MINISTERIO DE
ADMINISTRACIONES
PÚBLICAS

MAGERIT – version 2

Methodology for Information Systems Risk Analysis and Management

III – Techniques

Madrid, 20 June 2006
NIPO: 326-06-044-8
Catálogo general de publicaciones oficiales
http://publicaciones.administracion.es

PROJECT TEAM

Director:
Francisco López Crespo
Ministerio de Administraciones Públicas

Miguel Angel Amutio Gómez
Ministerio de Administraciones Públicas

Javier Candau
Centro Criptológico Nacional

External consultant:
José Antonio Mañas
Professor
Universidad Politécnica de Madrid

Index

1. Introduction

This book of techniques completes the guide to the Magerit methodology. It assumes that the concepts of risk analysis and management, as explained in the methodology guide, are already known and understood.

The aim is to describe techniques to be used in risk analysis and management projects[1]. Techniques are considered to be a set of heuristics and procedures supported by standards. It is implied that they use one, or several, specific notations for syntax and semantics and apply criteria of excellence when applied. Practices are procedures to achieve specific objectives rapidly, securely and precisely, with minimal room for the unexpected.

For each of the techniques and practices referred to below:

- there is a brief explanation of the aimed objective,
- the basic associated elements are described,
- the basic principles, on which the technique is based, are described,
- a text and/or graphic notation is presented, and
- bibliography sources deemed of interest to readers who wish to study each subject further are provided, although the list is can never be complete.

All the techniques in this book can be used without automated aids; however, for repeated or complex use, it is recommended to use tools as widely and frequently as possible.

It is important to point out that the notation proposed for applying the technique is in no case compulsory. Each organization may adapt to the available tools or sector specific notations.

1 Several of the techniques referred to have been incorporated from Métrica version 3.

2. Specific techniques

This chapter focuses on very specific techniques for risk analysis and management projects. These are techniques that are not used in other work contexts.

The following are thought to be of special interest:

1. the use of tables to derive simple results
2. algorithmic techniques to derive complex results
3. attack trees to complement the reasoning behind which threats could attack an information system

and are dealt with in the sections below.

2.1. Analysis using tables

An analysis is defined as differentiating and separating the parts of a whole until disclosing its principles or elements. Risk analysis involves working with several elements, which have to be combined into a system and put in order of importance, without the many details obscuring the vision of the whole.

Experience has proved the usefulness of simple methods of analysis using tables, which, although not very precise, certainly succeed in identifying the relative importance of the various assets subject to threat.

The following scale is a tool for grading the value of the assets, the size of the impact and the size of the risk:

- **VL:** very low
- **L:** low
- **M:** medium
- **H:** high
- **VH:** very high

Impact estimation

Impact can be calculated from simple, double-entry tables:

impact		***degradation***		
		1%	10%	100%
value	VH	M	H	VH
	H	L	M	H
	M	VL	L	M
	L	VL	VL	L
	VL	VL	VL	VL

Any assets that are graded as very high impact (VH) should receive immediate attention.

Risk estimation

The frequency is also modelled from a simple scale:

- **VF:** very frequent (daily)
- **F:** frequent (monthly)
- **NF:** normal frequency (yearly)
- **I:** infrequent (every few years)

The impact and the frequency can be combined into a table to calculate the risk:

risk		***frequency***			
		PF	FN	F	MF
impact	VH	H	VH	VH	VH
	H	M	H	VH	VH
	M	B	M	H	VH
	L	VL	L	M	H
	VL	VL	VL	L	M

Any assets that are graded as very high risk (VH) should receive immediate attention. Those graded as high risk should be subject to immediate safeguard planning.

2.1.1. References

- ISO/IEC 13335-1:2004 – Information technology – Guidelines for the management of IT security – Part 1: Concepts and models for Information and communications technology security management.

2.2. Algorithmic analysis

An analysis is defined as differentiating and separating the parts of a whole until disclosing its principles or elements

In chemical science, a qualitative analysis is used to find and isolate elements or ingredients of a compound body, unlike the quantitative analysis, which is used to decide the quantity of each element or ingredient.

Two algorithmic approaches are presented in the following sections. First, there is a qualitative model that seeks a relative valuation of the risk on the assets (what is the greatest, as opposed to what is the least?). Second, there is a quantitative model which aims to answer the questions of how much more and how much less. A step-by-step model is shown below which represents a typical assessment of impact on the availability of information systems. Finally, there is a model to calculate the impact of a package of safeguards.

2.2.1. A qualitative model

A qualitative risk analysis aims to find out what there is, without quantifying it more precisely than necessary to make relative the components of the model

This section shows a calculation model that works on a discrete scale of values.

Values

A risk analysis needs to be able to assess, relatively at least, the elements involved. Specifically, the assets, the impact of the threats and the risk run.

A scale of symbolic levels is used throughout:

$$V = \{ \ldots, v_0, v_1, \ldots, v_i, \ldots \}$$

this series of levels satisfies the following properties:

- total order: $\forall$ i, $v_i < v_{i+1}$
- there exists a special element, *"v_0"*, which is ranked as "negligible"[2].

