MINISTERIO DE
ADMINISTRACIONES
PÚBLICAS

MAGERIT – version 2

Methodology for Information Systems Risk Analysis and Management

Book I – The Method

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

Contents

1. Introduction to Magerit

The CSAE[1] prepares and promotes Magerit[2] in response to the perception that the government (and, in general, the whole society) increasingly depends on information technologies for achieving its service objectives. The purpose of Magerit is directly related to the generalised use of electronic, computerised and telematic media, which bring evident benefits for the public but which is also subject to certain risks that must be minimised with security countermeasures that generate confidence in the use of these media.

Since Magerit was first published in 1997, risk analysis has been consolidated as a necessary step for security management, as clearly recognised in the OECD guidelines[3], which state in principle 6:

> *6) Risk evaluation. The participants must carry out risk evaluations.*

This methodology is of interest to anyone working with mechanised information and the computer systems that handle it. If this information, or the services that are provided thanks to it, are of value, this methodology will allow them to know how much of this value is at risk and will help them to protect it.

Knowing the risks to which working elements are subject is simply essential to be able to manage them. This fact has given rise to a large number of informal guides, methodical approaches and support tools, all of which aim at an objective analysis to know how safe (or unsafe) systems are. The great challenge of all these approaches is the complexity of the problem they face, a complexity in the sense that there are many elements to be considered and that, if they are not rigorous, the conclusions will be unreliable. This is why a methodical approach is required that leaves no room for improvisation and does not depend on the whim of the analyst.

Even though serious responsibilities for complying with the organisation's objectives have been placed in the hands of information systems, doubts about their security continue to arise. Those affected, often not technicians, wonder if they can place their trust on these systems. Each failure lowers the trust on information systems, especially when the investments made in defending the means of work do not rule out failures. The ideal situation is that systems do not fail. But the reality is that most of us are used to living with systems that fail. The matter is not as much the absence of incidents, but the confidence that they are under control; it is known what failures may occur and what to do when they do occur. Fear of the unknown is the main source of lack of confidence and, as a result, knowledge brings confidence: knowing the risks allows them to be faced and controlled.

1.1. Objectives of Magerit

Magerit seeks to achieve the following objectives:

Direct objectives:

1. To make those responsible for information systems aware of the existence of risks and of the need to treat them in time.
2. To offer a systematic method for analysing these risks.
3. To help in describing and planning the appropriate measures for keeping the risks under control.

Indirect objectives:

4. To prepare the organisation for the processes of evaluating, auditing, certifying or accrediting, as relevant in each case.

[1] CSAE: Higher Council for Electronic Government (Consejo Superior de Administración Electrónica).

[2] MAGERIT: Risk Analysis and Management Methodology for Information Systems.

[3] OECD Guidelines for the Security of Information Systems and Networks, 2002.

It also aims to achieve uniformity in the reports containing the findings and conclusions from a risk analysis and management project:

Value model

Description of the value of the assets for the organisation as well as the dependencies between the various assets.

Risk map

The account of the threats to which the assets are exposed.

Safeguard evaluation

Evaluation of the effectiveness of the existing safeguards in relation to the risk facing them.

Risk status

Classification of the assets by their residual risk; that is, by what could happen, taking the safeguards used into consideration.

Deficiencies report

Absence or weakness of the safeguards that appear appropriate to reduce the risks to the system.

Security plan

Group of security programs that put the risk management decisions into action.

1.2. Introduction to risk analysis and management

Security is the capability of networks or information systems to resist accidents or illegal or malicious actions that compromise the availability, authenticity, integrity and confidentiality of the data stored or transmitted and of the services that these networks and systems offer or make accessible, with a specific level of confidence.

The objective is to protect the organisation's purpose, taking the different security dimensions into account:

Availability

The readiness of the services to be used when necessary. The lack of availability causes an interruption of the service. Availability directly affects the organisation's productivity.

Integrity

The maintenance of the completeness and correctness of the data. Without integrity, information may appear to be altered, corrupt or incomplete. Integrity directly affects the correct undertaking of an organisation's functions.

