WHITE PAPER

RISK MANAGEMENT

-

Concepts and Methods

Methods Commission / Espace Méthodes

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

Table of Contents

ACKNOWLEDGMENTS

CLUSIF would like to extend special thanks to the members of the Methods space who made this document possible:

Dominique	**BUC**	*BUC SA*
Olivier	**CORBIER**	*DOC@POST*
Éric	**DERONZIER**	*YSOSECURE*
Jean-Philippe	**JOUAS**	*CLUSIF*
Gérard	**MOLINES**	*MOLINES CONSULTANTS*
Jean-Louis	**ROULE**	*CLUSIF*

We would also like to thank our associate in Québec Martine **GAGNE** for her invaluable help in carefully re-reading the French document and making helpful suggestions.

1 INTRODUCTION

Starting or developing a business always requires taking risks.

On this basis it is clearly important to identify, analyse, control and manage these risks, and sensible to do so using a methodological framework.

Various methods of analysing and managing risk exist, each offering different definitions of risk management, which can be confusing.

This document aims to define different types of risk management methods and describe resulting key steps.

Presented in this light, the following study can be applied to a wide range of risks. However due to the development and importance of specific standards for managing IT security-related risks, we will often refer to and cite examples from this particular field.

This study focuses strictly on risk management and is not intended as an evaluation of the pros and cons of different methods used as security management tools in a given context.

2 SUMMARY

The following study identifies significant differences between various risk management methods.

The key areas in which differences exist are briefly described below.

2.1 Identification of risk situations

The process of identifying risk situations may entail the broad participation of the management team and be focused on “strategy” and the “entity's primary objectives”, or on the contrary occur at an operational and technical level.

Even the manner in which risks are defined will vary depending on the approach taken.

2.2 Options for managing risks

Risk can be managed in one of two principal ways:

- by analysing each identified risk situation and taking specific measures that are adapted to each one, with the broad participation of the management in risk management, or

- by using more general analysis to establish security goals and guidelines in order to globally reduce risk without managing it through direct and personalised means and likely with less management participation.

The first risk management option requires an advanced risk analysis model that the second option does not.

These risk management options have a direct effect on each phase of the related process. These effects are described later on in the document.

2.3 Tools and knowledge bases

Various risk management tools exist, ranging from the strict minimum to comprehensive methodological approaches that include knowledge and expertise bases, auditing tools, simulation tools for gauging risk levels in relation to the security measures taken, performance indicators, etc.

It should also be considered how far these tools could be customised.

3 RISK: GENERAL PRINCIPLES AND DEFINITIONS

Before discussing management, we must first try to address the issue of what a "risk" is, as each method uses its own definition.

These definitions are based on a few generally established concepts. These are presented below and followed by an examination of points of divergence that allow different decisions to be taken.

3.1 Basic concepts

Risks exist because entities, companies and organisations have "assets" of a material or immaterial nature that could be subject to damage that has consequences on the entity in question.

Four concepts are important here:

- assets, a term often used in the field of IT security[1],
- asset damage,
- consequences for the entity,
- possible but uncertain causes.

3.1.1 Assets

In very general terms, an asset can be defined as anything that could be of value or importance to the entity.

In information security, the ISO/IEC 27005 standard distinguishes between:

- Primary assets including:
    - Processes and activities,
    - Information
- Supporting assets including:
    - Equipment,
    - Software,
    - Networks,
    - Personnel,
    - Premises,
    - Organisational support

[1] The term "asset" is clearly defined and explained in the ISO/IEC 27000 series of standards, which specifically address risks linked to information security. This term does not appear in more general standards like ISO Guide 73 or the ISO 31000 standard,.

This is of course a very general definition that, while common to all methods, translates into a range of practical applications.

3.1.2 Asset damage

Clearly, risks (and their consequences) differ depending on what type of damage occurs.

Different categories of assets will be damaged in different ways, and while it is easy to list the ways in which information can be damaged (by being lost, tampered with or exposed, among other things), few standard classifications exist for processes or certain support-related assets.

The type of damage an asset sustains is not clearly specified in the ISO/IEC 27005 standard, which does not distinguish either damage from consequences. In our view however it is important to distinguish between direct consequences of damage to assets, and secondary or indirect consequences affecting processes and the entity's activities.

3.1.3 Consequences for the entity

The nature of consequences can vary widely, depending on whether the entity in question is a commercial business, public organisation or association for example.

The only important thing to keep in mind at this stage is that an evaluation of these consequences will have to focus on the entity rather than its information systems or the technical scope of analysis, and that an evaluation of risk must include an assessment of the impact that damage of a particular asset would have on the entity.

3.1.4 Possible but uncertain causes of damage to an asset

Definitions of risk usually make reference to the cause or type of cause – necessarily uncertain – of damage to an asset. The ISO guide 73 uses the term "event" to describe this notion of cause.

Generally speaking:

- A risk (as opposed to an observation or certainty) exists only if an uncertain action or event happens that leads to the occurrence of that risk – in other words the damage of the asset in question,

- Risk evaluations must include an assessment of how likely this action or event is to occur.

While our use of the word "cause" can be ambiguous in the sense that there are direct causes (what Guide 73 calls "events") and indirect causes (what the same guide calls "sources"), it represents well the general idea of something that will lead to damage.

3.1.5 Defining threat

ISO/IEC 27000 series of standards on risk related to information systems refer to the idea of "threat"[2]. Which is not really defined, except to say "a threat has the potential to harm assets such as information, processes, and systems and therefore organizations" (ISO/IEC 27005).

One might assume that a threat is similar to the "cause" mentioned above, but it is in fact quite different: threats can apply to a wide range of aspects, particularly:

- Events or actions that can lead to the occurrence of a risk (for example an accident, fire, media theft, etc.),
- Actions or methods of action that make the occurrence of risk possible without causing it (for example abuse of privilege, illegal access rights or identity theft),
- Effects related to and which indicate undetermined causes (for example the saturation of an information system),
- Behaviour (for example unauthorized use of equipment) that is not in itself an event that leads to the occurrence of risk

These examples show that a threat is not strictly linked to the cause of a risk, but it does make defining typologies of risk possible using a list of typical threats.

3.1.6 Defining vulnerability

The term vulnerability is sometimes used in risk analysis but more widely in the domain of information systems security[3].

Vulnerability can be defined in two ways.

Linguistically speaking, the most correct definition describes vulnerability as a **feature of a system, object or asset that may be susceptible to threats**.

If we take the example of a typed or handwritten document, where the threat would be rain or storms in general, possible vulnerabilities would be:

- that the ink is not waterproof,
- the paper is water-sensitive,
- the material it is written on is degradable.

Often, it is more useful to think of vulnerabilities in terms of security controls and their potential shortcomings. **Then, vulnerability is defined as a shortcoming or flaw in a security system that could be used by a threat to strike a targeted system, object or asset**.

---

[2] The term "threat" does not appear in more general standards like ISO Guide 73 or the ISO 31000 standard, but is used in the present document because it is widely employed in certain risk management methods.

[3] Similarly, the term "vulnerability" is not used in general standards on risk management, particularly in ISO Guide 73, but is widely referred to in certain risk management methods.

In the example above, the exploited vulnerability was a lack of protection against storms.

From here, vulnerability branches out in many directions, as every security system has weaknesses and any solution intended to reduce vulnerability is vulnerable itself.