Informally, an asset is said to have "i points" to indicate that it has been assessed as *"v_i"*[3].

The value of assets

Each asset in each dimension receives a value on the scale *V*.

The various dimensions of an analysis are not inter-related, and each asset has to have a value in each of the dimensions.

The dependency between assets

The only concern is whether asset A depends, significantly, on another asset B. In other words, dependency between assets is a Boolean value: yes or no.

$$A \rightarrow B$$

The dependency can be transitive:

$$(A \rightarrow B) \wedge (B \rightarrow C)$$

A depends on B; B depends on C.

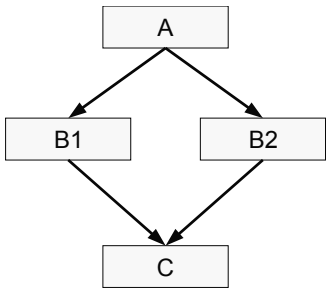
2 This negligible level establishes a subjective boundary between what can be appreciated and should give cause for concern, and what is insignificant and can be disregarded. Values below v_0 are disregarded.

3 If the reader wishes, the points on this assessment system can be interpreted as orders of magnitude, for example v_x can be read as 10^x.

It can even be represented as a diamond shape:

$(A \rightarrow B_1) \wedge (A \rightarrow B_2) \wedge (B_1 \rightarrow C) \wedge (B_2 \rightarrow C)$

A depends on B1 and B2; B1 and B2 depends on C.



The transitive closure of direct dependencies between assets is of interest.

$A \Rightarrow C \Leftrightarrow \exists B, (A \Rightarrow B) \wedge (B \rightarrow C)$

A depends (indirectly) on C if and only if
there is an asset B, so that A depends directly or indirectly on B and
B depends directly on C.

The following does not differentiate between direct and indirect dependencies.

The accumulated value

Let SUP(B) be the unit of assets higher than B, i.e. the set of assets that depend directly or indirectly on B:

$SUP(B) = \{ A_i , A_i \Rightarrow B \}$

The accumulated value over B is defined as the highest value among B and any ones above:

$accumulated\_value(B) = \max (value(B), \max_i \{value(A_i)\})$

The above formula states that the accumulated value on an asset is the highest of the values included, either of itself, or any one above it.

The degradation [of the value] of an asset

When an asset falls prey to a threat, it loses part of its value. A subjective "percentage of degradation of the asset" is given, which may be between 0% and 100%. *"d"* is set as a real value between 0.0 (0% degradation) and 1.0 (100% degradation).

The accumulated impact of a threat on an asset

This is the measurement of what a threat involves; in other words, it is the accumulated loss of value. If an asset has an accumulated value of *"v_x"* and it is degraded by a percentage *"d"*, the value of the impact will be

$impact = v_{round(x \times d)}$

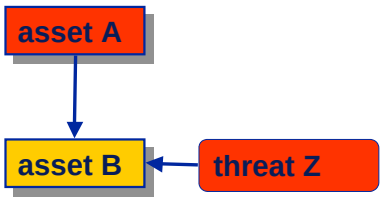
Example

If an asset is valued at *"v_8"* and it degrades by *90%,* the impact will be *"v_7":*

$round(8 \times 0.9) = round(7.2) = 7$

When the impact is reduced to *"v_0"*, it is said to be negligible.

The defected impact of a threat on an asset



If asset A depends on asset B, threats to B will affect A. If B undergoes a degradation *"d"*, this will also occur on A, with the impact on A being the loss of the basic value. If the value of A is *"v_x"*, the impact is:

$$impact = v_{round(x \times d)}$$

> **Example**
>
> If A has a value of *"v_5"* and depends on B (whose value is not of interest here) which degrades by *20%*, the deflected impact on A will be *"v_1":*
>
> $$round(5 \times 0.2) = round(1.0) = 1$$

When the impact is reduced to *"v_0"*, it is said to be negligible.

The frequency of threats

The frequency of threats is described on a scale of symbolic values:

$$F = \{ ..., f_0, f_1, ..., f_i, \dots \}$$

In other words, a series of frequency levels which are the elements or particles of analysis.

This series of levels complies with the following properties:

- total order: $\forall\ j, f_j < f_{j+1}$
- there is a separate element, *"f_0"*, referred to as "negligible frequency"
- there is a separate element *"f_n"*, referred to as "normal frequency"[4]

Informally, it is said that a threat has "j frequency points" to show the frequency as *"f_j"*.

The risk

Risk is measured by the scale of values, being a function of the impact and the frequency:

$$risk = \Re(impact, frequency)$$

a function that has to be defined in line with the following requirements:

- it grows with the value: $\forall\ f_i, \Re(v_i, f_j) < \Re(v_{i+1}, f_j)$
- it grows with the frequency: $\forall\ v_i, \Re(v_i, f_j) < \Re(v_i, f_{j+1})$
- $\Re(v_0, f_n) = v_0$

A simple function that satisfies these properties is

$$\Re(v_i, f_j) = v_{i+j-n}$$

When the value of risk is *"v_0"* (or less) it is regarded as negligible.

