



MEHARI 2007

Security Stakes Analysis and Classification Guide



Methods Commission

Mehari is a trademark registered by the Clusif

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

30, rue Pierre Semard, 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

1. Introduction	3
2. The malfunction value scale	4
2.1. Identification of main activities and their objectives	4
2.2. Identification of potential malfunctions	5
2.3. Security stakes analysis: evaluating the seriousness of identified malfunctions	7
2.4. Malfunction value scale	9
3. Classification of information and supporting assets	10
3.1. Identifying elements for classification	10
3.2. Classification criteria	13
3.3. The classification process	14
4. Building the Intrinsic Impact table	15
5. Practical Advice	18
5.1. Important points to consider in creating the value scale	18
5.2. Important points during classification	19
5.3. Boundaries for the classification	19
5.4. Action plans	19
Appendix 1: Example of a value scale (industrial enterprise)	21
Appendix 2: Intrinsic Impact Table	25

Acknowledgments

The CLUSIF wishes to thank everybody who has contributed to the creation of this document, and in particular:

Dominique Buc	BUC SA
Jean-Philippe Jouas	INDIVIDUAL
Gérard Molines	MOLINES CONSULTANTS
Jean-Louis Roule	INDIVIDUAL
Olivier Corbier	ORSID

The supervision of the translation effort has been managed by :

Jean-Louis Roule and Jean-Philippe Jouas

Please send your questions or comments to: mehari@clusif.asso.fr

1. Introduction

The need for an analysis of what is at stake for information risk management has been recognized in the “*MEHARI Concepts and Mechanisms*” document.

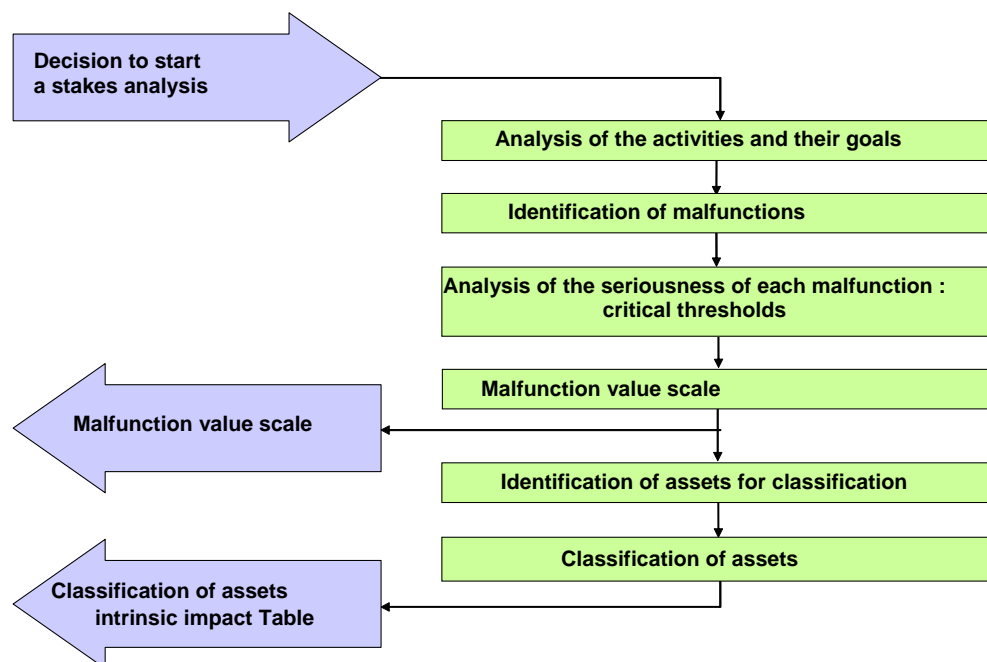
This analysis has to provide two principal sets of results:

- The malfunction value scale,
- The valuation or classification of assets related to information.

From these two sets of results, it is possible to deduce the intrinsic impact table, used for assessing the risk scenarios provided by MEHARI (see “*MEHARI Risk Analysis Guide*”).

The procedure for stakes analysis is described below.

The MEHARI approach consists in analyzing the activities of the enterprise or organization, and therefore its business processes dealing with information, to deduce what malfunctions could occur, and to evaluate how serious these malfunctions could be. Then it is possible to value the assets related to information.



2. The malfunction value scale

This process is designed to provide a scale of values for the malfunctions that may significantly affect the activities of an entity¹.

The analysis comprises four stages:

- The analysis of the main activities and their goals
- The identification of possible malfunctions for each activity, which can be made at the following levels:
 - Technical,
 - Functional.
- An evaluation of the seriousness level of the malfunctions, activity by activity,
- The determination of a global scale of values for the entity.

2.1. Identification of main activities and their objectives

A good starting point is to identify the main activities of the domain being analyzed, to briefly describe them, and to identify their goals or at least the expected results.

2.1.1 Expected results

The activities will be described in functional terms.

In addition to a functional description, it is worth defining the expected results or goals of the activity. These intended results should be defined from the entity's point of view, and that of the "client" entities.

Here is an example:

Function	Goals and expected results
Create and maintain a consolidated view of the treasury and its needs.	Enable accounts department to top up accounts as required (and avoid unsupported payments).

2.1.2 Approach

A rigorous and exhaustive identification of activities can be done through an analysis of the process in which they act. This entails identifying all the processes in the domain under examination, even sub-dividing them into as many sub-processes as are required to bring out the various dependencies and intermediary results.

Experience shows that a global and more intuitive approach, if it has a high enough level of management sponsorship, can quickly identify the main functions and their goals. This is amply sufficient for the needs of this approach.

The approach is based therefore on individual interviews (60 to 90 minutes long) with managers responsible for different activities in the enterprise or organization.

¹ This may be the company itself or an operational entity, for which security objectives are being defined, or for a particular project, where specific risks need to be identified.