Confidentiality

Information must only reach authorised persons. Lack of confidentiality or secrecy could cause leaks of information as well as unauthorised accesses. Confidentiality is difficult to recover and could undermine the confidence of others in the organisation when the person responsible for maintaining secrecy is not conscientious and it could involve the lack of compliance with laws and contractual undertakings relating to the safekeeping of data.

Authenticity (of who uses the data or services)

There must be no doubt as to who is responsible for information or for providing a service, both in order to trust on them and to follow up non-compliances or errors. Lack of authenticity causes falsifications and tricks that could lead to fraud. Authenticity is the basis for fighting against repudiation and it is thus basic to electronic commerce and electronic government, providing confidence without paperwork or physical attendance.

All these features may or may not be required, depending on the case. Where required, they not achieved at zero cost; usually means and effort are required to achieve them. Risk analysis and management methodologies are used to rationalise this effort.

Risk

An estimate of the degree of exposure to threat to one or more assets causing damage or prejudice to the organisation.

The risk shows what could happen to the assets if they are not suitably protected. It is important to know which features are of interest in each asset as well as the degree to which these features are in danger, that is, to analyse the system:

Risk analysis

A systematic process for estimating the size of the risks to which an organisation is exposed.

Knowing what may happen, decisions must be made:

Risk management

The selection and implementation of safeguards for knowing, preventing, reducing or controlling the identified risks.

Note that one legitimate option is to accept the risk. One frequently hears that absolute security does not exist; effectively, it is always necessary to accept a risk which however, must be known and subjected to the quality threshold required by the service.

Because all this is very delicate and is not merely technical, and includes the decision to accept a certain level of risk, it is essential to know in which conditions one is working and thus be able to ascertain to what level the system is trustworthy. This requires a methodical approach that allows decisions to be made with reason and to explain the decisions rationally.

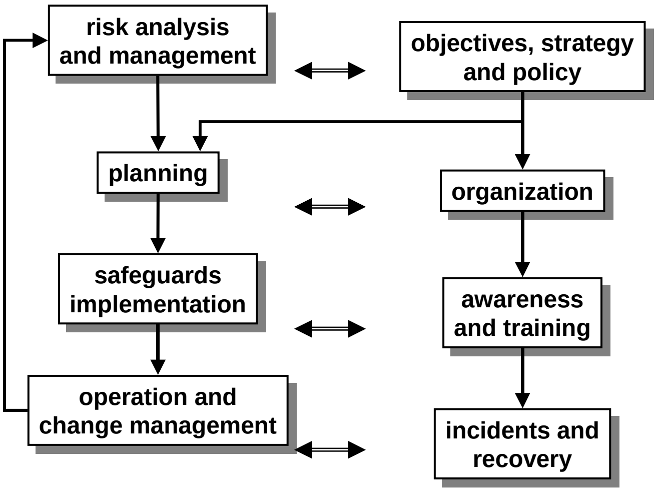
1.3. Risk analysis and management in context

The risk analysis and management tasks are not an end in themselves but form part of the continuous activity of security management.

Risk analysis allows the determination of the assets, their value and how they are protected. In coordination with the organisation's objectives, strategy and policies, risk management activities allow a security plan to be prepared which, when implemented and operated, meets the proposed objectives with the level of risk accepted by management.

The implementation of security controls requires a managed organisation and the informed participation of all persons working with the information system. These persons are responsible for the daily operation, the reaction to incidents and the general monitoring of the system to determine if it effectively and efficiently meets the proposed objectives.

This working plan must be repetitive since information systems are rarely unchangeable; normally they are subject to continual development, their own (new assets) and to changes in the environment (new threats), requiring periodic reviews to learn from experience and to adapt to the new context.


risk analysis and management
objectives, strategy and policy
planning
organization
safeguards implementation
awareness and training
operation and change management
incidents and recovery

Risk analysis provides a model of the system in terms of assets, threats and safeguards and is the foundation for controlling all activities on a well founded base. Risk management is the structuring of the security actions to meet the needs detected through analysis.