If we go back to the example of the document made of degradable material an initial solution is the storage away from storms

- Resulting vulnerabilities:
    - Faulty plumbing systems within the building,
    - Inadequate or poorly executed storage procedures,
    - Activation of fire protection sprinklers,
    - Etc.

When examining the notion of vulnerability, it may be useful to keep in mind that these two approaches are not the same.

* * * * *

By using these general concepts, several definitions of risk are possible and in fact proposed by different risk management methods. At the same time, they are compatible with standard-setting documents.

3.2 Defining risk

The notion of risk in general is not problematic, but difficulties arise when we look for a formal definition that identifies every element of a risk. These elements come into play during the risk identification process, and the assessment process later.

Paradoxically, risk management methods rarely provide such a formal definition. Possible definitions fall into one of two major categories:

- Threat-based definitions of risk, linked or not linked to vulnerabilities,
- Scenario-based definitions of risk.

3.2.1 Defining risk based on an "asset /threat" or "asset /threat/ exploited vulnerability" framework

Risk can initially be defined as:

The combination of an asset with a threat capable of damaging that asset.

Risk management methods that use this definition often provide a typology of different types of threats[4].

Another approach, seen in some methods, is to include certain vulnerabilities that are exploited by a threat in the definition of risk. Here, the idea is that risk only exists in the presence of an exploitable vulnerability.

[4] Appendix C of the ISO/IEC 27005 standard provides a list of typical threats.

Risk is then defined as:

The combination of an asset, a threat capable of damaging that asset and vulnerabilities exploited by the threat to damage the asset.

From these definitions, certain "common" or "typical" risks emerge based on types of threats, assets and, in some cases, vulnerabilities.

This is a **"static" model of risk** in that the elements under consideration do not incorporate time as a variable, and it is impossible to describe sequences of events, causes or consequences.

3.2.2 Defining risk based on a scenario

Another definition of risk incorporates asset damage and a description of the circumstances in which the damage took place.

Circumstances can refer to a:

- Place: for example, media theft from one type of location or another,
- Time: for example, an action carried out during or outside business hours,
- Processes or phases of a process: for example, altering files during maintenance.

Risk is then defined as:

The combination of an asset, a type of damage that may occur to the asset and the circumstances in which this damage may occur.

The term threat can still be used if taken to mean a general description of the types of circumstances in which a risk may appear. Circumstances are hence described as:

- a generic threat that describes a typology of circumstances, and
- specific circumstances that identify a generic threat.

In practice, this definition leads to a definition of **"risk situations"** or **"risk scenarios"** that simultaneously describe the damage to an asset and the circumstances in which the damage occurred.

This is exactly how risk is described in the ISO Guide 73, which defines a risk as consisting of dangerous sources or phenomena (circumstances), triggering events and consequences.

This is a **"dynamic" model of risk** in which time plays a role, and as a result, different phases of the risk scenario in question result in different types of action. This dynamic model makes it possible to describe and take into account chains of events, causes and consequences.

It is interesting to note that the ISO/IEC 27005 standard addresses the notion of incident scenarios, very similar to the "risk scenario" mentioned above, but not exactly equivalent. Incident scenarios involve the exploitation of a given vulnerability or set of vulnerabilities, but the particular circumstances in which a risk occurs can be linked to a range of elements that, as explained above, are not

necessarily linked to vulnerabilities.

* * * * *

* * *

*

There are obviously other ways of defining risk and its components, but we will focus on these two definitions, which are a significant feature of risk management.

4 RISK MANAGEMENT: BASIC OPTIONS

Independently of a definition of risk, the goals of risk management can also be very different.

Practically speaking, risk management aims to achieve one of two things, which when studied closely, appear fundamentally different:

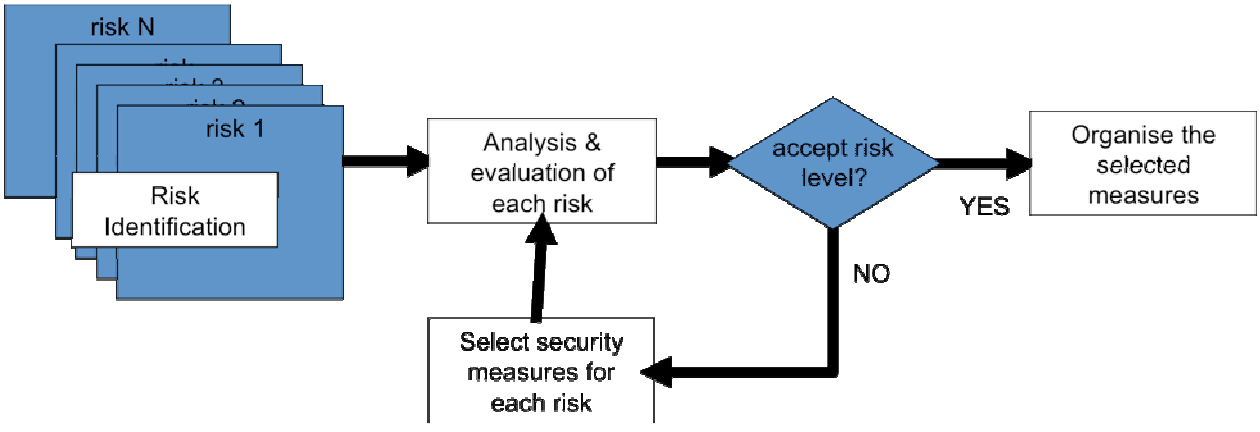
- direct and individual management of each risk within the framework of a risk management policy,
- global and indirect risk management using a security policy that is adapted to possible risks.

Note: The content and level of detail of this policy is discussed in Chapter 8.

4.1 Direct and individual risk management

This management approach, which is defined by and built around a risk management policy, aims to:

- Identify all the risks to which the company is exposed
- Determine the level of each risk
- Take measures to reduce the level of each risk identified as unacceptable to an acceptable level
- Ensure constant monitoring of risks and levels of risk using the appropriate tools
- Ensure that each individual risk is well managed and that a decision has been taken to accept, reduce, or transfer each risk.



This management method is highly oriented towards the entity's activities and

fundamental interests, and can only be used successfully in full agreement with the entity's management team, who must participate actively.

It is also highly adapted to project-based organisations in which project managers are responsible for risk management.

Underlying principle and pre-condition

Clearly, managing each risk on an individual basis requires knowing when to examine all existing or planned security measures that may influence the level of risk.

The underlying principle and pre-condition of a management method of this type then is a risk model that, for each identified risk, determines:

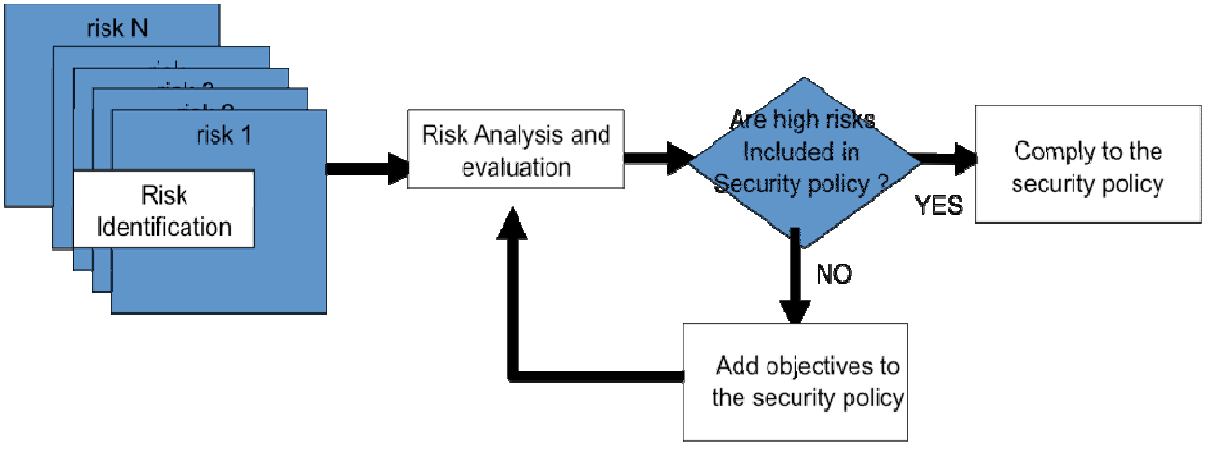
- Structural risk factors related to the entity's activities and current context that are independent of security measures
- The role of security measures and their effects on the risk in question
- The overall level of risk that results

Without such a model, it would be impossible to link the decision to implement security measures to the resulting level of residual risk. This link is necessary however for individual risk management.