2.2. *Identification of potential malfunctions*

Once the activities are identified, the potential or suspected malfunctions associated with them should be brought to light.

2.2.1 *Expected Results*

The description of the malfunctions should be such that the seriousness can be evaluated. However, it should be noted that a malfunction can be described in a number of ways:

- At the level of the element that disturbs or is disturbed in the process being examined. This could be, for example, the unavailability of the treasury management system or the associated database; so, at a technical level.
- At the level of the process itself (at the functional level). For example, the inability to provide a consolidated view of treasury needs.

The same malfunction can thus be described either in terms of the unavailability of data required to produce a specified result, or in terms of the inability to perform the task that would produce the result. The first of these is known in MEHARI as the *technical level analysis of the security stakes*, and the latter is known as the *functional level analysis of the security stakes*.

2.2.1.1 *Potential malfunctions identified at the functional level*

At the functional level, the goal is to identify potential malfunctions that have a significant impact on the enterprise's activities. These will typically be malfunctions in the processes. The following generic profile criteria of a process malfunction will usually apply:

- **Incorrect timing:** the tasks or activities that are planned are not completed in time ;
- **Lack of compliance:** the tasks or activities that are planned are not completed in accordance with the specifications;
- **Lack of completeness:** the tasks or activities that are planned are only partially completed (although the parts that are complete are as specified);
- **Lack of correctness:** additional tasks or activities are performed that were not planned or specified;
- **Lack of discretion:** information is improperly disclosed while the tasks or activities are performed;
- **Lack of Control :** the tasks or activities are performed and completed as planned but without any control or visibility of their execution.

It is, therefore, possible to describe a malfunction in terms of the task or activity that is concerned by the kind of malfunction.

It is also often useful to describe the potential consequences, so as to better apprehend their seriousness.

So, using the hypothetical example of improper disclosure of employees' salaries, it is worth identifying the potential consequences: strike action, obligation to make numerous pay rises for certain categories of personnel, de-motivation of personnel, and so on.

Likewise, if the imagined malfunction concerns changes to pay, it is worth identifying whether the potential consequences involve fraud and the loss of money, or strike action on the part of staff (or their de-motivation), or the need to make numerous and complicated corrections.

Each malfunction, at the functional level, should be described as a change to the

business process. Thus it should be described in terms of the process or activity concerned, as well as by the type of malfunction and the type of potential consequences.

Using the treasury management example, mentioned above:

Function	Goals and expected results
Delay in payment into treasury accounts.	Inability to pay suppliers, implying an interruption of deliveries and thus of production.

2.2.1.2 Potential malfunctions identified at the technical level

At the technical level, the goal is to identify significant malfunctions in the deployment of assets required for the enterprise or organization.

The assets being deployed might be:

- Physical assets:
 - Common assets for any enterprise (office space, office equipment, telephones and faxes, other more specific equipment, etc.);
 - IT assets (servers, workstations, data networks, etc.);
 - Documentary assets in general, and those specific to the task or activity;
 - Communication assets (mail, telephone networks, etc.).
- « Soft » assets:
 - Data (files, databases, reference elements specific to requirements of the activity);
 - Programs (basic software, applications, etc.)
- Human resources and assets:
 - The staff required (competence, delegation and decision, etc.).

The classic types of malfunction are the **loss of availability, of integrity or of confidentiality**.

In the same way as for functional level malfunctions, and for the same reasons, it is also often useful to describe the potential consequences, so as to better apprehend their seriousness.

The technical malfunctions thus identified will be described in terms of the degradation that might occur at the level of the assets used by the process, and of the consequences of such degradation.

Using the previous treasury example, we get:

Malfunction	Consequences
Treasury database unavailable Management of the Treasury database unavailable	Delays in payments to accounts, which implies an inability to pay suppliers, which in turn leads to an interruption of deliveries and of production.

Note:

The example used highlights the duplication of results. A given malfunction can, effectively, be expressed as well at a functional or technical level. However, technical level descriptions can have a number of consequences, and they will be less durable as they depend on the technologies that are used. It is therefore preferable to give priority to the functional level descriptions.

2.2.2 Approach

Here again a very systematic approach could be used, based on a process analysis and imagining all possible « deviations » in the process and sub-processes: incoherent results, delays in (or absence of) results, indiscretion, etc.

Experience shows that an appropriate level of responsibility in the organization will rapidly identify the main malfunctions through a more global approach, which comes down to asking managers what it is that they fear the most or what presents their major worry.

At a functional level, they know the critical processes perfectly well. At a technical level, even if they cannot make an exhaustive list of the applications and databases used, they can certainly describe them globally using generic terms that will suffice (“pay”, for those programs and applications concerned, for example).

The description of malfunctions, whether at a functional or technical level, can thus be constituted through individual interviews, as previously mentioned, with the managers of the various activities in the enterprise or organization.

2.3. Security stakes analysis: evaluating the seriousness of identified malfunctions

The third phase in determining the malfunction value scale aims to ***evaluate the seriousness of the malfunctions previously identified***. To do this, a standard seriousness scale should be used as a reference.

2.3.1 The seriousness scale

MEHARI identifies 4 levels of seriousness or criticality. These are noted from 1 to 4. their general definitions are described below:

Level 4: Vital

At this level, the potential risk is very serious, and even the existence and survival of the entity (or at least one of its main activities) is in danger.

If such a malfunction were to occur, it would concern the entire workforce, and they may feel that their jobs are threatened.

For organizations, such as public services, whose function cannot be questioned, this level of seriousness could well lead to a transfer to another government department, or to the private sector.

For commercial companies, and in financial terms, it is worth considering that such a malfunction would generate losses of such a level that shareholders would pull out (and result in drastic drops in share prices).

In human medicine, this would be the equivalent of an “extremely bad” accident or illness, or where doctors reserve their judgment.

Should the organization survive such a malfunction, there would be serious and durable consequences.

Level 3: Very Serious

These malfunctions are considered very serious at the level of the entity, although its future would not be at risk.