1.3.1. Awareness and training

The best security plan will be seriously compromised without the active collaboration of the persons involved in the information system, especially if the attitude is negative, and contrary or one of "fighting against the security measures". This requires the creation of a "security culture" which, coming from top management, encourages the awareness of all those involved of its need and relevance.

There are two basic pillars for creating this culture:

- A corporate security policy which is understood (written so as to be understood by those who are not experts in the matter) which is published and kept updated.
- Continuous training at all levels, with reminders of routine precautions and specialised activities, depending on the responsibility of each work post.

So that these activities fit into the organisation, it is essential that security be:

- Unobtrusive, so that it does not unnecessarily impede daily activities or compromises the achievement of the proposed productivity objectives.
- "Natural," so that it does not cause avoidable errors and facilitates compliance with the proposed good practices.
- Practised by management as an example in a daily activity with quick reactions to changes and incidents.

1.3.2. Incidents and recovery

Persons involved must be aware of their role and continued relevance to prevent problems and to react when they do occur. It is important to create a culture of responsibility in which potential problems, discovered by those close to the affected assets, can be channelled towards the decision points. Thus, the safeguards system will respond to the situation.

When an incident occurs, time starts to act against the system: its survival depends on the speed and correctness of the reporting and reaction activities. Any error, lack of precision or ambiguity in these critical moments is amplified, turning what could be a mere incident into a disaster.

It is necessary to learn continuously from both successes and failures and to incorporate them into the risk analysis and management process. The maturity of an organisation is reflected in the orderliness and realism of its value model and, as a result, in the suitability of all types of safeguards, from tactical measures to an optimal organisation.

1.4. Organisation of guides

This version 2 of Magerit has been structured into three books: this one, which describes "The Method", the "Elements catalogue" and a "Guide to Techniques."

This guide describes the method from three angles:

- Chapter 2 describes the steps for carrying out an analysis of the risk status and for managing its mitigation. This is an entirely conceptual presentation.
- Chapter 3 describes the basic tasks to be carried out in a risk analysis and management project, on the understanding that it is not sufficient to have a clear idea of concepts but it is necessary to guide roles, activities, milestones and documentation so that the risk analysis and management project is constantly under control.
- Chapter 4 applies the methodology to the development of information systems on the understanding that system development projects must include risks from the start, both the risks to which they are exposed and those that the applications themselves introduce into the system.

As a complement, Chapter 5 discusses a series of practical aspects arising from the accumulated experience over time for carrying out a really effective analysis and management.

The Appendices contain reference material:

1. A glossary.
2. Bibliographical references used in developing this methodology.
3. Legal references covering the tasks of analysis and management.
4. Standards for evaluation and certification.
5. The features required from present or future tools for supporting the risk analysis and man-

agement process.

6. A comparison of how Magerit version 1 has developed into this version 2.

Finally, a practical case is given as an example.

1.4.1. Method of use

Readers new to the subject should start with Chapter 2.

Those who already have some knowledge of the concepts will find the example helps to centre ideas and terminology.

For those about to start a risk analysis and management project, Chapter 3 helps to structure and plan it. If the information system is simple and small or if only a first approximation is required, an informal plan may be sufficient, but when the project is large, it is necessary to be methodical.

For those carrying out a risk analysis and management project, Chapter 5 helps to centre the activity without distractions.

Chapter 4 is for those about to collaborate in a project to develop a new information system or in a maintenance cycle.

Appendix 4 is for those working with approved systems, whether interested in a mechanism for specifying what they need or because they are interested in a mechanism to specify what they have.

The planning of these guides has followed a “maximums” criterion, considering all types of assets, all types of security aspects and all types of situations. In practice, the user may find situations in which the analysis is more restricted, as in some frequent practical cases:

- Only a study of the files affected by personal data legislation is required.
- Only a study of information confidentiality guarantees is required.
- Only a study of the availability of services is required (typically because a contingency plan is being developed).
- Etc.

These frequent situations are formally contained in the tasks for activity A1.2 with the informal comment that concentrating on a reduced domain and increasing it according to requirements is more constructive than tackling it in its entirety.

