detection system can be considered sufficient in providing level 2 for the corresponding sub-service.

We have therefore added a minimum threshold, which is the minimum service quality score if the measure is active.

The column "Min" shows that if a positive answer is given to a question for which a minimum threshold has been fixed, then that threshold has been reached or surpassed by the sub-service.

Another view of the earlier table is shown below, this time with the "Min" column added.

Audit Questionnaire: Domain: Security of Systems Architecture (07) A - Control of access to systems and applications				
A02	**Management of access authorizations and privileges (granting, delegation, revocation)**	**1**		
Quest. Nr	**Question**	**V1**	**W**	**Min**
07A02-01	Does the procedure of granting access authorization require the formal approval of line management (at a sufficiently high level)?	0	4	
07A02-02	Are authorizations granted to named individuals only as a function of their profile?	1	2	
07A02-03	Is the procedure for granting (or changing or revocation) authorization to an individual (either directly or via his profile) strictly controlled?	1	4	3
07A02-04	Is there a systematic process of updating the table of authorizations at the time of departure of personnel or at the end of contract for external personnel or change of function?	0	2	
07A02-05	Is there a strictly controlled process (as above) which allows to delegate his/her own authorizations, in part or in whole, to a person of choice for a determined period (in case of absence)?	0	4	
07A02-06	Is it possible to control at any time, for all users, the rights, authorizations and privileges in force?	1	1	
07A02-07	Is there a regular audit, at least once a year, of the profiles and authorizations granted to all users and of the procedures for management of attributed profiles?	0	1	

In the example, the fact that the process for allocation, modification or removal of rights (question -03) is strictly managed was considered sufficient to increase the quality of service score to the threshold minimum of 3.

2.4.3 Essential measures

On the other hand, certain measures may be considered mandatory in ensuring a certain level of quality of service.

MEHARI associates with the questions concerning those measures considered mandatory in ensuring a certain quality level, a quality threshold. If this threshold is to be surpassed, the implementation of the measure is obligatory.

In other words, the threshold shown in the "Max" column is the maximum quality level that the sub-service can obtain if the measure is not implemented.

When there is clash between the minimum and maximum thresholds, it is the max value that takes priority.

With this addition to the previous table we get the following view:

Audit Questionnaire: Domain: Security of Systems Architecture (07) **A - Control of access to systems and applications**					
A02	**Management of access authorizations and privileges (granting, delegation, revocation)**	**1**			
Quest. Nr	**Question**	**V1**	**W**	**Max**	**Min**
07A02-01	Does the procedure of granting access authorization require the formal approval of line management (at a sufficiently high level)?	0	4	2	
07A02-02	Are authorizations granted to named individuals only as a function of their profile?	1	2		
07A02-03	Is the procedure for granting (or changing or revocation) authorization to an individual (either directly or via his profile) strictly controlled?	1	4	2	3
07A02-04	Is there a systematic process of updating the table of authorizations at the time of departure of personnel or at the end of contract for external personnel or change of function?	0	2		
07A02-05	Is there a strictly controlled process (as above) which allows to delegate his/her own authorizations, in part or in whole, to a person of choice for a determined period (in case of absence)?	0	4		
07A02-06	Is it possible to control at any time, for all users, the rights, authorizations and privileges in force?	1	1		
07A02-07	Is there a regular audit, at least once a year, of the profiles and authorizations granted to all users and of the procedures for management of attributed profiles?	0	1	2	

In the above example, expert opinion says that negative responses to questions 1 and 7 mean that the service quality level cannot be higher than 2. This limit has priority over the level 3 value proposed earlier.

This triple system of quality of service measurement avoids the risk of seeing a series of inefficient measures being given an over-evaluated quality level when the essential measures are not active or, on the contrary, a series of poorly weighted measures under-evaluating the quality of service when an essential measure is implemented. This approach is one of the distinctive features of MEHARI, providing real value based on the expertise of the people who maintain the knowledge bases.