At this seriousness level, all (or, at least, a large part) of the personnel is concerned, in working conditions and social relations, but their jobs are not directly at risk.

In financial terms, this would have a seriously negative impact on the profits for the period, although there would not be a massive pull-out by shareholders.

In terms of public image, this level of malfunction often damages the organization's reputation to such an extent that it would take several months to restore it, even if the financial impact cannot be precisely evaluated.

Accidents that lead to months of organizational disorder for an enterprise would also be evaluated at this level.

Level 2: Serious

Malfunctions at this level would have a clear impact on the entity's operations, results or image, but are globally manageable.

Only a limited part of the staff would be involved in dealing with the consequences of the malfunction, with a significant impact on their working conditions.

Level 1: Not significant

At this level, any resulting damage would have no significant impact on the results or image of the entity, even if some staff members are deeply involved in re-establishing the original status.

2.3.2 Malfunction criteria and criticality thresholds: elementary results

The identified malfunctions do not necessarily have a single and unique seriousness. On the contrary, in many cases the malfunctions need to be characterized by one or more parameters that are key to the seriousness level.

For example, a delay in completion of a process is a malfunction whose seriousness will generally depend on the quantitative lateness and the number of people impacted by the delay.

For each malfunction, the significant parameters should be defined, with the threshold values that move the malfunction from one seriousness level to another.

The criticality criteria and their corresponding thresholds will therefore enable the evaluation of the seriousness of each malfunction, from the malfunction that has minimal impact, to one that is vital to the entity in question.

As an example, and using the earlier case study, the malfunction would produce the following table:

Malfunction	Level 1 Insignificant	Level 2 Serious	Level 3 Very Serious	Level 4 Vital
Inability to keep bank accounts properly provisioned, because treasury databases are unavailable.	Duration : less than 4 hours	Duration : between 4 hours and 2 days	Duration : more than 2 days	

2.3.3 Approach

The identification of malfunction criteria and the evaluation of criticality thresholds will be made during interviews with operational managers in the enterprise. During the same interview (of 60 to 90 minutes duration) the activity will also be defined, as well as the identification of potential malfunctions, and the determination of their criticality as a function of significant parameters.

Elementary results of each interview will therefore consist of a description of these activities, a description of potential malfunctions, and an evaluation of their seriousness level.

2.4. *Malfunction value scale*

A compilation of the various results will then be made for each activity.

A partial example² is shown below, for an HR activity.

Malfunction	Level 1 Insignificant	Level 2 Serious	Level 3 Very Serious	Level 4 Vital
Falsification of pay data, leading to fraud	Loss < 0.1 M€	Loss between 0.1 M€ & 1 M€	Loss between 1 and 10 M€	Loss > 10 M€
Disclosure of personal information	Disclosure of an employee's salary	Disclosure of the salaries of all employees	Repeated disclosure of the salaries of all employees	
Late payment of salaries	Delay < 2 days	Delay between 2 and 15 days	Delay > 15 days	
Destruction of basic data used for paying salaries (calculations & parameters)	Deletion of recent data (during last month)	Deletion of previous year's data	Deletion of all data, and historical traces	

Having thus examined each activity, the compilation of results will provide malfunction value scales for each activity, and at a global, corporate, level of the organization or company.

The resulting value scale is simply a documentary compilation of all the types of malfunction and their critical thresholds, and can be seen as a formalization step. Experience shows that compiling all malfunction types, and their critical thresholds, can show up discrepancies that would not be seen at the level of individual activities.

A consolidation step is therefore required.

In any case, any conclusions or action items that can be deduced from the value scale, or use it, will only be taken seriously if the value scale reflects a true consensus of opinion of the managers of the entity.

It is therefore strongly recommended that there be a real discussion, and that a consensus of opinion be sought concerning the value scale, with management agreement on it.

The final outcome will be a validated malfunction value scale.

A complete example is given in Appendix 1.

² In the example, the values and criteria are only used to illustrate the principle, and should in no case be taken as standards for application in real cases.

3. Classification of information and supporting assets

The malfunction value scale is the main result of a security stakes analysis. It is directly linked to the fundamental activities and processes of the enterprise or organization.

This being said, the risk analysis mechanisms, and certain more systematic approaches used for choosing solutions or building action plans, require that the malfunctions (initially expressed in activity-dependant terms) be reformulated in technical terms relating to the information system, in the broadest sense of the word. Examples are: loss of confidentiality of such and such database, unavailability of a given server, etc.

This reformulation consists in defining the value scale in the form of “classification”.

This complementary formalization consists in:

- Identifying the assets that must be classified (information, information system components, devices, etc.).
- Qualifying each asset as a function of:
 - How it could bring about an identified malfunction
 - The resulting seriousness.

Classification or valuation of information and supporting assets aims to produce "labels" that can be put on each asset so that people who use the asset are informed of its importance in security.

3.1. *Identifying elements to be classified*

All assets could potentially be individually classified, whether information or supporting elements (like site, processing elements, or network and communications ones).

In practice, it is more efficient to group information, objects, or assets having similar roles, and which require the same type and level of protection. So, an application and its associated tools, a set of database tables, etc., will often be grouped together for classification purposes.

Not all of the objects that can be identified in an entity should be individually classified. They should be grouped. It will be these groups of information and assets that will be classified.

Whatever, it is practical and efficient to distinguish between

- The elements and assets that are specifically linked to given processes or activity domains, on the one hand;
- Shared infrastructure elements and common services, used by the various activity domains, on the other.

3.1.1 *Identifying elements linked to business processes*

For those elements and assets that are linked to business processes or activity domains, it is recommended to start with a list of processes or activities (or IT applications). These really should

be united into homogeneous groups, as explained above. For each process, application or activity domain, the assets that need to be classified should be identified.