1.4.2. The elements catalogue

A separate book proposes a catalogue - open to additions - that provides guidelines for:

- Types of assets.
- Dimensions for evaluating assets.
- Criteria for evaluating assets.
- Typical threats to information systems.
- Safeguards to be considered for protecting information systems.

There are two objectives:

1. Firstly, to facilitate the work of those involved in a project in the sense of giving them standard elements that they can adapt quickly, concentrating on the specifics of the system under analysis.
2. And secondly, to provide uniform results from the analysis, promoting uniform terminology and criteria that allow the comparison with and even integration of analyses carried out by different teams.

Each section includes XML notation to be used for regularly publishing the elements in a standard format that can be processed automatically by analysis and management tools.

If the reader uses a risk analysis and management tool, this catalogue will form part of it. If the analysis is carried out manually, this catalogue provides a wide starting base for quick progress without distractions or oversights.

1.4.3. The Guide to techniques

A separate book provides additional information and guides on some techniques often used when carrying out risk analysis and management projects:

- Techniques specific to risk analysis:
  - Analysis using tables.
  - Algorithmic analysis.
  - Attack trees.
- General techniques:
  - Cost/benefit analysis.
  - Data flow charts.
  - Process charts.
  - Graphical techniques.
  - Project planning.
  - Work sessions: interviews, meetings and presentations.
  - Delphi evaluation.

This is a reference guide. As the reader progresses through the project's tasks, the use of certain specific techniques is recommended, to which this guide is an introduction, and references are provided so that the reader can learn more about the techniques described.

1.5. For those who have worked with Magerit v1.0

If you have worked with Magerit v1.0, all the concepts will be familiar although there has been a certain evolution. Specifically, you will recognise the so-called elements sub-model: assets, threats, vulnerabilities, impacts, risks and safeguards. This conceptual part has been validated over time and continues to be the centre around which the fundamental phases of analysis and management revolve. The so-called "security sub-states" has been corrected and enlarged, giving it the new name of "dimensions"[4] and introducing new yardsticks for measuring the interesting aspects of the assets. The process sub-model appears under the heading of "structuring the risk analysis and management project."

Although Magerit v1.0 has resisted the passing of time well in its conceptual aspects, the same cannot be said of the technical details of the information systems involved. An update has been attempted but above all the difference has been defined between what is essential (and permanent) and what is temporary and will change over time. This translates into giving parameters to the working method, referencing it to external catalogues of threats and safeguards that can be updated to adapt to the passing of time, both because of technological progress and progress in the subject, because, just as the system changes, so do the subjects around it, good and bad. The more successful the systems are, the more users they will have and, simultaneously, more subjects will be interested in abusing them or, simply, destroying them. Thus, the method remains open so that while what is being done and how it is being done remains clear, it can be adapted to details at all times.

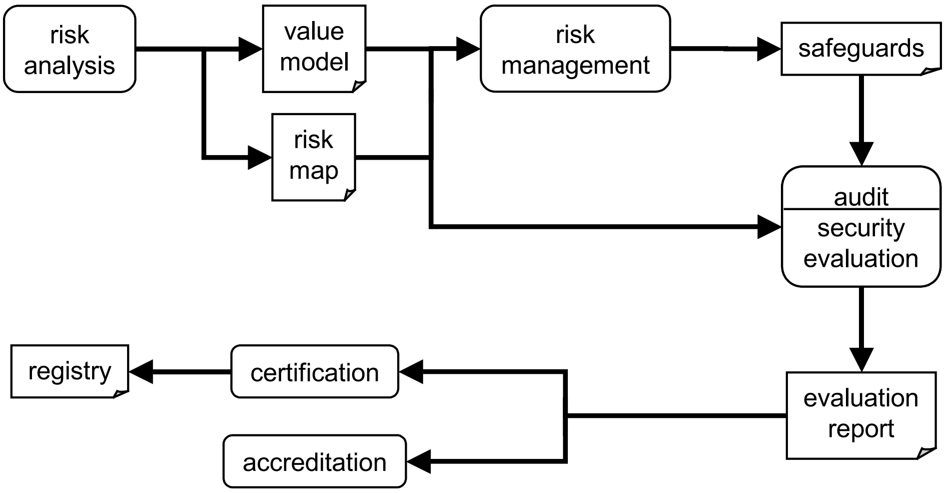
[4] Dimension, according to one of the definitions in the official Spanish dictionary, is "each of the magnitudes of a group that serve to define a phenomenon. For example, the four-dimensional space in the theory of Relativity."