4.2 Global and indirect risk management

Here, the goal is to develop a security policy based on evaluating risks. The aim is to:

- Identify certain elements that can lead to risks
- Classify these elements by order of importance
- Determine a policy and security goals
- Ensure constant monitoring of risks and levels of risk using the appropriate tools



This management method requires less intervention from the entity's management

and can be applied on a technical level.

Underlying principle and pre-condition

The principle of this type of management is to define security needs or goals by classifying levels of risk according to whether these goals are reached or not and whether or not these needs are met.

This may result in a partial view of risk that only takes into consideration some of the elements that affect the real level of risk - in particular certain vulnerabilities (or types of vulnerabilities) exploited by typical threats.

The underlying principle and pre-condition of a management method of this type then is a risk model that, for each identified risk, determines:

- a level of risk as a function of elements listed in the description of this risk
- The influence of the choice of goals in the security policy
- The "relative" level of risk that results

It is important to note that this evaluation of risk levels is only valid "based on elements identified during the risk identification process" and "based on the impact of the security policy on these elements". Therefore it does not represent the real level of risk faced by the entity, but the importance of the security goals that are held in the security policy.

4.3 Definitions of risk and types of management

Clearly, scenario-based definitions of risk are particularly well adapted to direct and individual risk management, while definitions based on threats and vulnerabilities are in principle well adapted to global and indirect risk management.

In theory though, there is no reason why a scenario-based definition couldn't be used for indirect risk management in the framework of a security policy.

Nor is it impossible to use a definition of risk based on threats and vulnerabilities for direct and individual risk management; the search for scenarios that may lead to the risk in question or belong to this risk category becomes part of the risk evaluation process and the process of choosing security measures.

A note on the link between vulnerabilities and risk management methods

It is worthwhile to examine the link between incorporating vulnerabilities into risk identification and the style of management.

Incorporating vulnerabilities into the process of defining risks (as opposed to the risk analysis phase) has several consequences worth examining:

- Not incorporating vulnerabilities into risk identification implies that a risk results simply from the combination of an asset element that has value and of circumstances in which this value could be put at risk. It also implies that

it is the situation to be managed and that vulnerabilities will be taken into account later, during the analysis of this risk situation.

This is a direct approach to risk management. Incorporating vulnerabilities into the process of defining risks however implies that it is the vulnerabilities that will be evaluated and managed. This, then, is indirect risk management.

- In a given risk situation though, several vulnerabilities are often involved and exploited rather than just one. For example, a case of piracy from outside the company that leads to application data theft can simultaneously exploit vulnerabilities such as weak network access control, a lack of network partitioning or confinement of sensitive files, weak system access control, weak application access control, a lack of file encryption, etc.

  In this context, incorporating a list of exploited vulnerabilities into the risk definition process would definitely make direct risk management more difficult. It would also add a technical analysis task (searching for all the vulnerabilities related to a risk situation) to what is supposed to be a management task (risk identification).

Therefore, it is fair to say that incorporating vulnerabilities into risk identification is compatible with global and indirect risk management, but much less so with direct and individual risk management.

* * * * *

* * *

*

After outlining these basic approaches, the chapters that follow will examine how they determine the content of the various phases described by standards and particularly by ISO Guide 73, which appears below (the phases to be analysed in detail are in bold; attention is not paid in particular to the process of moving from one step to another).

RISK MANAGEMENT			
	RISK ASSESSMENT		
		RISK ANALYSIS	
			RISK IDENTIFICATION
			RISK ESTIMATION
		RISK EVALUATION	
	RISK TREATMENT		
		RISK AVOIDANCE	
		RISK OPTIMISATION (reduction)	
		RISK TRANSFER	
		RISK RETENTION	
	RISK ACCEPTANCE		
	RISK COMMUNICATION		

5 RISK IDENTIFICATION

The nature of the risk identification phase depends on how risk has been defined.

Whatever the definition, a risk arises in the presence of values or asset elements that represent a stake for the company or organisation; where certain qualities must be maintained for the entity to function properly.

Identifying potentially critical assets is therefore the first step, and a part of all risk analysis methods.

The second step, which depends on how risk has been defined, involves looking for:

- threats that may damage these assets, and vulnerabilities that could be exploited (where risk is identified on a threat/vulnerability basis), or

- damage that may affect these assets and the circumstances in which this damage may occur (where risk is identified on a situation/scenario basis)

We will begin by looking at asset identification, followed by threat/vulnerability identification and risk scenario identification

5.1 Identifying critically important (or potentially critical) assets

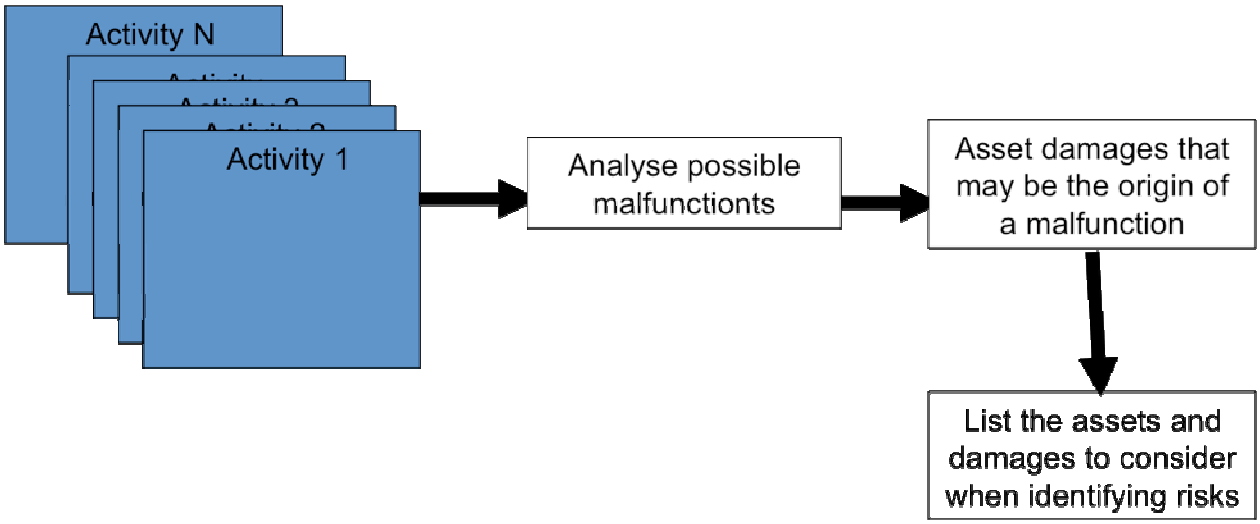
This is unquestionably an essential phase in risk identification. Two main approaches exist:

As seen in the diagram below, the first approach involves:

- analysing the processes and activities of the company or entity and looking for any process malfunctions that could have an impact on the entity's goals and expected results,

- Looking for the assets and damage to these assets that could be the origin of such malfunctions,

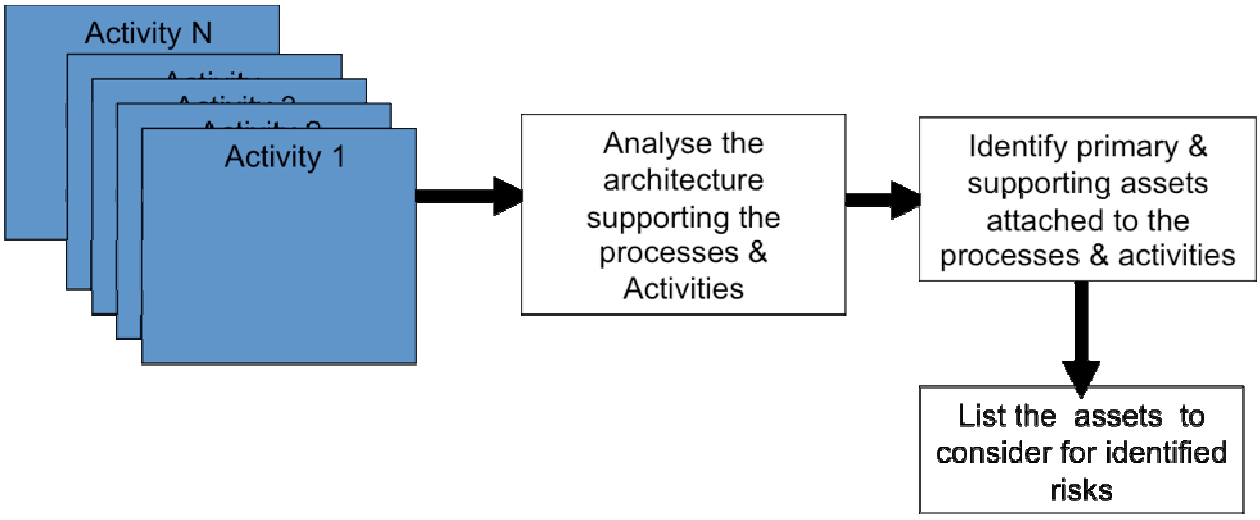
- Establish a list of assets (it may be useful to specify those of critical importance to avoid overloading the other risk management phases).



This approach focuses on the importance of the entity's different activities, and should ideally be carried out by high-level management. This approach quite naturally leads one to look for circumstances in which damage may occur and to define risk scenarios.

The second approach involves:

- Analysing how the primary means supporting the entity's activities are structured (be it the information system, or any other means like manufacturing, logistics and communication),
- If appropriate, looking for secondary means that support the primary means (like energy and organizational means, etc.),
- Establishing a list of assets to be considered when identifying risks.



This is a far more technical approach that can be carried out without the help of high-level management. It is conducive to a search for possible threats to these

assets and to the identification of risk based on threats and vulnerabilities.

One key difference is that with scenario-based definitions of risk, the type of damage an asset may suffer if a risk occurs is taken into account when looking for critically important assets.

In other words, the criteria used to value assets during the risk estimation process (in threat-based definitions of risk) are incorporated even into the asset identification process, when identifying risk scenarios.

As an illustration, here are a few examples involving three types of assets.

In a static conception of risk, identified assets could be:

- A strategic planning document
- the database for a particular business line
- the data server for a given operation

In a dynamic conception of risk based on scenarios, identified elements will also be linked to a type of damage:

A. A confidential strategic planning document

B. A database for a given business line, the integrity of which must be maintained

C. A data server for a given operation **which must remain available**

5.2 Identifying threats and vulnerabilities

Threat-based definitions of risk usually involve selecting, from a list of typical threats, standard elements that are relevant to the type of asset in question.

For the asset elements of the three examples listed above, there would be (based on just some examples from ISO/IEC 27005):

1. Strategic document

   Related threats
   - Media or document theft
   - Disclosure

2. Database

   Related threats
   - Tampering using software
   - Software malfunction

3. Data server

   Related threats
   - Fire
   - Water damage

- Serious accident
- Destruction of equipment
- Flooding
- Etc.

Definitions of risk that include exploited vulnerabilities usually involve selecting related vulnerabilities from a list that if necessary has been pre-sorted according to types of threats or vulnerabilities. For the examples listed above, there would be (also based on the examples given in the appendices of ISO/IEC 27005 standard):

1. Strategic document

   Threat and vulnerability:

   - Media or document theft due to insufficient data storage protection

2. Database

   Threat and vulnerability:

   - Tampering, due to downloading and uncontrolled use of software

3. Data server

   Threat and vulnerability:

   - Destruction of equipment due to a lack of provisions for its periodic replacement

5.3 Identifying risk scenarios

This consists in analysing the processes involving the asset element in question, the life cycle of this element, or its structure, to see what may put it at risk.

This inventory is done either directly or using a knowledge base that lists frequently encountered risk scenarios where possible (depending on the method used).

For the same examples:

1. Confidential strategic document

   Calls for the analysis of how this type of document is produced, monitored and distributed. It is possible to list various circumstances that lead to specific risks:

   - when the document is produced (a computer file either on the PC of the manager or his/her assistant, or on a shared server)
   - when the document is saved
   - when the document is printed (on a shared printer)
   - when it is sent by e-mail
   - when it is sent in the mail
   - when it is stored

2. A database whose integrity must be maintained

   Also calls for an analysis of the various processes involving the database that may put its integrity at risk. It is possible to list various circumstances that lead to specific risks:

   - when the database is accessed simultaneously (software risks)

- in the case of malevolent access
- during software maintenance
- during development or maintenance tests
- during maintenance operations

3. A data server which must remain available

Calls for analysis and list of various types of possible causes and internal processes involving this asset element, which could make it unavailable:

- Physical accidents (fire, water damage, etc.) and their origin:
  - fire caused by a short circuit within a cable,
  - fire caused internally (ashtray, secondary heating source, etc.)
- Common and less common breakdowns and the specific conditions surrounding them:
  - Common breakdowns handled by maintenance
  - Breakdowns requiring escalation
  - Etc.
- Denial of service attacks
- Equipment or software maintenance error
  - due to insufficient training
  - due to insufficient documentation
  - Etc.

Note: Including the circumstances in which a risk may occur in the risk identification process reveals - through context and the processes involved - whether a given asset element is in fact, at a given moment, particularly at risk.

The different results obtained from these three examples clearly demonstrate that beyond the words and terms used, there is a profound difference in how risk definitions are construed.

Identifying threats to an asset and the vulnerabilities that these threats can exploit to affect that asset makes it possible to characterize a given type of risk, but does not aim towards, or in any case make possible, the direct identification of "risk situations" that potentially require specific actions as part of a direct risk management process.

6 ESTIMATING IDENTIFIED RISKS

The step referred to as “risk estimation" in ISO standards actually involves risk quantification.

This step covers very different things depending on what risk management method is used.