Usually, the primary assets will be:

- Applications and procedures (ap), i.e.: the source and object code for IT processes. For non-IT processes, this would require a documented description of the procedures ;
- Application data or databases (da) ;
- Data that is transmitted or exchanged between applications (tm);
- Desktop files that are associated with the process or application domain (fb) ;
- Listings and printouts generated by the application (li) ;
- Documents and personal archives kept by people involved in the process (ec) ;
- Mail (electronic or other) concerned with the application process (cf) ;

The various supporting components of the IT architecture are identified so as to indicate whether they are involved in each process or application domain. These components could be:

- Application servers (ASA) ;
- Desktop servers (ASB) ;
- Networks used (either wide-area (WAN), local-area (LAN), public (PUB)) ;
- Any specific equipment used (AED) ;
- Portable PCs and any other mobile equipment (APM) ;

The completed table will look somewhat like the “Business Processes” upper part of the T1 table below³:

Table T1 (Example)		CLASSIFICATION															INFRASTRUCTURE									
Business Processes or activity domains and Common Services	Service types	Application and/or procedures			Application data (databases)			Application data in transit Messages			Associated desktop files			Listings or printouts	Hand written docs or archives		email or postmail Fax			Indicate (by a 1 or a name) that the application, process or application domain, requires the availability of the quoted assets (servers, network, specialized equipment, mobile or portable devices, etc.)						
	Typ	A	I	C	A	I	C	A	I	C	A	I	C	C	A	C	A	I	C	Appl. Serv.	desktop serv.	LAN	WAN	PDN	Spec equipt.	Mobile devices
column name for Classification -->		Aap	Iap	Cap	AAa	IAa	CAa	Atm	Itm	Ctm	Afb	Ifb	Cfb	Cli	Aec	Cec	Acf	Icf	Ccf	ASA	ASB	ARL	ARE	ARP	AED	APM
Business processes																										
Process 1 : HR		2	3	1	2	3	2	2	3	2	1	1	3	2	2	1	1	1	2	1						
Process 2 : Sales management		2	2	4	2	2	4	2	2	4	1	3	3		1	3	3	2	4	1		RLC	1			1
Process 3 : Strategic planning																										
Process 4 : Financial and accounting domain		2	2	3	2	2	3	2	2	3				1						1		1				
Process 5 :		2	3	1	2	3	1	2	3	1	2	3	1								1	1				
Process 6 : CAD/CAM		3	3	3	3	3	3	3	3	3	3	3	3							Ulysse		1				1
Process 7 : commercial website		3	3	1	3	3	1	3	3	1	1	1	1							1		1	1	Internet		1
.../...																										
Process N		2	2	1	2	2	1	2	2	1	2	2	1						1		1	1				
Common Services																										
e-mail	MSG	3	3	1	3	2	1	2	2	2										1		1		Wan		
postal service	COU		3															3	2	1						
Archiving of IT files	ARI	3	3	1	3	3	1	1	1	1	2	1	1													
Document archives	ARD	3	3	1	3	3	1	1	1	1	2	1	1							1		1				
System administration	ADM	2	3	1	2	3	1	1	3	1	1	1	1	3		1	3				1	1				
User help & support	HLP	3	1	1	3	1	1	1	1	1	1	1	1							1		1			1	

Table T1. Classification of assets and supporting components.

It is worth noting that, in this table, the infrastructure components (supporting assets) are mentioned for each process that uses them. The classification applies only to the components specific to the processes of the entity: applications, procedures and various types of data or information. The classification of shared or dedicated infrastructure components used for creating,

³ It is possible to consider other supporting components (working spaces, premises, ...) in additional columns.

processing, transmitting or consulting information can be logically deduced from the classification of dependant functional elements.

It should also be borne in mind that the infrastructure components mentioned in the table can be dedicated (such as application servers) or shared (such as the wide-area network). This table is important because it shows up, during classification, the constraints imposed by the security stakes of each activity on the IT and communication architecture. This, in itself, can lead to a need to define sub-domains for certain activities (or sub-processes), so as to bring out specific infrastructure assets (for example, to highlight the activities that use portable PCs).

The infrastructure components that are used by the various processes should be identified, application by application:

- Either by simply noting that they are used by the application, by a 1 (otherwise empty cell);
- Or by specifying their name: (sub)network name, server name, etc. if it is needed to differentiate elements of the same nature.

3.1.2 Identification of elements linked to common services

It is always possible that certain common services had not been identified as critical elements during the analysis of the business processes. However, they may be critical (to a greater or lesser extent) to the enterprise or organization as a whole.

This would be the case when, for example, they could influence on the IT planning or development strategy, or when they might impact the professional image of the organization or its support services, whether internally or externally.

Below is a non-exhaustive list of what are usually considered as common services:

- Electronic mail (MSG) ;
- Postal services (COU) ;
- Archiving of IT files (ARI) ;
- Archiving of documents (ARD) ;
- System administration for IT and telecommunications (ADM) ;
- User help services (HLP) ;
- etc.

These common services should be identified and classified, just as for the business processes mentioned above. They are included in the lower part of table T1.:

3.1.3 Identifying shared supporting infrastructure to be classified

As far as **dedicated** supporting assets are concerned (those used by application processes to create, process, transmit and consult information) ; their classification can be easily deduced from that of the data and information. So, a server that hosts an application (data or program) will have the same level of classification for a given criterion (availability, for example) as the application being hosted.

As far as shared assets are concerned, the level of classification, for each criterion (A, I, C), is the maximum level induced from all the dependant application processes.

Certain elements of the overall infrastructure should still be identified separately. These are those whose classification will not depend purely on the classification of those processes which use them.

These would be infrastructure assets whose modification would have an influence on IT and

user behavior or corporate image of the organization and its support services (internally or externally). Such infrastructure assets deserve a complementary evaluation of their critical levels. These would typically be:

- local area network(s) (RL) ;
- wide-area network(s) (RE) ;
- telephone network (RT) ;
- application (SV) and shared (SS) servers;
- peripherals (including, for example, printing services, and their print servers) (PF);
- gateways to external services (e.g. Internet) (PA);
- work-space (ET).