For practical purposes, the above paragraph means that the types of assets, the dimensions and evaluation criteria, the threats catalogue and safeguards catalogue have been placed in a separate book, the “Elements catalogue,” so that they can evolve.

Appendix 6 gives more precise details of the differences between version 1.0 and this one.

1.6. Evaluation, certification, auditing and accrediting

Risk analysis is the cornerstone in the processes of evaluating, certifying, auditing and accrediting that establish to what extent the information system is trustworthy. Given that no two information systems are alike, the evaluation of each specific system requires adapting to its components. Risk analysis provides an overview of each system, its value, the threats to which it is exposed and the safeguards with which it is equipped. Risk analysis is therefore an obligatory step towards carrying out all the above mentioned tasks, listed in the following diagram:



This section provides a conceptual presentation of these activities. The reader will find a specific discussion of the standards relating to management systems and security products in Appendix 4.

Evaluation

The evaluation of security and information systems is increasingly frequent, both internally as part of management processes and by independent external evaluators. Evaluations establish to what extent an information system is trustworthy.

Certification

The evaluation may lead to a certification or registration of the system’s security. In practice, products are certified and security management systems are certified. The certification of products is in any case impersonal: “This has these technical properties.” However, the certification of management systems is concerned with the “human component” of the organisations, seeking to analyse the way in which the systems are used.[5]

Certification means assuring a behaviour responsibly and in writing. The subject of the certification - product or system - is submitted to a series of evaluations aimed at an objective: What is it wanted for?[6]. A certificate states that a system can protect data from threats with a certain level of quality (protection capacity). It states this on the basis that a series of safeguards has been observed to exist and operate. This means that there are risk analysis concepts behind a certificate.

[5] There are vehicles with high technical features and others with lower ones, just as there are drivers who are real professionals and others of whom it is impossible to explain how they are qualified as “suitable to handle vehicles.” The ideal is to put a powerful car in the hands of a great driver. From there downwards, we have a great variety of situations of lesser confidence: greater risk of something going wrong.

[6] And thus we have systems suitable for “human consumption” or for “use in conditions of extreme heat.”

Risk analysis must have been carried out before certification in order to know the risks and control them by adopting suitable controls. This will also be a control point for the management of the product or system.

Accrediting

Some certifications are designed to accredit the product or system. Accrediting is a specific process, the object of which is to qualify the system to form part of wider systems. It can be seen as a certification for a specific purpose.

Audit

Although not the same, internal or external audits of information systems are not very far from this world.

- Some are required by law in order to operate in a specific sector.
- Others are required by the organisation's management itself.
- Others are required by collaborating organisations that have their own level of risk connected with ours.

An audit may serve as a risk analysis that allows (1) to know what is at play; (2) to know what the system is exposed to; and (3) to evaluate the effectiveness and efficiency of the safeguards.

Frequently, auditors start with an implicit or explicit risk analysis either carried out by themselves or audited by them in the first phase of auditing, because it is difficult to form an opinion of what is not known. On the basis of the risk analysis, the system can be analysed and the management informed as to whether the system is under control, that is, if the security measures adopted are justified, implemented and monitored so that the system of indicators available to the management can be trusted for managing the systems' security.

The conclusion of the audit is a report on the deficiencies found, which are simply inconsistencies between the needs identified in the risk analysis and those discovered during the inspection of the system in operation.

> The audit report must describe the suitability of the measures and controls to the present regulations, identifying their deficiencies and proposing corrective or complementary measures. It will also include the data, facts and comments that support the conclusions reached and the proposed recommendations. [RD 994/1999, article 17.2.].

In the case of the government, there are some fundamental references with regard to which audits can and must be made:

- Royal Decree 994/1999, 11 June, approving the regulations for security measures for automated files containing personal data.
- "Criteria for security, standardisation and conservation of applications used for processing jurisdictions," MAP, 2004.