6.1 Risk estimation for individual risk management

The goal, for each identified risk, is to evaluate the level of risk to which the entity is exposed.

It is generally agreed that the level of risk depends on two factors: impact (or how serious the consequences will be) and potentiality (or probability). To make these evaluations in a situation where security measures have already been taken, attention must also be paid to the quality of these measures.

As already stated, a risk model is a necessary pre-requisite. Different methods suggest different models, but it is nevertheless possible to list some reoccurring elements that are always necessary. These are:

- Analysis of the stakes or consequences of the risk
- Analysis of the probability that the risk scenario will occur
- Effects of security measures

6.1.1 Analysis of the stakes or consequences of the risk

Since the definition and description of the risk include that of the asset element in question as well as the type of damage, the goal is to evaluate the seriousness of this damage.

This is of course a question of method that cannot be examined in any more detail here.

We can however highlight general principles, which must be followed.

Evaluating the most serious consequences of damage

The first principle involves identifying what the most serious consequences of damage would be.

This is often done during what is called classification. Classification must include the following:

a. the creation of a scale of seriousness

One of the first things to do is establish a scale of seriousness.

The scale should express the varying levels of seriousness of different consequences (such as death or loss of the entity, lasting after-effects, temporary loss of competitiveness, etc.), in the same way we would speak about the effects of accidents on people (critical condition, permanent disability, need for ongoing care, common illness requiring a few weeks of bed rest, etc.).

In the public service sector, the level of seriousness can refer to the degree of service unavailability (in terms of duration, percentage of the population affected, etc.).

b. An evaluation of the seriousness of consequences (not of the inconvenience they cause an entity's managers)

The goal of this exercise is to evaluate how serious the consequences of risk are for the entity. The evaluation and analysis of consequences must therefore target the processes of the entity. During this analysis, it is important not to over-rate inconveniences to the entity's managers (but to correctly evaluate inconveniences to clients).

c. the approval by management of the scale of seriousness

The consequences of different risks should be evaluated at the business level by activity managers themselves, and approved by an executive committee.

Not doing this can, and generally does, result in the overestimation of certain consequences: events seen as serious by lower- and middle-ranking staff are often seen as tolerable or inconsequential by high-level management.

Because risk management is primarily the responsibility of a company's managers, it is they who should determine how serious risks really are.

Evaluating the specific consequences of an analysed risk

The evaluation described above, sometimes summarised in asset classifications, looks at the highest level of consequences faced by the entity due to a particular type of damage to a given asset element.

In certain circumstances and in the case of certain threats however, consequences may be less significant.

As a result, direct risk management methods must provide for the correction, if necessary, of the evaluation of consequences to reflect a potentially lower impact.

6.1.2 Evaluating the probability that a risk will occur

Because risk "estimation" relies in part on the likelihood that this risk will occur, it is necessary to evaluate the a priori probability of occurrence without any security measures.

Access to adequate statistical data would of course be ideal, so as to base these a priori probabilities on completely impartial and objective information.

This is rarely possible however, for various reasons:

- Agencies that collect accident- or loss-related information are reluctant to disclose it (insurance companies in particular)

- data can be biased due to the fact that not all accidents/losses are declared (particularly those that may effect the organisation's image)

- Certain accidents/losses are not even known to the victim (particularly in the case of data theft).

There is often little choice but to subjectively evaluate these a priori probabilities, noting however that:

- consensus from a working group reduces subjectivity

- existing methods may offer data that provides an adequate starting point

That said, the method used to define these a priori probabilities must be included in the risk model associated with this type of management and must include elements described below:

a. the creation of a scale of probability

One of the first things to do is establish a scale of probability.

This scale should express levels of probability that are easily understood by everyone involved in the risk analysis process.

The number of levels should be limited so that consensus can be easily reached as to the levels of probability of each threat.

b. an evaluation of the a priori probability of a risk scenario

Evaluating maximum and a priori probability, independently of security measures, will most often be associated with each category of scenario.

This will indeed apply if the method provides for a structured knowledge base. Otherwise, it is advisable to group scenarios together under similar types of probabilities. In reality, this amounts to distinguishing threats that are common to several types of scenarios.

Practically speaking, this probability often refers to the probability of a threat, independently of the specific context of the entity.

c. an evaluation of the entity's exposure to the analysed scenario

The notion of exposure (sometimes called natural exposure) is of fundamental importance. However probable the occurrence of a certain risk may or may not be in general, the important thing is to know if the entity is particularly exposed or not to this type of risk.

This exposure brings several factors into play:

- the interest this action holds for the person who carries it out

- the more or less unique character of the entity as a target of the threat

- the social context

- the economic context

It is also important to note that this exposure can fluctuate over time.

The risk management method must therefore allow for an evaluation of this exposure depending on the specific context of the entity, to ultimately define the "intrinsic potentiality" of a risk without any security measures.

6.1.3 Evaluating the effects of security measures

It is undoubtedly here that the various risk models common to this type of management can be a source of significant and distinctive help.

Nonetheless, it is a good idea to highlight certain imperative elements that must be described in detail in any risk analysis model associated with direct risk management:

- the differentiation of types of effects that security measures may have
- the integration of a certain level of quality in these measures
- the measurement of a security measure's efficiency
- the integration of the idea of "security assurance" (beyond the technical quality of a measure, how can we be sure of its actual efficiency?)
- the manner in which simultaneous effects of several security measures are integrated and combined

Differentiating types of effects that security measures may have

Security measures can have a variety of effects that must be clearly noted in the risk model to ensure accurate risk assessment.

It is important for example to distinguish between effects that reduce the probability of a risk and those that mitigate consequences.

Aside from that, other slight variations should be highlighted, including:

- the effect of deterrence
- the effect of prevention (preventing an action or the successful completion of that action)
- the effect of detection followed by prevention
- the effect of detection followed by action to mitigate consequences
- the effect of confinement to mitigate consequences
- the effect of restoration
- the effect of palliative recovery measures
- Etc.

This is not an exhaustive list, and the risk model must provide for a typology of these effects, by grouping them together if necessary, to describe the actions of security measures and allow for an individual evaluation of each risk.

Integrating a certain level of quality in security measures

Evidently, the effect(s) of a given security measure depend on the quality of that measure.

Some measures or some procedures are more effective than others, and it is important to know how to judge quality.

As a result, the risk model should include a method of evaluation.

The method of evaluation itself may or may not involve experts, but it is highly recommended that it at least rely on a knowledge base.

Measuring a security measure's efficiency

The intrinsic quality of a security measure does not in itself indicate whether the measure will effectively reduce the level of a particular risk, even if experience shows it can play a positive role in reducing this risk.

The efficiency of a measure may also depend on the type of effect as one measure may produce several effects.

Using the risk model then, a relationship must be established between the quality of a security measure and how effective it is in producing a given effect on different types of risk scenarios.

Security assurance

This notion, perfectly described by ITSEC and common criteria, aims to distinguish between the level of efficiency of a security measure and the assurance that this measure is effectively in place.

It involves a separate evaluation of the strength of a technical measure and whether it will be definitely implemented and maintained over time.

The integration of this notion into the risk model is therefore a parameter that should be examined.

The combined effects of multiple security measures

Lastly, the manner in which simultaneous effects of several security measures must be explained in the risk model for a correct evaluation of the residual level of risk when several measures are active and appropriate, which is the case most of the time.