These infrastructure assets should be examined specifically, and can then be documented in a new table (T2), with specific columns. An example is shown below:

Table T2 (Example)		CLASSIFICATION									
Infrastructural components	FUNCTION (description) Optional	Infra-struct sub-class	cabling & equip.			configuration files			System program library		
			A	I		A	I	C	A	I	C
Column name for clasification formulae ---->		SCA	Aeq	leq	Afc	lfc	Cfc	Alp	Ilp	Clp	
LANs		RL	2	3	3	3	3	1	2	1	
WANs		RE	2	2	3	3	2	1	2	1	
Telephone network		RT	3	2	2	3	3	1	2	1	
Application servers & data servers		SV	2	2	3	2	1	1	2	1	
IT or network service servers (DNS, LDAP, authentication server, etc.)		SS	2	2	2	3	1	1	3	1	
Peripherals		PF	1	1				1	2	1	
Access gateways		PA	2	2	1	2	1	1	2	1	
Global working environment		ET	2	1							

Table T2: shared infrastructure classification

3.2. Classification criteria

The loss of availability, integrity, or confidentiality⁴ of an asset may have operational and business consequences which need to be evaluated. The tables above need to be filled with a value (from 1 to 4) for each type of asset and criterion.

The consequences of the loss of availability, integrity, or confidentiality for application data are displayed under the columns Ada, Ida, Cda of table T1;

The same applies to associated office data (Afb, Ifb, Cfb);

For print-outs, generally only confidentiality is concerned (Cli). However, for written documents and archives, availability can be added to confidentiality (Aec, Cec).

For applications and programs, it is usually loss of availability or integrity (Aap, Iap) that is the main concern. However, confidentiality (Cap) may also be a concern for certain applications that provide competitive advantage for the entity.

⁴ It is possible to define additional causes of malfunction, and therefore classification criteria. The fourth one being usually: “proof” or “value of proof”.

Mail, whether electronic or not, is rarely considered at the application domain level, except for confidentiality. Availability of the mail server is covered elsewhere, as a part of the common services (line MSG+column ASA of Table T1).

For infrastructure cabling and components, configuration files and program libraries, the main concern is the loss of availability or integrity, except in specific cases (see Table T2).

For configuration files, all three criteria apply.

3.3. The classification process

3.3.1 Classification of assets supporting business processes

For each group of assets supporting business processes or an activity domain, an analysis will be made to determine if a loss of confidentiality could lead to one or more possible malfunction, and, if so, what level of malfunction. If several potential malfunctions could result from a loss of confidentiality for a asset, it is the highest classification level of them (on a scale of 1 to 4) that is retained for the confidentiality criterion.

The same applies for the other criteria (availability and integrity) resulting, for each group of assets identified, in a classification value for each criterion (Availability, Integrity, Confidentiality).

The aim of classification is to thereby define, for the identified asset groups, “labels” that will show the levels of consequences of a loss of availability, integrity or confidentiality for each class of asset.

3.3.2 Classification of elements linked to common services

The same approach applies for common services. It is, however, worth noting that in this case the notion of availability of application data represents rather a global discipline that aims to provide total preservation of data (for example, the entire messages base of the mail service), whereas in the activity part, it is rather a question of availability in terms of required response-time.

For these common services, it may be necessary to return to a stakes analysis approach (as for the malfunction value scale), to evaluate the impact of a change to the services.

3.3.3 Classification of global infrastructure elements

Likewise, for global infrastructure elements, efforts should be concentrated on the overall impact of altering the elements. The particular impact on the business was analyzed by the malfunction value scale and during the creation of table T1.

In particular, the impact of configuration files being unavailable should be evaluated (Table T2), taking into consideration the time that may be required to reconfigure all the components concerned. This may be necessary if there is a general loss of configuration or parameter files, for whatever reason, as a part of a back-up/restore plan, etc. The unavailability of each single configuration file (at the level of an individual activity) being already evaluated at the application process level (which could have a considerably lower impact).

4. Building the Intrinsic Impact table

During the MEHARI risk analysis process, the notion of intrinsic impact of a scenario is introduced. This is the evaluation of the consequences of the occurrence of a risk scenario independently of any security measures (See the “*MEHARI General Concepts and Principal Mechanisms*” document, as well as the “*Risk Analysis Guide*”).

To be more precise, the MEHARI knowledge base refers to an intrinsic impact table, which can be completed with information from the classification tables discussed earlier.

An extract from this table (shown in Appendix 2) is given below:

<i>Intrinsic Impact Table</i>			
<i>Classification of data, information and infrastructure components</i>	A	I	C
Data and information			
D01 Data files or application databases			
D07 Mail and faxes			
.../...			
IT and telecom infrastructure			
R02 LAN equipment and links			
S01 Mainframes, information servers,.....			

The process for completing the intrinsic impact table benefits from the asset classification tables (T1 and T2) that were defined and described in the previous section.

Overall, the process consists in, for each line of the intrinsic impact table, and for each classification criterion (A, I or C):

- Selecting the relevant elements in the classification tables;
- Identifying, for each selected element, the maximum classification level, and copying this across to the intrinsic impact table;

The selected elements are shown in the table T3 below, where each field shows:

- In columns A, I or C, the highest value found in identical column(s) of tables T1 and T2;
- In the Condition column, the criterion for selecting lines from tables T1 and T2 so as to only extract those elements in each table that are in both the selected lines and columns.