2.4.4 Inapplicable questions

Certain questions can be considered inapplicable for some organizations. In this case, entering a "X" in the answer column will make that question not taken into account in the service evaluation process.

Attention must be paid to ensure that an inapplicable question remains so, whatever the planned evolution of the IT system and the security services.

3. The evaluation process

Before describing the actual evaluation process, a preliminary question must be addressed concerning the services requiring action. Several variants of the same service may exist and this might need to be kept in mind.

3.1. The audit schema

Security services, as defined by MEHARI, are security functions, which are provided by **solutions** implemented in the enterprise or organization.

The vulnerability review entails, in practice, the analysis and audit of solutions and procedures implemented to ensure the security functions.

However, there are generally a number of solutions that ensure a given type of protection.

For example, physical access control to premises is certainly provided by different mechanisms and solutions – and these will be different for access to computer rooms, or other technical centers, such as PABX installations, conference rooms, and major electrical installations.

It is also obvious that logical access control to different systems (mainframes, UNIX, NT, and so on) will be managed in different ways depending on the type and level of sensitivity of the system.

Before even thinking about a process of analysis and evaluation of security services, the CISO or the security auditor should first identify which specific solutions should be analyzed and audited.

In MEHARI this is called the "**audit plan**" or **"audit schema".**

3.1.1 The purpose of an audit schema

In an ideal world, each single security service should be examined, and all of the solutions that provide these services in the organization should be identified, so that they can be individually audited.

This would lead to an unbelievably heavy workload for a result whose level of detail would be largely superfluous. Simplification is, therefore, recommended by grouping similar services so that they can be analyzed as homogeneous sets.

However, it is not generally possible to consider as equivalent all of the solutions implemented in the enterprise. This would be the same as considering that all the buildings and rooms are protected in the same way, that all parts of the IT infrastructure have the same back-up plans, or that all data are stored and backed up in the same way. Obviously, this is not the case.

It is, of course, always possible to group different objects into a single set, that would then be considered as a homogeneous whole. But it should be noted that a cautious vulnerability review may apply the most pessimistic evaluation to all objects of a given set. This would give a very poor overall perception of the whole set.

We have, therefore, to find a middle road. This will allow us to differentiate between several solutions of domains that should be audited separately, and inside of which the security solutions can be considered homogeneous. The definition of these domains is represented by the "audit schema".

3.1.2 Building an audit schema

The MEHARI approach is to consider that the security services are defined and implemented by teams of limited size, with a security policy (whether or not it is explicitly documented) that will make them take homogeneous and consistent decisions, even when technical constraints require solutions that differ in detail.

On this basis, MEHARI's principles are to:

* Distinguish between domains of responsibility where a person can be clearly defined as having **responsibility for a domain that has a consistent security policy**.
* Analyze, inside these domains, whether different people exist that could have different security policies, and thereby define separate sub-domains of responsibility. For example, site managers may have, for the security of their site, policies that are different from those of another site.
* Analyze, in each domain or sub-domain, **the sub-sets that may have different policies for whatever reason (technical or other).**

3.1.3 The responsibility domains of Mehari

The finality of the audit schema is to define specific audits for each domain. The MEHARI audit questionnaires are themselves broken down following this organization. They are organized in this way to optimize the audit process.

The first structural level of the audit schema will therefore reflect this decomposition. Then the auditor will have to decide, for each domain to be covered, how many variations should be defined:

* How many different organizations should be separately audited for the security functions that depend on the organizations?
* How many site managers can have a specific security policy, requiring separate vulnerability reviews?
* How many local managers of premises can have a specific security policy, requiring separate vulnerability reviews?
* Are there a number of local area network managers who should be separately interviewed?
* And so on.

Each time that there is a need to distinguish between entities or responsibilities (for reasons of autonomy, or impossibility to apply consistent policies), sub-domains should be created, and the questionnaires replicated for each of them.

Remark: reversely, in small entities, a same person may manage several responsibility domains or security services. It is then judicious for the auditor to group them in order to simplify the audit.