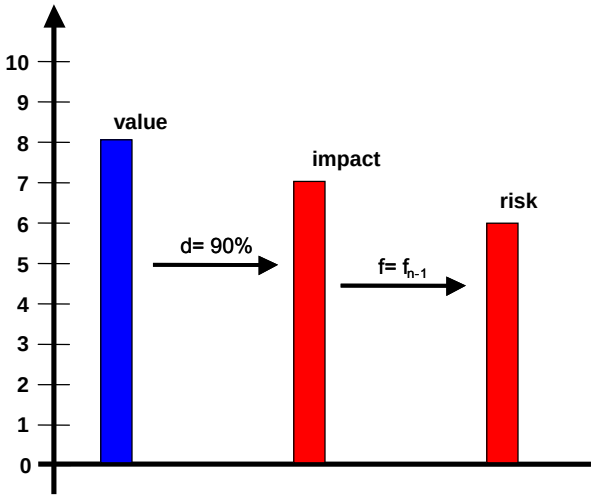
4 If a yearly study is to be made, f_n refers to "once a year".

Example

If an asset has a value of *"v_8"* and it degrades by *90%,* the impact will be *"v_7":*

round(8×0.9) = round(7.2) = 7

If the estimated frequency for the threat is *"f_2"*, and *"f_3"* is considered the normal frequency, then the risk will be *"v_6"*.



The accumulated risk

When calculating accumulated risk, the accumulated

The deflected risk

When calculating the deflected risk, the deflected im

Safeguard packages

When a threat is in force, a series of safeguards is implemented, a safeguard package, whose efficiency, *"e",* is calculated as shown below. For now, it is sufficient to say that efficiency is a real value between 0.0 (no protection) and 1.0 (fully efficient safeguard), a value that can be broken down into efficiency against impact, *"e^i",* and efficiency against frequency *"e^f".*

The residual degradation

If the asset was subject to a degradation "d", safeguards will reduce this degradation to a residual value "dr":

$$dr = d \times (1-e^i)$$

where *"e^i"* measures the effectiveness of safeguards to reduce the degradation of this asset (that is, limiting the impact). The value ranges between:

- *e^i= 0* y *dr= d,* when safeguards have no effect
- *e^i= 1* y *dr= 0,* when safeguards are perfect

Example

If an asset has been degraded by 66% (that is, by 2/3 of its value), but the safeguards are 90% efficient, residual degradation is 7%:

$$dr = 0.66 \times (1-0.9) = 0.07$$

The residual impact

Residual impact is calculated in the same way as the impact, but using residual degradation:

$$residual\_impact = v_{round(x \times dr)}$$

A package of safeguards that is fully efficient reduces the impact to a residual value *"v_0",* that is, to negligible levels. If the safeguards are not strong enough, the impact will continue to be perceived.

The accumulated residual impact is calculated on the accumulated value.

The deflected residual impact is calculated on the basic value.

The residual frequency

As with the impact, the frequency of the threat on the asset is reduced to a residual value. If the frequency was *"f_j",* it is now:

$$residual\_frequency = f_k \qquad \text{where } k = round(j \times (1 - e^f))$$

With *"e^f"* being the efficiency of the safeguards mitigating the frequency of occurrence of the threat. *"e^f"* is a value between 0.0 (0% efficiency, i.e. unusable) and 1.0 (100% efficiency, i.e. perfect).

The residual risk

This is the risk calculated from the residual frequency and impact:

$$residual\_risk = \Re(residual\_impact, residual\_frequency)$$

The residual accumulated risk is evaluated using the residual accumulated impact.

The residual deflected risk is evaluated using the residual deflected impact.

Example

Supposing an asset A with a value of *"v_5"*, which depends on another asset B with a value of *"v_8"*.

Supposing a threat to asset B that degrades it by 90%, with an estimated frequency of *"f_2"*, with *"f_3"* being the normal frequency.

A package of safeguards is deployed in the system which reduces the impact by 50% and the frequency of occurrence by 50%.

The calculations provide the following indicators:

for A	**for B**
accumulated value: v_5	accumulated value: $v_5 + v_8 = v_8$
deflected impact: v_4	accumulated impact: v_7
deflected risk: v_3	accumulated risk: v_6
residual degradation: *45%*	residual degradation: *45%*
residual impact: v_2	residual impact: v_3
residual frequency: f_1	residual frequency: f_1
residual risk: v_0	residual risk: v_1

Summary

This is the qualitative model, where the assets have been placed on a scale of relative value by defining an arbitrary value *"v_0"* as drawing the line between values of concern and those that are negligible.

On this scale of value, measurements are taken both of the basic or accumulated value of the asset and the impact of a threat when it occurs and the risk to which it is exposed.

While the impact measures the value of the potential problem, the risk weights this impact with the estimated frequency at which the threat may occur. The impact is the measure of the cost if the problem should occur, while the risk measures the exposure during a specific period of time.

Estimations of the impact and residual risk include the efficiency of the safeguards to deal with the threat, either by limiting the impact, *"e^i"*, or by reducing the frequency, *"e^f"*.