6.1.4 Estimating levels of risk

An estimation of levels of risk must summarise partial estimations and as a minimum result in:

- an evaluation of the potentiality of a risk occurring (its probability)
- an evaluation of its impact (the seriousness of its consequences)

The risk model must of course describe the manner in which these summary values are obtained.

6.1.5 The impact of how risk is defined

Clearly, the operations described above are perfectly adapted to scenario-based definitions of risk.

If risks are defined as based on threats and vulnerabilities, it will be necessary, for each risk defined in this way, to identify all possible scenarios (incident scenarios, as defined in ISO/IEC 27005) and estimate the level of risk for each scenario. The different points developed above will be necessary then for this estimation.

A method for establishing a summary for each risk will also be necessary.

6.2 Risk estimation for global risk management

It is possible of course to use a complete risk model as described above to individually estimate each risk identified as a risk scenario and, as a result, develop a security policy and goals that are adapted to global risk management.

Here however, we will look at risks defined by a threat and an exploited vulnerability (or group of vulnerabilities).

With this representation of risk it is very important to note the partial view of risk it provides by listing only some of the vulnerabilities. By not taking into account all the security measures that may influence a level of risk, this representation makes it possible to attribute a certain value to risk (by looking at the exploited vulnerability but not the other security measures that could reduce the risk). While this value can be used to classify vulnerabilities by order of importance, it is not a full evaluation of the level of risk to which the organisation is exposed.

That said, a "relative" model for risk estimation must include several things:

- an estimation of the stakes or consequences of the risk
- an estimation of the level of the threat
- an estimation of the level of vulnerabilities listed in the description of the risk (this level could be a function of the security policy)

6.2.1 Estimating the stakes or consequences of the risk

The risk estimation must of course take into account the damage to an asset element when the risk occurs.

Since the description of the risk includes a description of the asset element in question and the type of damage it suffers (even though this damage is not referred to explicitly and must be found in the type of threat), the task at hand is to evaluate the seriousness of this damage.

This is, here again, a question of method that will not be examined here.

It is possible however to highlight the general principles to be followed. These are shaped by the fact that obtaining an absolute value of the level of risk is not the goal.

Describing a reference point for the seriousness of risk consequences

In the sense that an absolute value of risk levels is not necessary here, a reference point for seriousness can be more loosely defined.

For example, a reference point for a scale of seriousness could be:

- the real seriousness of consequences for the entity (as seen in Chapter 6.1.1)
- the inconvenience to users,
- the inconvenience to management
- the recovery costs
- any other criteria that reflect a certain order of importance of consequences (how long a service is unavailable, for example)

Defining a scale of seriousness

After the reference point, a scale must also be established.

The number of levels is relatively unimportant for this type of management; a scale with few levels will facilitate later steps in the quantification process.

6.2.2 Estimating the level of threat

The value given to a risk must of course take into account the level of threat.

The manner in which this level is evaluated must appear in the risk estimation model, and can include different parameters such as:

- The “a priori” probability that an event will occur which triggers the threat
- the destructive potential of the threat
- the entity's exposure to this type of threat, in relative terms
- the “ease of occurrence” of the threat
- Etc.

Of course, a function combining the a priori probability of occurrence with the entity's exposure to this type of threat seems the closest thing to the idea of probability. In this “relative” risk estimation however, the process of evaluating the level of threat must above all allow for good communication and be understood by decision makers. The theoretical validity of this evaluation is not of major importance, though.

6.2.3 Estimating the level of vulnerability

Lastly, the risk estimation must take into account the level of the vulnerabilities in

question, as these represent a key element in the identified risk.

The following points should be discussed and described in the management model:

- The determination of the level of each vulnerability
- The manner in which several combined vulnerabilities are accounted for and valued, if several vulnerabilities are described in the risk identification process.

Measuring the level of each vulnerability

To manage possible risks over time, even in the framework of a partial risk model, the level of vulnerability must be measured.

This evaluation can be carried out:

- subjectively
- based on a vulnerability audit and a knowledge base.

One way or another, the method must describe the evaluation process which in turn must take into account elements from the security policy.

Measuring several combined vulnerabilities

Furthermore, if several vulnerabilities are described in a type of risk, the method of globally evaluating the level of vulnerability should be described and include:

- a typology of vulnerabilities (can such different vulnerabilities as access control and back-up weaknesses be compared?),
- the way in which vulnerabilities of the same type are combined (the minimum, maximum, or another formula?),
- the way in which different types of vulnerabilities are combined.

6.2.4 Estimating the level of risk

An estimation of the level of risk must take into account all the preceding evaluations and result in a classification by order of importance of the risks described.

7 EVALUATING IDENTIFIED RISKS

The step referred to in ISO standards as “risk evaluation” actually involves judging whether a described risk is acceptable or unacceptable.

7.1 Risk evaluation for individual risk management

For this type of management, the risk estimation step leads to an evaluation of the impact (I) and the probability (P) of each risk.

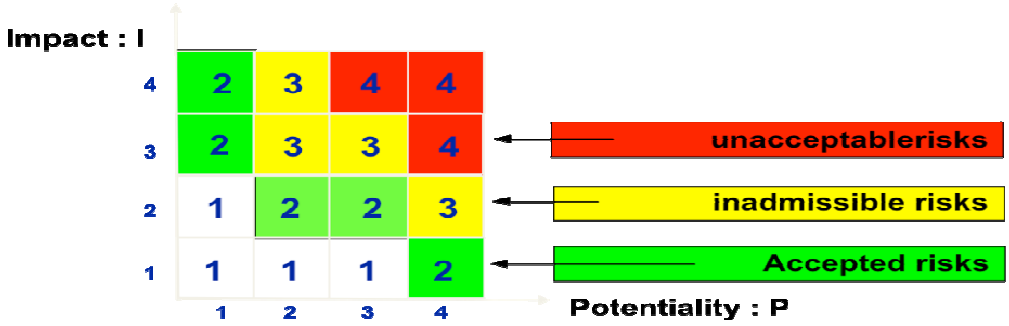
The only task remaining is to give an overall mark or, simply, to establish a range of risk acceptability.

The easily accessible nature of the two basic concepts makes it easy for management to deal with this aspect.

A possible decision-making tool could be:

- A function of Seriousness of a risk S = f(P,I)

- An acceptability table as a function of P and I, like the one below for example.



7.2 Risk evaluation for global risk management

In this type of management, evaluation leads to an overall mark according to which risks can be classified by order of importance.

The decision to treat a risk or not is made based on a cut-off limit that must be set by a special committee.

8 RISK TREATMENT

After their assesment, risks need to be treated. This means a decision about:

- accepting them as such,
- avoiding them completely due to structural changes to make the risk disappear,
- reducing them,
- transferring or sharing them with a third party.

In this section we will examine the last two options: risk reduction and the transfer of risks to a third party.

Clearly, reducing risks that are considered critical is linked to the management method that has been chosen. But it is also linked (primarily perhaps) to the actual definition of those risks.

8.1 Directly reducing critical risk situations

As its name implies, direct risk management involves deciding, on a scenario-by-scenario basis, what measures should be taken.