3.1.4 Subset types that should be customized for security audits

The second level of audit schema decomposition deals with technical strategies, or other reasons that require differentiation, inside each domain, between subsets that could demand specific security policies. The sort of questions that should be posed at this level is:

* How many different types of organization need to be separately audited for the security functions that depend on the organization?
* How many different types of site have a specific security policy, requiring specific

vulnerability reviews (chemical plants, sites with specific defense agreements, that deal with personal, social or tax details, and so on)?

* How many types of premises should be differentiated in the security plan (offices, computer rooms, technical centers, and so on)?
* How many extended inter-site and external networks (internet, for example)?
* How many types of local area networks?
* Etc.

For each domain, you will have to identify how many different variations need to be individually identified and audited.

3.1.5 Creating a detailed audit schema

The audit schema is the result of these two structural components: the responsibility domains on the one hand, and the customized variations on the other.

A corporate global audit schema that is the result of this approach could, typically give a table of the type shown below:

Domain	Sub-domains (examples)	Sub-domain types
Organization	None (no decomposition)	Whole enterprise
Sites	HQ and sales agencies Production sites (managed by the industrial production department)	HQ Sales agencies Production sites
Premises	Offices and other premises run by central works dept. IT, electrical, technical and telecommunications areas.	Areas run by third parties (e.g. electric power connection) Computer rooms Other technical areas
Extended network architecture	None (no decomposition)	Extended inter-site network
Local area network architecture	IT networks Production process networks (managed by the industrial production department)	IT networks Production process networks
Network operation	IT networks Production process networks (managed by the industrial production department)	IT networks Production process networks
Systems	IT systems Production process systems (managed by the industrial production department)	Mainframe(s) Open systems (Unix & NT) Process management systems Process security management systems
IT systems operation	IT systems Production process systems	Mainframe(s) Open systems (Unix & NT)

	(managed by the industrial production department)	Process management systems
Application security	None (no decomposition)	Mainframe applications Open system applications
IT development	Development run by the IT department Specific development done by users	Development run by the IT department Specific development done by users
User workstations management	For office applications For specific applications	HQ Sales outlets Production sites
Management of the telecommunications	None (no decomposition)	
Management processes	None (no decomposition)	
Information Security Management (ISM)	None (no decomposition)	

Such an audit schema allows the definition of a detailed organization for the vulnerability review, and to identify the need for a specific vulnerability review for each of the items listed in the right-hand column. The security auditor can therefore replicate the questionnaire (if questionnaires are being used) in as many copies as there are lines in the corresponding domain.

3.1.6 Building specific audit schemas

It is, of course, possible to build specific audit schemas corresponding to specific needs and which do not cover all domains.

It is possible, for example, to build an audit schema specific to a department or project (from the users' working environment through to the systems and applications used). This would be done by selecting the domains concerned and linking the appropriate subsets with the areas concerned.

It should be noted, however, that if the diagnostic process must be followed by a risk analysis, non-audited components might cause problems during the risk analysis.

3.2. The audit process

3.2.1 The review process in itself

Because the security service audit questionnaires are organized by responsibility domains, once the audit schema is defined, they can be duplicated to cover any variations of the domains to be analyzed. The questions should be answered with the appropriate person or people best qualified for that domain. The same general approach can be used for direct evaluation of security service quality.

It may be that, during the audit, certain sub-services appear not to be applicable for the given organization. The corresponding questionnaires can then be deleted.

Responding by only yes or no on the questionnaires can sometimes create difficulties. Natural

answers might be:

- "Generally, YES, but there are exceptions"
- "In theory, YES, but in practice, I am not sure that it is applied everywhere"
- "YES, partially (X %)"
- "YES, being deployed right now"
- "YES, it is planned, but not yet applied"
- Etc.