Therefore, the model combines the following analysis parameters:

- rating the value of the asset through a discrete scale
- rating the degradation posed by a threat as a percentage
- rating the frequency at which a threat occurs through a discrete scale
- the integration of a package of safeguards
- rating the efficiency of the safeguards through a percentage

All these parameters allow for upward or downward movement on the scale of values.

2.2.2. A quantitative model

A quantitative risk analysis seeks to find out what there is and to what extent, by quantifying all

possible aspects.

The following model does not function on a scale of discrete values, but with real positive numbers (in a mathematical sense).

The value of assets

The value of an asset in a specific dimension is a real value higher than zero.

A specific value, *"v_0"*, is set as the boundary between the negligible values and those that are relevant.

The dependency between assets

It must be established whether asset A depends on asset B, and to what extent. The concepts of direct or indirect dependency stated in the qualitative model are applied, but now the dependency is rated by a coefficient between 0.0 (independent assets) and 1.0 (assets with absolute dependency). This coefficient is called the degree of dependency.

As the dependency can be direct or indirect, it is calculated on the basis of the transitive closure of the direct dependencies between assets.

$$A \Rightarrow C \Leftrightarrow \exists\ B,\ (\ A \Rightarrow B\ ) \wedge (\ B \rightarrow C\ )$$

A depends (indirectly) on C if, and only if, there exists an asset B so that A depends directly or indirectly on B, and B depends directly on C.

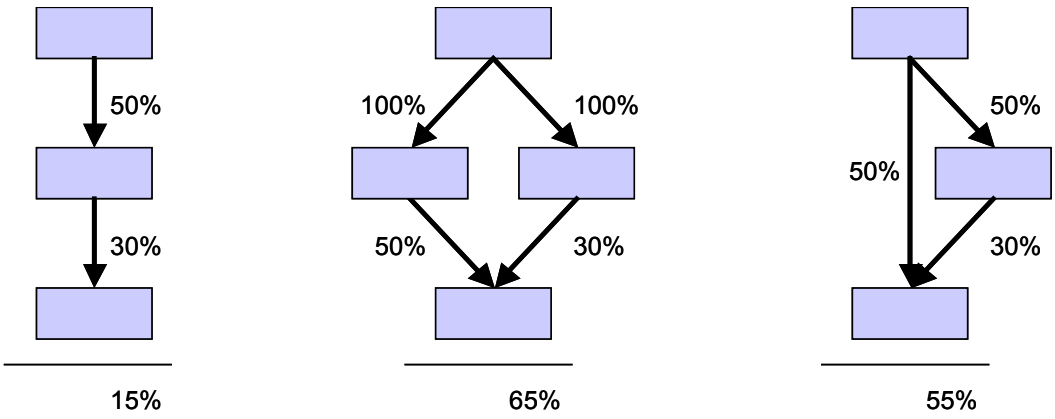
By calculating the degree of dependency as:

$$\text{degree}(A \Rightarrow C) = \sum_i \{\ \text{degree}\ (A \Rightarrow B_i) \times \text{degree}\ (B_i \rightarrow C)\ \}$$

Where the sums are carried out following this formula:

$$a + b = 1 - (1 - a) \times (1 - b)^5$$

Examples



The following does not differentiate between direct or indirect dependencies.

The accumulated value

Let SUP(B) be the unit of assets higher than B, i.e. the set of assets that depend directly or indirectly on B:

$$SUP(B) = \{\ A_i\ ,\ A_i \Rightarrow B\ \}$$

5 This addition satisfies the commutative, associative properties and the existence of a neutral element, in addition to containing the result within the range [0..1] if the addends are within this range.
The choice of this peculiar formula, taken from the Bayes calculation of probability, arises from the need to reflect the fact that, if an asset depends on another through various routes (diamond structures), the total dependency cannot exceed 100%.

The value accumulated on B is defined as the (traditional) sum of the values of the higher assets, weighted by the degree of dependency:

$$\text{accumulated\_value}(B) = \text{value}(B) + \sum_i \{ \text{value}(A_i) \times \text{degree}(A_i \Rightarrow B) \}$$

The degradation [of the value] of an asset

When an asset falls prey to a threat, it loses part of its value. A subjective "percentage of degradation of the asset" is given, which may be between 0% and 100%. *"d"* is set as a real value between 0.0 (0% degradation) and 1.0 (100% degradation).

The accumulated impact of a threat on an asset

This is the loss of accumulated value. If an asset has an accumulated value *"v"* and undergoes a degradation *"d",* the impact is

$$\text{impact} = i = v \times d$$

Example

If an asset is valued at 1,000,000 and undergoes a degradation of 90%, the accumulated impact amounts to 900,000.

When the impact is reduced to *"v_0",* or less, the impact is said to be negligible.

The deflected impact of a threat on an asset

If asset A depends on asset B, the threats on B affect A. If B undergoes a degradation *"d",* A loses by the proportion of its dependence on B. If asset A has a basic value *"v",* the impact is

$$\text{impact} = v \times d \times \text{degree}(A \Rightarrow B)$$

Example

Suppose there is asset A valued at 1,000,000, which has a 30% dependency on another asset B (whose value is not important here). If B falls prey to a threat that degrades it by 90%, A undergoes a deflected impact of the amount

1,000,000 x 90% x 30% = 270,000

When the impact is reduced to *"v_0",* or less, the impact is said to be negligible.