That said, several options are available depending on what is allowed by the risk management method. The two main options are:

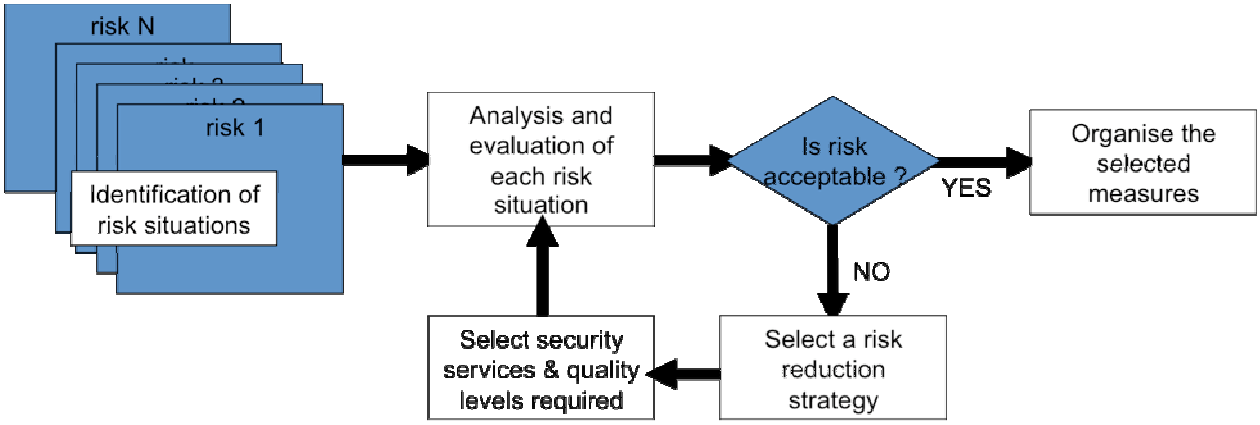
- a reliance on a risk scenario knowledge base in which appropriate security measures are referenced and which allows an evaluation of their effects in terms of reducing the level of risk ,
- direct reduction of risk situations by the managers of the activity, project or process.

8.1.1 Directly reducing risks using a knowledge base

The most interesting option is a risk scenario knowledge base in which pertinent security measures are referenced for each scenario and which allows an evaluation of the effects of these measures in terms of reducing the level of risk.

An additional element to consider is whether the risk management method offers other types of assistance, in particular a choice of risk reduction strategies, then allowing optimised decisions. Otherwise the risk manager will have to decide by himself which security measures will be implemented.

The risk management diagram given in Chapter 4.1 is thus modified to include the following:

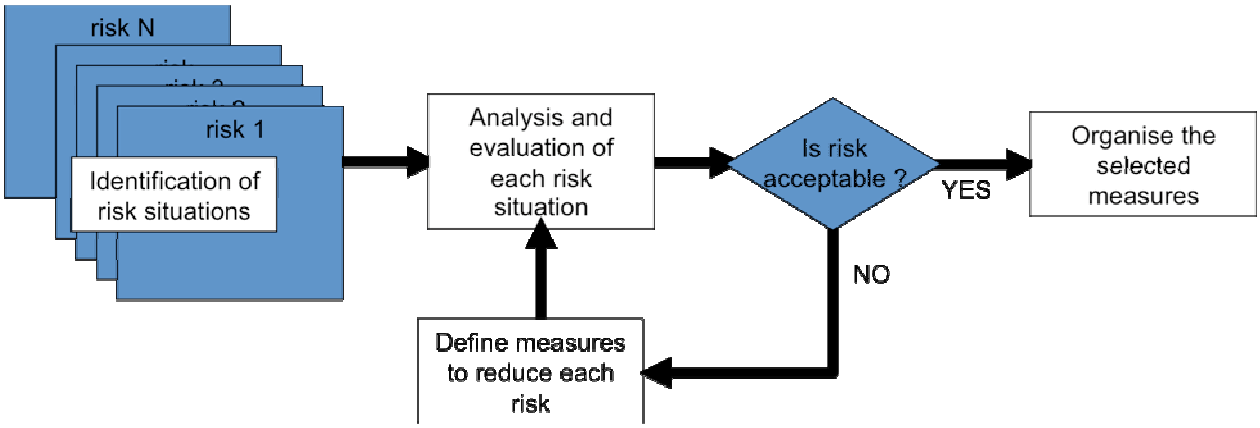


8.1.2 Direct risk reduction by the activity, project or process managers

As the circumstances in which each risk may occur are completely defined, it is possible for the activity, project or process managers to directly manage the solutions to be implemented and this often proves to be economical.

Considering the scenario of a confidential strategic document being diverted while it is printed on a shared printer. The decision could be to simply modify the process and print this same document locally on a printer that isn't shared, rather than having to secure the printing process on a shared printer.

The risk management diagram given in Chapter 4.1 is thus modified to include the following:



8.2 Indirect treatment of critical risks

In an approach where risks are defined based on threats and vulnerabilities, the objective is generally to reduce the vulnerabilities.

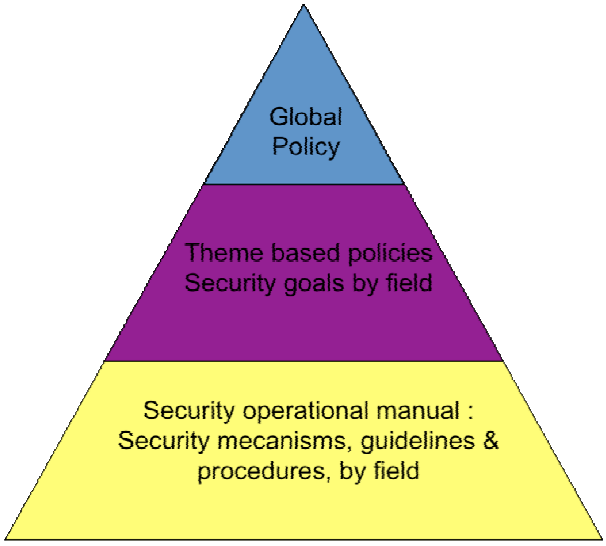
Here it is important to know what level of detail is considered with such a risk management method.

This is because decisions on how to treat risks, and possible orientations can be

linked to different levels of detail.

As indicated in the diagram below, they can be linked to:

- a global security policy that outlines broad general directions
- theme-based security policies that outline security goals to be reached concerning different security-related domains or themes
- a security operational manual that describes required mechanisms and security guidelines in detail



So, treating certain risks may consist of:

- as part of a theme-based policy, the implemention of procedures for processing and storing information in order to protect it from illicit use and dissemination at the level of security objectives (although the content and even the chapter headings of these procedures are not defined or decided at this level)

- an analysis of each element that plays a role in achieving information protection and a decision regarding each of these elements, in a security operational manual, as well as, for example: (from a non-exhaustive list suggested in the ISO/IEC 27002 standard)

    - labelling of all media based on how they are classified
    - Access restrictions
    - a continually updated list of those authorised to receive information
    - data entry and output validation controls
    - Data protection prior to publication or transmission
    - Media storage in keeping with supplier specifications
    - information publication restrictions
    - labelling media copies
    - periodical review of publication and distribution lists
    - Etc.