Our advice in such circumstances is:

- Always note down any explanations that accompany the answers, and keep them. In the paper questionnaires that are used during audit meetings, a "comments" column for such explanations should be added.
- As the scoring system requires a "yes" or "no" response, the security auditor will have to make a decision. The "safe" route would be to reply "no" to all questions where doubt arises (such as the answers above). Whatever the choice, it is important that the answers do not improperly influence the decisions resulting from the audit. Particularly, they should not hide any imperfections. .
- It should be borne in mind, however, that it could de-motivate staff and harm the credibility of the audit to enter a "no" response for those areas that are clearly being corrected and are under control – especially if they are minor.
- A reasonable approach seems to be to reply "yes" each time the correction process and reaction to lack of measures or implementation is under control, and "no" otherwise.

Note that, for these answers to be acceptable, the audit must be run through a face-to-face meeting between the auditor and the person responsible for the domain being audited, and the questionnaires must be filled in during that meeting. Questionnaires completed by the person being audited without the auditor's presence may totally mask reality and introduce serious errors into the audit and its overall quality.

3.2.2 Scoring and correcting the scoring

For those scores obtained through questionnaires, once they are completed, a scoring for the security services can be made. This will be done using the weighting system in MEHARI , as explained earlier.

The weighting system has been designed and tuned by CLUSIF experts. However, it may be that certain imperfections appear locally. It cannot, effectively, take into account every local or specific case that might be encountered during an audit, nor can it be specifically adapted to every organization.

The auditor should, therefore, prior to drawing his conclusions and presenting the conclusions of the audit, check that the scoring used for each service and sub-service is appropriate, by referring to the definitions of the quality levels obtained.

It is, therefore, mandatory that the auditor should be an experienced security professional.

4. Customizable evaluations

The Mehari questionnaires were designed to be as "expert-based" as possible and to be used for individualized risk management.

This leads to a "precautionary" approach in which the quality of security services may be somewhat underestimated to prevent underestimating a risk that could be critical.

While this attitude is duly cautious, it can be disheartening if it is not used to manage risks but to form an opinion on the level of security.

Furthermore, for entities that are in the beginning stages of security, the questionnaire as a whole can be disproportionate given the state of security already achieved.

For this reason, questionnaires can be limited to more or less key questions.

To this end, every question in Mehari questionnaires is assigned a coefficient that reflects both the type of question and the level of acquired security addressed by the question.

The first part of the coefficient is a letter: E, R or C:

- E indicates a question dealing with the effectiveness of the service,
- R indicates a question dealing with the robustness of the service,
- C indicates a question dealing with placing it under control (permanence).

The second part of the coefficient is a number related to the entity's level of maturity based on which the question is pertinent: 1, 2 or 3 (3 is only used for questions dealing with service effectiveness):

- 1 indicates a basic question which must be answered regardless of how mature the entity is,
- 2 indicates medium-level maturity (a company or organization with advanced security but which still needs to make progress),
- 3 indicates questions that only apply to totally mature entities.

This makes it possible to exclude from the questionnaires any questions relating to control or questions that are of too high a level for a summary analysis.

5. Deliverables

The raw results are either the completed questionnaires, with accompanying comments as described earlier, or the direct evaluation of the security service quality.

Generally, the deliverables are presented through a number of synthetic graphics.

5.1. The security service synthetic graphic

The final vulnerability review is usually presented as a "spider diagram" graphic, with a number of dimensions:

- By security service (showing the different sub-services and their scoring),
- By domain of responsibility (showing the different services that make up the domain and their scoring, obtained through the mean scoring of their component sub-services),
- Globally (showing the different domains and their scoring).

5.2. The "thematic" synthetic graphic

Certain security services, although they appear in different audit domains, are complementary in reaching a global security objective. Therefore, to have a general idea of the quality of back up plans, you will have to combine the results of the network and IT security plans, continuity plans, electrical security plans, and so on.