The frequency of threats

The frequency of a threat is a real value higher than zero.

A value of *"f_0"* is set as a "negligible" frequency, below which the threat is not considered to be of consequence.

The risk

The risk is calculated as

$$\text{risk} = \text{impact} \times \text{frequency}$$

This is a real value, higher than zero.

A threshold "r_0" is set below which the risk is "negligible", that is:

$$r_0 = v_0$$

Example

Supposing there is an asset valued at 1,000,000, which has fallen prey to a threat that has degraded it by 90%. The impact is of the amount

1,000,000 x 90% = 900,000

If the asset is exposed to the threat at an estimated frequency of 0.1, the estimated risk is of the amount

900,000 x 0.1 = 90,000

If the values are in euros and the frequency measures yearly occurrences (i.e., if 0.1 signifies once every 10 years), then the possible loss in value is 900,000 euros, while the annual loss is forecast at 90,000 euros.

The accumulated risk

When calculating the accumulated risk, the accumulated impact on the asset is used, i.e. the loss in accumulated value due to threats to the asset.

The deflected risk

In order to estimate the defected impact, the deflected impact shall be used; that is, the loss of its own value due to tretas on assets below.

Safeguard packages

When faced with a threat, a series of safeguards, the safeguard package, is deployed, whose efficiency, *"e",* is calculated as shown below. For now, it is sufficient to say that the efficiency is a real value between 0.0 (no protection) and 1.9 (safeguard fully effective), a value that can be broken down into efficiency against impact, *"e^i",* and efficiency against frequency *"e^f",* so that

$$(1 - e^i) \times (1 - e^f) = 1 - e$$ [6]

The residual degradation

This is the part of the degradation that the efficiency of the safeguard package in use does not succeed in counteracting.

The residual impact

A completely inefficient system of safeguards ($e^i = 0$) leaves the impact where it was, while a fully efficient system of safeguards ($e^i = 1$) reduces the impact to 0. In calculation form:

residual_impact = impact x $(1 - e^i)$

Example

Supposing there is an asset valued at 1,000,000, which has fallen prey to a threat that has degraded it by 90%. The impact is of the amount

1,000,000 x 90% = 900,000

If the safeguards are 90% efficient on the impact, the residual impact is

900,000 x (1 – 0.9) = 90,000

The accumulated impact is calculated from the data of the accumulated impact on an asset and the proper safeguards against threats on the asset.

The deflected impact is calculated from the data of the deflected impact on the higher value asset

6 The chosen formula has the following properties. If e^i= 0% and e^f= 0%, e= 0%. If e^i= 0%, e= e^f. If e^f= 0%, e= e^i. If e^i or e^f= 100%, e= 100%. Therefore, the results increase with the components e^i and e^f, while at the same time remaining within the range [0%..100%].

and the proper safeguards against threats to the lower value asset.

The residual frequency

A system of completely inefficient safeguards ($e^f = 0$) leaves the frequency in the same position, while a fully efficient system of safeguards ($e^f = 1$) reduces the frequency to 0. In calculation form:

residual_frequency = frequency x $(1 - e^f)$

The residual risk

This may derive indirectly as

residual_risk = residual_impact x residual_frequency

Example

Supposing there is an asset valued at 1,000,000, which has fallen prey to a threat that has degraded it by 90%. The impact is of the amount

1,000,000 x 90% = 900,000

If the estimated frequency is 0.1, the risk amounts to

900,000 x 0.1 = 90,000

If the safeguards are 90% efficient on the impact, the residual impact is

900,000 x (1 – 0.9) = 90,000

If the safeguards are 50% efficient on the frequency, the residual frequency is

0.1 x (1 – 0.5) = 0.05

The residual risk is

90,000 x 0.05 = 4,500

The combined efficiency of the safeguards is

1 – (1 – 90%) x (1 – 50%) = 95%

If the amounts are in euros and the frequencies are yearly, the possible loss is 90,000 euros and the annual loss is estimated at 4,500 euros.

Summary

This is the quantitative model and functions with real values that are always higher than zero.

The degree of dependency between assets is modelled as a continuum between 0.0 (independent assets) and 1.0 (fully dependent assets; any incident on the lower one has a severe effect on the higher one).

The value of the asset, basic or accumulated, is measured, as well as the impact of the threat whenever it occurs and the risk involved.

While the impact measures the value of the potential problem, the risk weights the impact with the estimated frequency at which the threats will occur. The impact measures the cost, should the threat occur, while the risk is the measure of exposure over a period of time.

If the asset is valued in economic terms (the monetary cost entailed by its complete loss), the calculated impact is the cost deriving from the threat, and the calculated risk is the amount which has to be planned for as annual losses. Therefore, the quantitative model allows a comparison between the cost of safeguards and the reduction of losses.

The estimations of impact and residual risk incorporate the efficiency of the safeguards when dealing with a threat.