The audits must be repeated regularly both to follow the evolution of the risk analysis (which must be updated regularly) and to follow the evolution of the security plan determined by the Risk management activities.

1.7. When should risks be analysed and managed?

Carrying out a risk analysis is laborious and costly. Preparing a map of assets and valuing them requires the collaboration of many people within the organisation from management levels to technicians. Not only must many people be involved but uniformity of criteria must be achieved between them because, although it is important to quantify the risks, it is even more important to define their relationships since a mass of data typically appears in a risk analysis. The way to tackle the complexity is to concentrate on the most important (maximum impact, maximum risk) and to remove the secondary or insignificant, but if the data are not well sorted in relative terms, it is impossible to interpret them.

To summarise, a risk analysis is not a minor task that anyone can carry out in their spare time. It is an important task that requires effort and co-ordination and must therefore be planned and justified.

A risk analysis is recommended in any organisation that depends on information and communication systems to carry out its purpose; specifically, in any environment in which goods and services are handled electronically, whether in a public or private context. Risk analysis allows decisions to be made on investment in technology, from the acquisition of production equipment to the deployment of an alternative centre to ensure the continuity of the activity, including decisions on the acquisition of technical safeguards and on the selection and training of personnel.

Risk analysis is a management tool that allows decisions to be made. Decisions may be made before deploying a service or when it is operating. It is very desirable to carry it out beforehand so that the measures that must be taken are incorporated into the design of the service, in the choice of components, in the development of the applications and in the user manuals. Anything that involves correcting unforeseen risks is costly in both internal and external time, which could damage the organisation's image and may eventually cause a loss of confidence in its capability. It has always been said that prevention is better than cure and this applies here: don't wait until a service is failing - it is necessary to anticipate and be prepared.

For legal reasons

The risk analysis may be required for legal reasons, such as the case of Royal Decree 263/1996, 16 February, which regulates the use of electronic, computer and telematic techniques by the government. Its article 4 (Guarantees for the use of electronic, computer and telematic media and applications) states:

2. When using the media and applications referred to in the previous section, the necessary technical and organisational measures must be adopted to ensure the authenticity, confidentiality, completeness, availability and conservation of the information. These security measures must take into account the state of the art and be matched to the nature of the data and of the handling *and of the risks to which they are exposed* [7].

Similarly, Organic Law 15/1999, 13 December, on the protection of personal data, states in its article 9 (Data security):

1. The person responsible for the file and, where appropriate, the person responsible for its handling, must adopt the necessary technical and organisational measures that guarantee the security of the personal data and prevent its alteration, loss, unauthorised treatment or access, taking into account the state of the art, the nature of the data stored and *the risks to which they are exposed*, whether by human action or from the physical or natural environment.

This text is used again in the preamble to Royal Decree 994/1999, 11 June, approving the regulations for security measures for automated files containing personal data. This decree includes the obligation of preparing a security document:

1. The person responsible for the file must prepare and implement the security standards in a document that must be complied with by the personnel with access to the automated personal data and to the information systems.

It would be difficult to prepare this document without a prior analysis of the risks to the data, an analysis which allows us to determine the pertinent security measures.

Certification and accrediting

If certification for the system is sought, risk analysis is a prior requisite that will be required by the evaluator. It is the source of information for determining the relationship of relevant controls for the system and which must therefore be inspected. See Appendix 4.1 on the certification of information security management systems (SGSI).

[7] Risk analysis allows the determination of the risks to which they are exposed and risks management allows the measures to be matched to these risks.

The risk analysis is also a requirement for systems accrediting processes[8]. These processes are necessary for handling classified national, EU, Nato or other information from other international agreements. The first step in the process is to carry out a risk analysis to identify threats and safeguards and to satisfactorily manage risks to the system.

Finally, the use of protection profiles as a contracting mechanism should be mentioned. Protection profiles (ISO/IEC-15408) have the double purpose of the *a priori* specification of the security requirements for a system (for its acquisition or development) and can serve as an international reference for the meaning of a certification. In either case, it sets a “yardstick” with respect to which the suitability of the system’s security is qualified. See Appendix 4.2 on common evaluation criteria (CC).