CLUSIF has defined 16 "themes" that represent major security domains which can be used to build the graphics. These indicators, for which calculations are available in the MEHARI knowledge base, are:

- Security organization (roles and structures),
- Awareness and training on security,
- Physical site security (access control, installation),
- Access control to sensitive areas,
- Protection against various risks (fire, flooding, etc),
- Network architecture security (access control, logical sub-networks, firewalls, service levels, etc),
- Communications confidentiality and integrity management,
- Logical access control (systems, applications, and data),
- Data security,
- Operational procedures,
- IT media management,
- Crisis management and back-up plans,
- Back-ups, their planning, and service restoration plans,
- Maintenance,
- IT project and development security,
- Incident management.

It is worth noting that, during a partial audit, covering one or a number of themes (for example maintenance, or the security of development projects) it is easier to focus the audit on the security services that contribute to the selected themes.

5.3. Compliance measurements related to ISO/IEC 27002:2005 standard

As was explained in "*MEHARI: Fundamental Concepts and Functional specifications*" document, a security review can just as well serve as a means to document the level of good practice recommended by the ISO/IEC 27002:2005 standard.

Effectively, each question in the MEHARI audit process can be seen as an elementary control point that is intended to validate solutions and security processes implemented by the organizational entity.

As the organization of the MEHARI audit brings to light the capacity to reduce risk, at every operational level and with the contribution of operational managers, the structure of the services is not perfectly aligned with the « descriptive » structure of the standard.

Additionally, MEHARI questionnaires contain a number of services and controls that go beyond the recommendations of the standard. A mapping of MEHARI questions onto the practices of the ISO standard has therefore been made.

MEHARI 2007 audit questionnaires facilitate this mapping and a correspondence table (with appropriate formulae) is provided in the knowledge database.

It is thus possible to visualize[2] the operational entity's level of maturity for each control point of the standard (with a score of 0 to 4, for example). This is not MEHARI's primary goal, but this can provide useful information during the certification process or when comparing different organizations.

[2] The RISICARE tool provides this level of visualisation.

6. Practical advice

6.1. Important points to be included in audit schemas

An audit schema sometimes is perceived as complicated. There is no reason for this – it is only a snapshot of the state of different solutions and situations.

A mainframe and a UNIX system are different; and their security systems, just like their operations, are inevitably different. These differences can be ignored or taken into account, depending on circumstances. If the differences are to be brought out, the questionnaires should be duplicated appropriately, and similar questions posed to different groups. If you prefer to ignore the differences, the questions will only be posed once at a global level – ***but this is independent of the audit methodology***.

The audit schema is only a simple means to differentiate the different solution domains during the audit process.

Distinction between solution domains is only a question of choice. A generally good approach to the problem is to consider how many different people will have to be interviewed for the same domain.

Basically, the question is ***"how many different people can have so many different views of the same situation?"***. Because each different view requires a specific interview, and two closely similar views may not justify the time and energy of separate interviews.

6.2. Important points to be covered in the audit process

We have already insisted on the need for questionnaires to be completed during face-to-face interviews, so that comments and so on can be included.

We have also suggested that, where answers are not clearly "yes" or "no", that it is better to take a pessimistic view, while adding the explanations as comments, showing a more positive side.

The MEHARI knowledge bases and, in particular, the audit questionnaires, were designed using the following principle of caution:

The automated procedures of the approach must never allow a risk to be under-evaluated. It is always preferable to have a risk initially over-evaluated, when it can be later reduced, than to have it under-evaluated and not appear in a more detailed analysis.

One of the basic principles is to try to avoid cases where the automated procedures would eliminate a scenario as low risk, when it could be very serious indeed. A number of factors contribute to the under-evaluation of a scenario's seriousness; of which, the over-evaluation of certain security services.

Following this principle, as the results of a security audit could be used to analyze the risks run by an organization in general, the scoring applied to the security services is rather prudent.

The final scoring can sometimes appear severe, when compared to other audit systems. The reader should bear in mind that MEHARI insists that security services must be efficient, robust and permanent, which means subject to regular control. Our final word is that we seek to ensure security assurance through the approach. This is not always the case with other approaches