Intrinsic Impact Table formulae

Classification of data, information and infrastructure components						Rule
Data and information		A	I	C	Condition	
D01	Data files or application databases		T1 : column Ida	T1 : column Cda		1
D02	Desktop files stored on a shared access server	T1 : column Afb	T1 : column lfb	T1 : column Cfb	Lines such as ASB # ""	2
D03	Desktop files stored on a fixed personal workstation	T1 : column Afb	T1 : column : lfb	T1 : column Cfb	Lines such as ASB = ""	2
D04	Handwritten or printed information held by users, personal archives	T1 : column Aec		T1 : column Cec		1
D05	Listings or IT application printouts			T1 : column Cli		1
D06	Messages exchanged, data in transit	T1 : column Atm	T1 : column ltm	T1 : column Ctm		1
D07	POSTal mail and FAXes	T1 : column Acf	T1 : column lcf	T1 : column Ccf		1
D08	Historical archives, archives having a proof value	T1 : column Aec			Lines Typ ARI and ARD	3
D09	Data and information published on public websites	T1 : column AAa	T1 : column Ida	T1 : column Cda	Lines such as ARP # ""	2
IT and telecommunication infrastructure						
R01	WAN links and equipment (network systems and their software)	T1 : column AAa T2 : column Aeq	T1 : columns Cda, Ida and lap T2 : column leq		T1 lines such as ARE # "" T2 line: SCA = RE	2 and 4
R02	LAN links and equipment (network systems and their software)	T1 : column AAa T2 : column Aeq	T1 : columns Cda, Ida and lap T2 : column leq		T1 lines such as ARL # "" T2 line: SCA = RL	2 and 4
R03	WAN configuration data	T2 : column Afc	T2 : column lfc	T2 : column Cfc	T2 line: SCA = RE	4
R04	LAN configuration data	T2 : column Afc	T2 : column lfc	T2 : column Cfc	T2 line: SCA = RL	4
S01	mainframes, application servers, and dedicated central peripherals, shared file servers	T1 : column AAa T2 : column Aeq	T1 : columns Cda, Ida and lap T2 : column leq		T1 lines such as ASA # "" T2 line: SCA = SV or SS	2 and 4
S02	System and server configuration files	T2 : column Afc	T2 : column lfc	T2 : column Cfc	T2 line: SCA = SV	4
S03	Terminal equipment available for users (PCs, printers, peripherals, special devices,)	T1 : column AAa T2 : column Aeq			T1 lines such as AED # "" T2 line: SCA = PF	2 and 4
A01	Application software or programs, middleware	T1 : column Aap	T1 : column lap	T1 : column Cap		1
General infrastructure						
E01	User working environment	T1 : columns Afb and Aec T2 : column Aeq			All T1 lines T2 line: SCA = ET	1 and 4
E02	Oral or analogical telecommunications equipment	T2 : column Aeq	T2 : column leq		T2 line: SCA = RT	4
I01	All of the IT or telecommunications room installation	T1 : columns Aap and AAa T2 : column Aeq				1

The last part of table T3 corresponds to intrinsic impacts that do not depend on the classification of an asset. In fact, it requires the evaluation of intrinsic impact of some rather particular types of scenario. In practice, these will concern the non-availability of staff or the non-adherence to laws or directives.

This part should be the subject of a specific analysis taking into account the possible consequences of a risk scenario and the directly evaluated intrinsic impact, independently of any classification.

5. Practical Advice

5.1. *Important points to consider in creating the value scale*

5.1.1 *Focus on the most critical aspects*

It is important to focus on the main malfunctions, rather than to try to consider every possible risk scenario.

The first goal of security, whatever approach is used, is to avoid the occurrence of serious or very serious problems. These are the risks that must, therefore, be identified and examined.

This is why it is strongly recommended that the top management and those immediately responsible for a given activity be directly implicated in the evaluation process. It should never be delegated to a deputy.

In practice, for each activity, it is best to focus on a small number of critical malfunctions (generally, between 3 and 8).

5.1.2 *Exclusion of existing controls*

Secondly, but just as important, malfunctions that at first sight appear impossible should not be ignored. It is all too often seen that management dismisses the potential occurrence of an accident that could lose all key data, through the pretext that the data is computerized and therefore archived by the IT system. ***Malfunctions, and their seriousness, should be identified and evaluated without taking existing security controls into account, even if those measures are solidly implemented.*** Otherwise, this could lead to concluding that there is nothing at stake, and that the security controls are not required, and could therefore be dispensed with.

Likewise, the more or less probable nature of an event that leads to a malfunction should not be taken into account during this phase of the approach.

5.1.3 *Consistency of malfunctions of different kinds*

Another important point in determining criteria and critical thresholds is to maintain a consistency between different kinds of malfunction that have equivalent seriousness levels.

With this aim in mind, it is recommended to define strategic axes that can be used as references to ensure the consistency of seriousness levels for different malfunctions.

One of the valuation axes may be financial. Thus, financial equivalents would be sought for each kind of malfunction. Likewise, a “service to public” axis would be the reference for comparing individual impact, population size, etc.

5.1.4 *Strategic and decision-making aspects of the value scale*

Often, the seriousness of some malfunctions cannot be evaluated. This may be because the indirect consequences are difficult to identify, or because it is too difficult to seriously judge the efficiency of actions that could be made in the given situation.

In some situations, the seriousness of a malfunction can be the result of a simple decision.

There is no formal evaluation but a strategic decision for the enterprise or organisation that

says that a given malfunction should be considered serious, very serious, or vital.

5.2. *Important points during classification*

Firstly, it is important to properly group assets with similar goals so as not to have to analyse a vast amount of objects.

A good starting point is to group applications by domains.

Secondly, it is recommended to plan for a consolidation and validation step at the level of each entity, as for the value scale.

5.3. *Boundaries for the classification*

Clearly, the process that has been described, whether it be the creation of the value scale or classification, applies to an entity with decisional independence and its own goals. This could be an affiliate (national or regional) of a corporate group, or a business unit, or an operational or functional service with a well defined responsibility.

The malfunction value scale and the classification of information and assets that are defined for an entity are obviously valid for that entity. However, what is their value outside of that entity?

By definition, the classification defined for an entity is a means to share and communicate the sensitivity of an asset belonging to that entity. This classification is valid across the enterprise.