If the valuation of the asset is economic, the quantitative model allows a comparison between the cost of the safeguards and the reduction in losses.

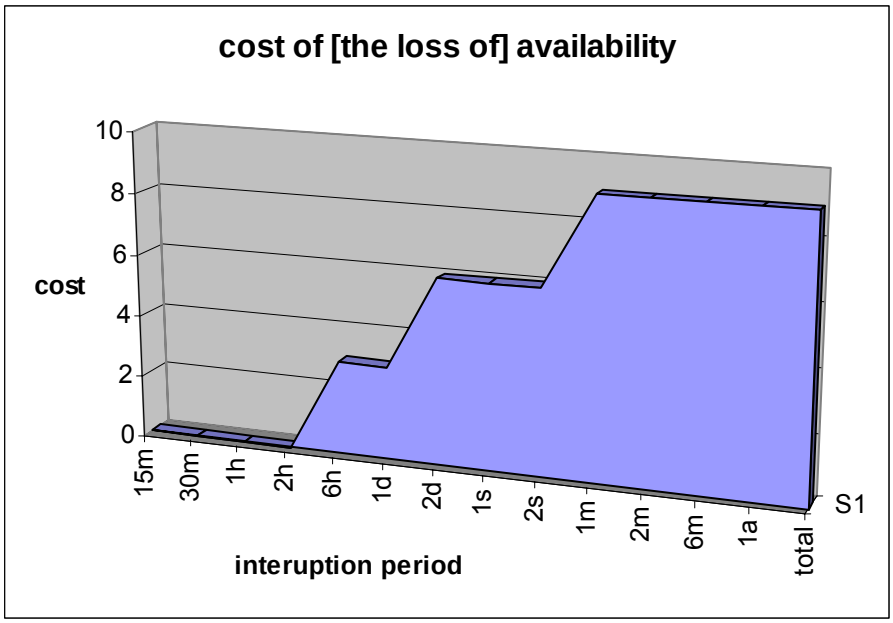
Therefore, the model combines the following analysis parameters:

- rating of the value of the asset through a numerical quantity
- rating of the dependency between assets through a percentage
- rating of the degradation posed by a threat through a percentage
- rating of the frequency at which a threat occurs through a frequency
- the integration of a package of safeguards
- rating of the efficiency of the safeguards through a percentage

All these parameters can be moved up and down the scale of values.

2.2.3. A model using steps

Sometimes, value degradation is best described as a series of [increasing] degradation steps. A typical case would be the interruption of services, as depicted below:



where cost of interruption grows up to a maximum limit corresponding to the thorough destruction of the asset (no remaining value).

The following sections show how to analyse these steps, either qualitatively (discrete scale of values) or quantitatively (continuous values).

The steps

An ordered series of value steps is determined:

$$E = \{ e_1, e_2, ..., e_n \}$$

Each step represents an interruption period (see the above diagram).

The value of the assets

Assets are assigned a value for each of the steps

$$v[e_i]$$

a value that can be qualitative or quantitative, depending on the type of analysis being made; however, the series must be monotonically growing:

$$v[e_1] \leq v[e_2] \leq \ldots \leq v[e_n]$$

Dependencies between assets

These will be treated either qualitatively (there is, or there is no, dependence), or quantitatively (there is a certain degree of dependence), as required.

Accumulated value

This is calculated independently (in parallel) for each step.

This means that an actual value and an accumulated value are calculated for each step.

Example

An administration unit provides a claims service that has traditionally been carried out via mail: the claimant sends in the claim by letter and is answered within the maximum period of 1 week. Currently, an alternative, online service has been set up with a reply given in less than 1 hour (during attendance hours), which is considered excellent. After one hour, the image offered to the public starts to suffer. If the service takes more than one day, it is considered useless, even though the seriousness is relative, as there is always the option of claiming by post.

Both services depend on computer equipment holding the data of both services:

asset	*1hr*	*1day*	*1wk*	
letter	[0]	[0]	[8]	
web	[3]	[5]	[5]	
server	[3]	[5]	[8]	accumulated

The degradation [of the value] of an asset

When a threat occurs, it stops the service for a given period, modelled as a step value *"e_i".*

The impact of a threat on an asset

It is the value corresponding to the degradation step, *"v[e_i]".*

To estimate the accumulated impact, the accumulated value (for the referenced step) will be used.

To estimate the deflected impact, the own value of the upper asset (for the referenced step) will be used. For a quantitative analysis, use that value times the dependency factor.

Example

In the previous example, a computer virus causes a 48-hour stoppage. The impact on the server is [5], the same as for the web service. The deflected impact on the postal service is [0].

The frequency of a threat

The qualitative or quantitative model is used, as required.

The risk posed by a threat to an asset

The qualitative or quantitative model is used, as required.

The efficiency of a safeguard on the impact

A safeguard against the interruption of a service is based on a reaction time, which measures how long it takes to resume service.

The efficiency of a safeguard is measured by taking the step corresponding to the time of "guaranteed reply"[7].