To conclude

Analyse and manage the risks when there is a direct or indirect legal requirement and whenever required for the responsible protection of an organisation’s assets.

[8] In the formal meaning of authorisation for handling classified information. The accrediting processes depend on the applicable standards in each case.

2. Undertaking the analysis and management

This chapter describes the concept of risk analysis and management, what is sought at each moment and what conclusions are achieved.

There are two large tasks to be carried out:

I. Risk analysis

which determines what the organisation has and estimates what may happen.

Elements:

1. Assets, which are the elements in the information system (or closely related to it) that give value to the organisation.
2. Threats, which are things that may happen to the assets, causing damage to the organisation.
3. Safeguards (or countermeasures), which are defence elements deployed so that those threats do not cause [so much] damage.

These elements allow the estimating of:

4. The impact: what may happen.
5. The risk: what will probably happen.

Risk analysis allows these elements to be analysed methodically to reach conclusions with a basis.

II. Risk management

which allows a thorough and prudent defence to be organised, so that nothing bad happens and at the same time preparations are made to cope with emergencies, survive incidents and continue operating in the best conditions. Because nothing is perfect, it is said that the risk is reduced to a residual level that the management can live with.

Informally, it can be said that the management of security in an information system is the management of its risks and that the analysis allows this management to be rationalised.

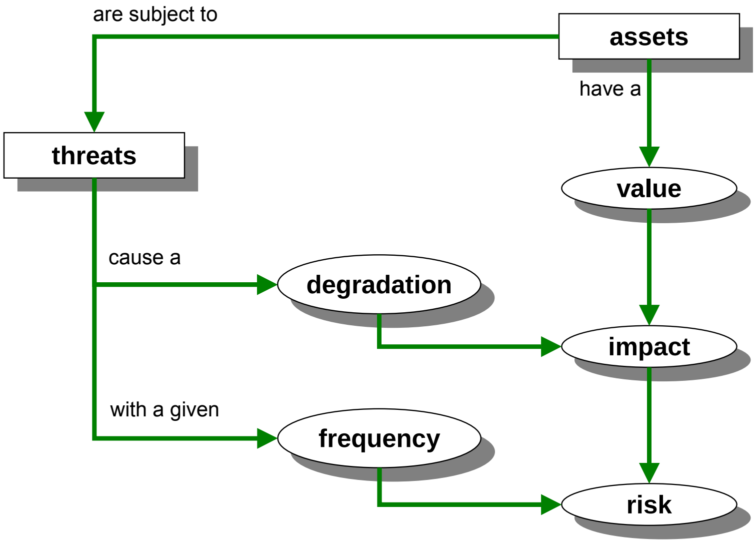
2.1. Risk analysis

Risk analysis is a methodical approach to determine the risk, following specific steps:

1. Determine the relevant assets for the organisation, their inter-relationships and their value i.e. what prejudice (cost) would be caused by their degradation.
2. Determine the threats to which those assets are exposed.
3. Determine what safeguards are available and how effective they are against the risk.
4. Estimate the impact, defined as the damage to the asset arising from the appearance of the threat.
5. Estimate the risk, defined as the weighted impact on the rate of occurrence (or the expectation of appearance) of the threat.

In order to organise the presentation, steps 1, 2, 4 and 5 are handled first, skipping step 3, so that any estimates of impact and risk are “potential” if no safeguards are deployed. Once this theoretical scenario is obtained, the safeguards are incorporated in step three, providing realistic estimates of impact and risk.

The following figure shows this first pass, the steps of which are described in the following sections[9]:



2.1.1. Step 1: Assets

The assets are the **resources in the information system or related to it that are necessary for the organisation to operate correctly and achieve the objectives proposed by its management**.

The essential asset is the information handled by the system, that is the data. Other relevant assets can be identified around these data:

The services that can be provided thanks to these data and the services needed to be able to manage these data.

The computer applications (software) that allow these data to be handled.

The computer equipment (hardware) that hosts the data, applications and services.

The information media, which are data storage devices.