In fact, this is a rule of exchange of elements (particularly information) between entities. If an entity A (a small agency, for example) considers that the confidentiality of information is vital, and classifies it as such, it is not possible for entity B (headquarter for example) to reconsider the classification and to decide that the information is not sensitive. If the latter were to be allowed, then entity A would have to decide not to transmit information to entity B.

This notion of limits of validity for classification is particularly important in security management based on a rule set called “Security reference framework”.

In the example above, the precautions or security controls which will be applied as a function of the classification are known. It would be stupid for an entity to protect information aligned on a level of classification and that different entities apply different protection rules for the same information. Particularly, it would be dangerous for an other entity to decide on its own that information need not be protected at the level decided by another entity.

5.4. *Action plans*

Here, we shall not cover the building of security plans directly from the stakes analysis.

However, it is worth noting that the individual interviews that contribute to the creation of the value scale, together with a management meeting, at which the most serious malfunctions are discussed, should give birth to urgent action plans. Any manager would naturally be frustrated to have spent time on an analysis and identification of vulnerabilities, only to find that nothing results from it.

An action plan for the most urgent actions should, therefore, be drawn up. This should potentially be discussed and approved in a management meeting, straight away after the stakes analysis is completed.

Appendix 1: Example of a value scale (industrial enterprise)

1. Finance and budget management

<i>Malfunction</i>	<i>Level 1 Insignificant</i>	<i>Level 2 Serious</i>	<i>Level 3 Very Serious</i>	<i>Level 4 Vital</i>
<i>Financial loss</i>	Loss < 1 M€	Loss between 1 M€ and 10 M€	Loss between 10 and 100 M€	Loss > 100 M€
<i>Fraud or embezzlement</i>	Fraud or embezzlement in purchasing and corresponding payment or in delivery management.			
<i>Inability to bill delivered goods</i>	Global inability to bill for less than a week	Global inability to bill for between a week and a month. Loss of information concerning deliveries made during one day.	Global inability to bill for more than one month. Complete loss of proof of delivery for a whole week.	
<i>Malfunction of customer reminder process</i>	Temporary unavailability of reminder system.	Long-term unavailability of reminder system.		

2. Strategy – General guidelines – Management and follow-up

<i>Malfunction</i>	<i>Level 1 Insignificant</i>	<i>Level 2 Serious</i>	<i>Level 3 Very Serious</i>	<i>Level 4 Vital</i>
<i>Disclosure of data or information concerning long term or strategic plans.</i>		Disclosure of an affiliate's long-term plans Disclosure of the budget Disclosure of the monthly reports	Disclosure of information concerning strategic evolution Disclosure of the consolidated long-term plans of the enterprise	
<i>Unavailability of the results analysis or internal reporting system</i>	Unavailability of the monthly reporting process	Inability to make reports or results analysis for more than 2 months.		
<i>Corruption of reporting data and monthly reports</i>	Corruption of elementary data or enhanced information based on elementary data.			

3. Business development – customer management

<i>Malfunction</i>	<i>Level 1 Insignificant</i>	<i>Level 2 Serious</i>	<i>Level 3 Very Serious</i>	<i>Level 4 Vital</i>
<i>Disclosure of information concerning business development operations</i>	Disclosure of notes and executive summaries concerning business development			
<i>Disclosure of financial conditions</i>	Disclosure of financial conditions specific to one customer to another	Disclosure of price fixing strategy documents	Disclosure of financial conditions made to all customers.	
<i>Disclosure of customer information</i>	Disclosure of some elements of customer information base	Disclosure of information on all customers		

4. Research and development

<i>Malfunction</i>	<i>Level 1 Insignificant</i>	<i>Level 2 Serious</i>	<i>Level 3 Very Serious</i>	<i>Level 4 Vital</i>
<i>Disclosure of technical information</i>	Disclosure of simulation models	Disclosure of current technical bulletins Disclosure of information about specifications or internal procedures and on current evolution	Disclosure of technical bulletins in exceptional cases Disclosure of information on the impact of technical evolution, resulting in the closure of facilities.	
<i>Confidentiality agreements breach</i>		Breach of confidentiality agreements with partners	Breach of confidentiality agreements with key technology suppliers	
<i>Loss of expertise</i>			Loss of all archives of memorandums and technical bulletins concerning technical development.	

5. Industrial process management – Projects for evolution - Maintenance

<i>Malfunction</i>	<i>Level 1 Insignificant</i>	<i>Level 2 Serious</i>	<i>Level 3 Very Serious</i>	<i>Level 4 Vital</i>
<i>Loss of evolution project document archives</i> <i>Loss of technical documentation for existing equipment</i>	Loss of project archives during the project's lifetime. Loss of original copies of equipment plans that have been approved by the appropriate authorities.	Total loss of long-term archives concerning equipment and modifications made thereto.		
<i>Malfunction leading to use of incorrect installation plans during evolution and updates</i>			Errors in, or changes to, existing installation plans, or malfunction of change management.	
<i>Disclosure of technical information</i>		Disclosure of work themes and pre-project research programme.	Disclosure of entire pre-project dossiers (including strategic positioning of the project)	
<i>Unavailability of project management tools(planning, order management, administrative dossiers, etc)</i>	Unavailability of the internal planning tool Unavailability of the order management tool for less than a week.	Unavailability of order management tool for the project for more than a week		
<i>Malfunction in maintenance management</i>	Loss of the planned maintenance action database	Unavailability of maintenance management tools for less than a month Loss of technical and historical data required for maintenance planning	Unavailability of maintenance management tools for more than a month. Changes to parameters of maintenance management tools	