Two options are available for the indirect management of common risks:

- The direct transformation of vulnerabilities to be reduced into security objectives specified in theme-based policies, and the deferral to a later phase of the transformation of these security goals into practical elements of a security operational manual

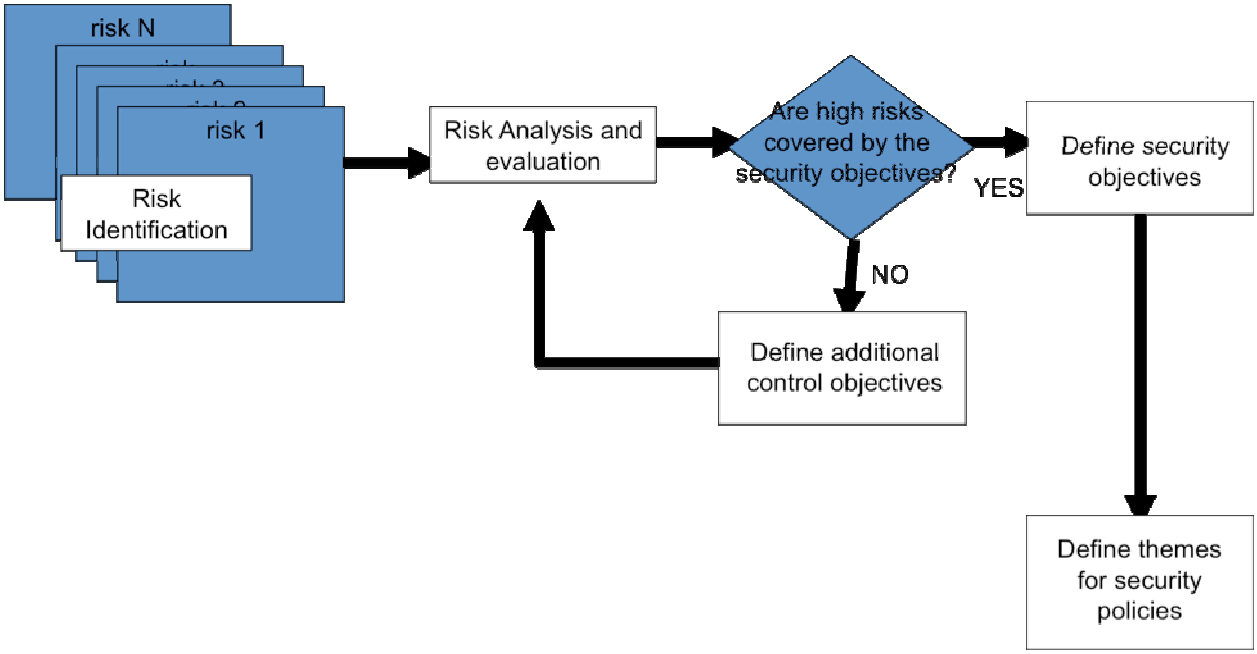
- a more detailed analysis of these vulnerabilities to determine, even this early on in the management process, which practical elements in a security operational manual should be implemented.

8.2.1 Transforming vulnerabilities into security goals

This transformation is relatively simple and does not require any specific tools; the lists of common vulnerabilities often pertain to the same level as lists of control objectives.

Note: One could imagine working with very detailed vulnerabilities, and defined at the same level as the elements of a security operational manual. This would make risk identification and analysis very complicated however by multiplying the number of vulnerabilities to be taken into account for each common risk without simplifying the way they are dealt with

The risk management diagram given in Chapter 4.2 is thus modified to include the following:



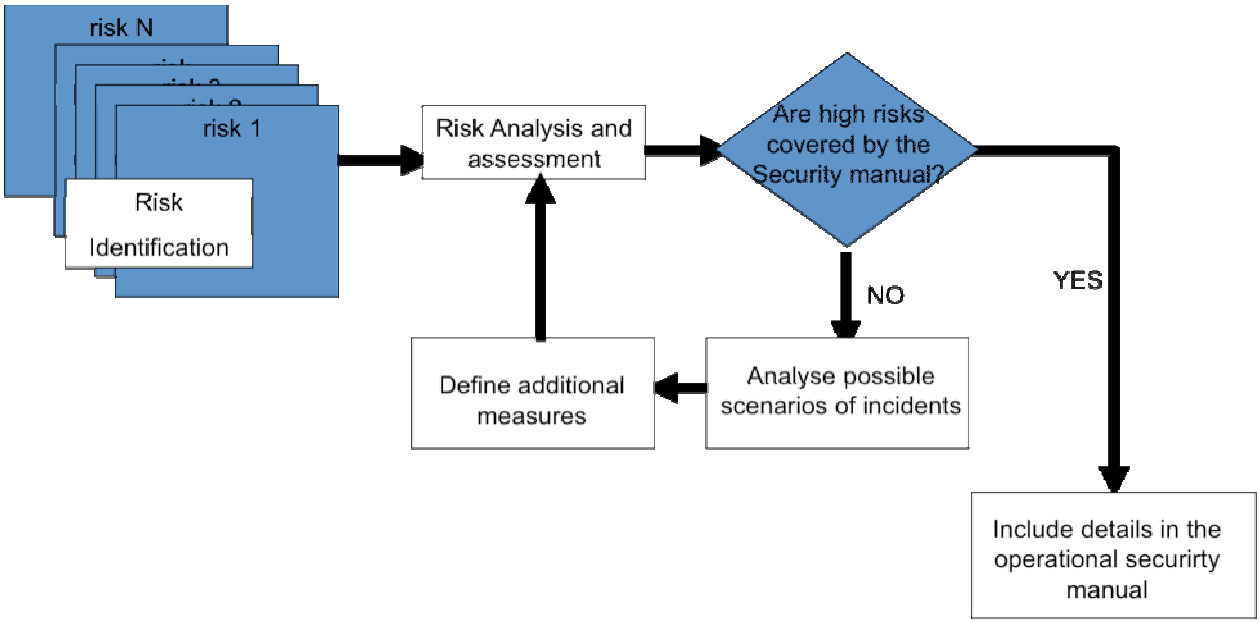
The methods relevant to this diagram are in fact security goal management methods based on an evaluation of the level of common risks that may exploit vulnerabilities not addressed by security objectives.

8.2.2 Analysing vulnerabilities to determine what elements to include in a security policy

Deciding on and implementing elements of a security operational manual requires the analysis of possible incident or risk scenarios that are compatible with the characteristics – threats and vulnerabilities – of the risk that is analysed.

Risk treatment involves looking for scenarios, choosing appropriate measures for reducing the level of risk, and including measures in the security operational manual.

The risk management diagram given in Chapter 4.2 is thus modified to include the following:



The methods relevant to this diagram are in fact methods for managing elements of the operational security manual, based on an evaluation of the seriousness level of risks resulting from incident scenarios that may exploit vulnerabilities not yet addressed by the security manual.

8.3 Risk transfer

Risk transfer most often refers to an agreement between the entity and one or more third parties to share certain responsibilities.

The most typical example is that of insurance, but many other kinds of agreements are possible.

Methods are not particularly helpful in this area and agreements should be studied and concluded on a case-by-case basis.

Often however, an in-depth analysis of risk situations is more useful and more directly applicable to transfer agreements than a study of threats and vulnerabilities.

9 RISK COMMUNICATION

Authoritative texts in the field of risk management all highlight the importance of risk-related communication.

We indeed feel that when an organisation commits to serious risk management, it is essential that there be shared knowledge and a consensus on:

- The risks that are tolerated, but they still may well occur and require action in the future,
- the risks whose reduction has been decided, allowing time for related projects to be started and to complete,
- the risks that are high and theoretically inadmissible that must be tolerated because no avoidance nor reduction solution.

This shared knowledge relies entirely on appropriate communication methods.

Regardless of communication tools, it is obvious that communicating about risk situations serves a purpose and is conducive to responsible behaviour. In contrast, communicating about threats and vulnerabilities will be harder to manage and may not be supported by the staff.

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS
30, rue Pierre Sémard
75009 Paris
✆ 01 53 25 08 80
clusif@clusif.asso.fr

www.clusif.asso.fr