7 The reasoning is as follows. If a stop of longer than x1 hours involves damage of v1, and a stop of longer than x2 hours, damage of v2; then a stop of x hours, being x1 …≤ x < x2, means damage of v1, given that it has not reached the level of x2.

Example

In the above case, an anti-virus system can be used that will enable the service to be resumed in 6 hours. The efficiency is said to be on the 6-hour step.

The efficiency step may be e_0, if the safeguard is so effective that it does not allow even the first step e_1.

This efficiency step is the same as the degradation when the safeguard is unable to reduce the impact[8].

This efficiency step can never be higher than the degradation step, as a safeguard cannot worsen the situation of an asset under threat.

In addition to the efficiency step, the safeguards applied to the case constitute a package characterised by their efficiency in reducing the impact, e^i, and their efficiency in reducing the frequency, e^f. How to calculate these coefficients is described below.

What must be shown, however, is how to calculate the effectiveness step for a package of safeguards:

step(ps)=	step(s)	if s is separate
	$\max_k$ { step(ps_k) }	if ps= all (ps_k)
	$\min_k$ { step(ps_k) }	if ps= some (ps_k)
	$\min_k$ { step(ps_k) }	if ps= one (ps_k)

Where the special value *"na"*[9] behaves as a neutral element in the operations.

Therefore, a set of alternative safeguards must contain at least one that will be effective. In a set of concurrent safeguards, efficiency is rated by the worst of these.

Residual degradation

If the unprotected asset is positioned on degradation step *"e_d"*, the safeguards will place it on the step proposed as efficiency step, *"e_s";* but modulated by efficiency *"e^i"* against the impact, resulting in a residual step *"e_r":*

$$r = \lfloor d - ((d - s) \times e^i) \rfloor$$ [10]

Where the special value "na" is assessed at 0.

Residual impact

This is the value corresponding to the residual step:

$$residual\_impact = value[e_r]$$

Example

In the case above, if an antivirus system is deployed that enables service to be resumed in 6 hours, the residual impact on the server and Internet service is [3].

If an antivirus system is deployed that guarantees service to be resumed in 30 minutes, the residual impact will be [0].

Residual frequency

The qualitative or quantitative model is used, as necessary.

8 A back-up centre that starts up after 48 hours is useless against threats that stop the service for 6 hours.
9 na: not applicable.
10 Notation $\lfloor v \rfloor$ stands for the integer floor of the value.

Residual risk

The qualitative or quantitative model is used, as necessary, based on the residual impact and residual frequency.

2.2.4. On the efficiency of safeguards

All the models require an assessment of the efficiency of the safeguards deployed to protect an asset from a threat. Below is described a common model for assessing the efficiency of a set of safeguards applied to an asset.

Package of safeguards

When a threat appears, a package of safeguards is deployed which is simply a set of separate safeguards accumulated over an asset. The various safeguards can be accumulated concurrently (all are needed to produce the desired effect), or exclusively (only one of the set produces an effect) or additively (the more, the better).

```
ps::= safeguard
    | all(ps0, ps1, ...)
    | some (ps0, ps1, ...)
    | one (ps0, ps1, ...)
```

The efficiency of a safeguard

Each safeguard is valued according to its efficiency in reducing the risk to the asset it is protecting. The efficiency of a package of safeguards is a real number between 0.0 and 1.0:

- if a safeguard is perfect (100% efficient), then *e = 1*
- if a safeguard is insufficient, then *e < 1*
- if a safeguard is useless, then *e= 0*
- if a safeguard is not suitable for the context, then *e = na*

The efficiency of the safeguard depends on its natural capacity to protect the asset and on how it is deployed. The value of the efficiency unites both aspects into a single parameter.

The efficiency of a package of safeguards

e(ps)=	e(s)	if it is separate
	avg_k { e(ps_k) } [11]	if ps= all(ps_k)
	min { 1,0, Σ_k e(ps_k) }	if ps= some (ps_k)
	max_k { e(ps_k) }	if ps= one (ps_k)

Where the special value *"na"* behaves as a neutral element in the operations for calculating the maximum, product or sum.

As a result, the efficiency of a package of concurrent safeguards is the average of these; the efficiency of a package of additive safeguards is accumulated to a limit of 100%; and in a package of alternative safeguards, the efficiency is set by the best one.

Weighted efficiency of a package of safeguards

The average value of the efficiency of the components is taken as the efficiency of a package of safeguards. This calculation can be modulated if it is remembered that not all safeguards are of the same type, by introducing a weighting *"p":*

11 The average value is calculated as usual: efficiencies other than NA are added and divided by the number of addends.

$$e(ps) = \Sigma_k\, e(ps_k) \times p_k \;/\; \Sigma_k\, p_k$$

If all the safeguards should have the same importance, then *"p = 1".*

Efficiency against impact and the frequency of a threat

Risk combines impact and frequency. A safeguard can reduce the impact, or the frequency, or both. It depends on the type of safeguard acting on the impact or the frequency.

Consequently, in the above sections, a difference can be made between efficiency that reduces the impact, *"e^i",* and the efficiency that reduces the frequency *"e^f".* Both of these are calculated using the same criterion: fulfilment of the task. Finally, the efficiency can be calculated by reducing the risk, *"e",* as

$$(1 - e^i) \times (1 - e^f) = 1 - e$$

2.3. Attack trees

This section is only available in Spanish.