6. Production and delivery – Logistics

<i>Malfunction</i>	<i>Level 1 Insignificant</i>	<i>Level 2 Serious</i>	<i>Level 3 Very Serious</i>	<i>Level 4 Vital</i>
<i>Production stopped (no energy, control system unavailable, loss of a critical element...)</i>	No production for less than one week	No production for between 1 week and 1 month. Loss of a critical element, leading to production loss for less than 1 month.	No production for between 1 and 3 months. Loss of a critical element, leading to production loss for between 1 and 3 months	Production stopped for more than 3 months. Loss of a critical element, leading to production loss for more than 3 months.
<i>Production management tools not available</i>	Production management tools not available for less than 1 week	Production management tools not available for between 1 week and 1 month	Production management tools not available for more than 1 month	
<i>Corruption of production management tools or falsification of management parameters</i>			Modification of production management leading to non-conformity of products	Modification of production management leading to accidents or deterioration of production tools
<i>Inability to ensure the logistics for product delivery</i>	Inability to ensure critical deliveries for less than a week	Inability to ensure critical deliveries for more than a week		

7. Third-party relationships (other than commercial)

<i>Malfunction</i>	<i>Level 1 Insignificant</i>	<i>Level 2 Serious</i>	<i>Level 3 Very Serious</i>	<i>Level 4 Vital</i>
<i>Disclosure of information on corporate results</i>		Premature publishing of an affiliate's results	Premature publishing of consolidated accounts	
<i>Malfunction in the process for consolidating annual accounts</i>	Delay in publishing accounts less than 2 weeks	Delay in publishing accounts more than 2 weeks	Total loss of all financial elements required for producing annual accounts	
<i>Disclosure of notes or memos concerning fiscal risks, operations, or mechanisms</i>	Disclosure of notes or memos concerning fiscal risks, operations or mechanisms, depending on the content of the note or memo			
<i>Loss of historical elements that justify a fiscal operation</i>	Loss of historical elements that justify a fiscal operation			
<i>Late payment of charges and tax</i>		Unavailability of tax payment calculation tools		
<i>Loss of official documents or archives</i>		Loss of official authorizations to operate	Loss of official documents or archives that are legally required by administrative procedures (tax, export,...)	

8. Claims management – legal and penal aspects

<i>Malfunction</i>	<i>Level 1 Insignificant</i>	<i>Level 2 Serious</i>	<i>Level 3 Very Serious</i>	<i>Level 4 Vital</i>
<i>Disclosure of exhibits or arguments relating to a claim.</i>	Disclosure of information relating to an ongoing claim.	Disclosure of information relating to an exceptional claim.		
<i>Disclosure of parts of a penal brief concerning staff</i>		Disclosure of parts of a current penal brief	Disclosure of parts of a penal brief in exceptional circumstances	
<i>Loss or disappearance of originals of documents</i>	Loss or disappearance of originals of contracts	Loss or disappearance of originals of specific agreements, declarations of intent, etc		

9. HR management

<i>Malfunction</i>	<i>Level 1 Insignificant</i>	<i>Level 2 Serious</i>	<i>Level 3 Very Serious</i>	<i>Level 4 Vital</i>
Disclosure of personal information	Disclosure of an employee's salary	Disclosure of the salaries of all the personnel	Repeated disclosure of the salaries of all the personnel	
Delays in paying salaries	Delay < 2 days	Delays between 2 and 15 days	Delays > 15 days	
Destruction of basic data concerning payment of salaries (calculation, and parameters)	Erasure of recent data (less than a month old)	Erasure of the year's data	Erasure of all data, including historical data	

10. Information system

<i>Malfunction</i>	<i>Level 1 Insignificant</i>	<i>Level 2 Serious</i>	<i>Level 3 Very Serious</i>	<i>Level 4 Vital</i>
<i>Unavailability of network and servers (shared and personal data)</i>	Unavailability for less than one month	Unavailability for more than one month		
<i>Unavailability of the e-mail system</i>	Unavailability of the e-mail system			
<i>Unavailability of the telephone network</i>	Unavailability of the telephone network			
<i>Loss of all archives</i>		Loss of data servers, or e-mail archives		
<i>Illicit creation of administration rights on systems</i>			Corruption of the access rights table(s) and creation of administration rights	
<i>Disclosure of system or architecture information</i>			Disclosure of executive reports or detailed information concerning system security and uncorrected weaknesses.	

Appendix 2: Intrinsic Impact Table

Intrinsic Impact table				
Classification level of data, information and infrastructure components		A	I	C
Data and Information				
D01	Data files or data bases accessed by applications			
D02	Shared office files and data			
D03	Personal office files (on PC, etc.)			
D04	Written or printed information and data kept by users and personal archives			
D05	Listings or printed documents			
D06	Exchanged messages, screen views, etc. (partial data)			
D07	Mails and faxes			
D08	Patrimonial archives or documents used as proofs			
D09	Data and information published on public or internal sites			
Infrastructure : telecommunications and systems				
R01	Wide Area Network equipment and wiring (networking systems and associated software)			
R02	Local Area Network equipments and cables (networking systems and associated software)			
R03	Configuration data for the WAN			
R04	Configuration data for the LAN			
S01	Main systems, servers hosting applications and their peripheral equipments, shared file servers			
S02	Configuration files related to main systems et servers			
S03	Workstations and user terminals (PC, local printers, peripherals, specific interfaces, etc.)			
A01	Application software, package or middleware (executable code)			
A02	Source code			
A03	Configuration files related to applications			
A04	User or client software and applications			
General infrastructure				
E01	User workspace and environment			
E02	Equipments used for vocal exchanges (telephone, etc.)			
I01	Entirety of the computer room and the telecom premise			
Intrinsic impacts (global objects or not related to a specific object)				
Personnel unavailability				
P01	Teams of specialists (business related)			
P02	IT operation personnel			
Legal and regulatory non compliance				
C01	Non compliance to laws and regulations relative to private life protection			
C02	Non compliance to laws and regulations relative to financial controls			
C03	Non compliance to laws and regulations relative to intellectual property rights			
C04	Non compliance to laws and regulations relative to information system protection			
C05	Non compliance to laws and regulations relative to endangerment of personnel and public and environmental safety			