References

- J. Viega et al., “Risk Analysis: Attack Trees and Other Tricks”, Software Development Magazine, August 2002.
- A.P. Moore et al., “Attack Modeling for Information Security and Survivability”, Software Engineering Institute, Carnegie Mellon University, Technical Note CMU/SEI-2001-TN-001, 2001.
- B. Schneier, “Secrets and Lies: Digital Security in a Networked World”, John Wiley & Sons, 2000.
- B. Schneier, “Attack Trees: Modeling Security Threats”, Dr. Dobb's Journal, December 1999.

3. Generic techniques

This chapter deals with general techniques that are widely used, but that also apply to some stages of a risk analysis and management project. It is shown where do they apply, and how. This section builds on the methodology explanations.

The following techniques are referenced:

1. cost-benefit analysis
2. data flow diagrams (DFD)
3. process diagrams (SADT)
4. graph techniques
5. project planning (PERT)
6. working sessions
7. the Delphi method

3.1. Cost-benefit analysis

This section is only available in Spanish.

References

- R.A. Brealey and S.C. Myers, “Principles of Corporate Finance”, Mcgraw-Hill College; 6th edition, December 2000.
- A.E. Boardman, “Cost-Benefit Analysis: Concepts and Practice”, Prentice Hall, 2nd Edition, October 2000.
- H.M. Levin and P.J. McEwan, “Cost-Effectiveness Analysis Methods and Applications”, Sage Publications, Inc., 2nd edition, September 2000.
- Office of The Deputy Chief Information Officer, “Cost-Benefit Analysis Guide for NIH IT Projects”, Revised May, 1999.
- Office of Management and Budget, Circular No. A-94 Revised, “Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs”, October 29, 1992.

3.2. Data flow diagrams (DFD)

This section is only available in Spanish.

References

- S.W. Ambler, “The Object Primer. Agile Model Driven Development with UML 2”, Cambridge University Press, 3rd ed. 2004.
- C.P. Gane and T. Sarson, “Structured Systems Analysis: Tools and Techniques”, Prentice Hall, 1st ed. 1979.

3.3. Process diagrams

This section is only available in Spanish.

References

- Clarence G. Feldmann, “The Practical Guide to Business Process Reengineering Using IDEF0”, Dorset House Publishing Company, 1998.
- Hill, S. and L. Robinson, “A Concise Guide to the IDEF0 Technique”, Enterprise Technology Concepts, 1995.
- FIPS 183: “Integration Definition for Function Modeling (IDEF0)”. Federal Information Processing Standards. December, 1993.
- David A. Marca and Clement L. McGowan, “SADT: Structured Analysis and Design Techniques”. McGraw-Hill, New York, NY, 1988.

3.4. Graph techniques

This section is only available in Spanish.

3.5. Project planning

This section is only available in Spanish.

References

- R. Burke, “Project Management: Planning and Control Techniques”, John Wiley & Sons; 3rd edition. May 16, 2001.
- J.J. Moder, C.R. Phillips, E.W. Davis, “Project Management With Cpm, Pert & Precedence Diagramming”, Blitz Publishing Company; 3rd edition. February, 1995.
- K. Lockyer, J. Gordon, “Project Management and Project Network Techniques”, Trans-Atlantic Publications; 6th edition. December 1, 1995.
- R.D. Archibald, R.L. Yilloria, “Network-based Management Systems”, (Information Science S.) John Wiley & Sons Inc. March, 1967.

3.6. Working sessions

This section is only available in Spanish.

3.6.1. Interviews

This section is only available in Spanish.

3.6.2. Meetings

This section is only available in Spanish.

3.6.3. Presentations

This section is only available in Spanish.

References

- “Managing Information Security Risks: The OCTAVE Approach”, C.J. Alberts and A.J. Dorofee, Addison-Wesley Pub Co; 1st edition (July 9, 2002)
  http://www.cert.org/octave/
- Magerit, “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”, MAP, versión 1.0, 1997
  http://www.csi.map.es/csi/pg5m20.htm

3.7. The Delphi method

This section is only available in Spanish.

References

- J. Fowles, “Handbook of Futures Research. Westport, Greenwood Press, 1978.
- H.A. Linstone and M. Turoff (eds), “The Delphi Method: Techniques and Applications”, Reading, MA: Addison-Wesley Publishing Company, 1975.
- N.C. Dalkey, “The Delphi Method: An Experimental Study of Group Opinion”, RAND Corporation, RM-5888-PR, 1969.
- O. Helmer, “Analysis of the Future: The Delphi Method”. RAND Corporation Technical Report, P-3558, March 1967.
- N. Dalkey and O. Helmer, “An Experimental Application of the Delphi Method to the Use of Experts”. Management Science, vol. 9, no. 3, April 1963.
- M. Girshick, A. Kaplan and A. Skogstad, “The Prediction of Social and Technological Events”. Public Opinion Quarterly, Spring 1950.