The auxiliary equipment that complements the computer equipment.

The communications networks that allow the exchange of data.

The installations that house the computer and communications equipment.

The persons who use or operate all the above elements.

Types of assets

Not all the assets are of the same type. The threats and safeguards are different according to the type of assets[10]. Chapter 2 of the “Elements catalogue” gives a list of types of assets.

If the system handles personal data, these are usually important in themselves and require a series of safeguards frequently regulated by law. With these assets, it is interesting to determine what treatment must be imposed[11]. The fact that a datum is personal affects all the assets involved in its handling and safekeeping.

[9] Readers familiar with Magerit v1.0 will notice the absence of the “vulnerability” concept (the potential or possibility that a threat will occur to an asset) which is incorporated using the degradation measurements of the asset and the frequency with which the threat occurs.

[10] A telematic service is not attacked or defended in the same way as a work place.

[11] It is as though the legislator had carried out the risk analysis for us and had determined the appropriate safeguards. In any case, laws and regulations exist and help to protect these important data.

Something similar happens with data classified as confidential. When a certain report is "*classified*" so that its copies are numbered, may only reach certain persons, must not leave the premises and must be rigorously destroyed, etc, a series of safeguards is being imposed because of the sector or organisation-specific regulations.

Dependencies

The most notable assets are the data and services but these depend on other, more prosaic, assets such as the equipment, the communications or the often-forgotten persons who work with them. Thus, the concept of "dependencies between assets" or the degree to which a *higher* asset is affected by a security incident in a *lower* one seems important [12].

A "higher asset" is said to depend on the "lower asset" when the security needs of the higher one are reflected in the security needs of the lower one. In other words, when the appearance of a threat in the lower asset has a prejudicial effect on the high asset. Informally, this could be interpreted as the lower assets being the pillars that support the security of the higher assets.

Although it is necessary to adapt to the organisation being analysed in each case, the group of assets can frequently be structured into layers, where the upper layers depend on the lower ones:

- Layer 1: **The environment**: assets that are needed to guarantee the following layers:
    - Equipment and supplies: power, air-conditioning, communications.
    - Personnel: management, operations, development, etc.
    - Others: buildings, furniture, etc.
- Layer 2: **The information system** itself:
    - Computer equipment (hardware).
    - Applications (software).
    - Communications.
    - Information media: discs, tapes, etc.
- Layer 3: **The information**:
    - Data.
    - Meta-data: structures, indicators, encryption keys, etc.
- Layer 4: **The functions of the organisation**, which justify the existence of the information system and give it purpose:
    - Objectives and mission.
    - Goods and services produced.
- Layer 5: **Other** assets:
    - Credibility or good image.
    - Accumulated knowledge.
    - Independence of criterion or action.
    - The privacy of persons.
    - The physical well-being of persons.

[12] An example can be better than a thousand words. If the building housing the equipment burns down, what ceases to function is the service perceived by the user at a distance. If the portable computer of an executive containing strategic company information is stolen, what suffers is the confidentiality of that information. Installations can be rebuilt, but the opportunity of providing the service may be lost. Theft is overcome by buying another portable computer but the secret has already been lost.

Valuation

Why is an asset of interest? Because of its value.

We are not talking of what things cost but of their value. If something is not of any value, discard it. If an asset cannot be easily discarded, this is because it is of value. This is what has to be discovered since this is what has to be protected.

The value may be its own or may be accumulated. Lower assets in the dependencies diagram are said to accumulate the value of the assets that are supported by them.

The core value is usually the information (or data) that is handled by the system, with the other assets subordinated to the needs of using and protecting the information. Information systems also use the data to provide services, either internal to the organisation or for third parties, with a series of data being necessary to provide the service. Without going into technical details of how things are carried out, the group of data and end services allows an organisation to be classified functionally. The dependencies between assets allow the other assets to be related with data and services.

Dimensions

It may be interesting to look at the different dimensions of an asset:

- Its **authenticity:** To what extent would a lack of knowledge about who has done what be harmful?

  This valuation is typical of services (user authenticity) and of data (authenticity of the persons accessing the data for writing or, simply, querying).

- Its **confidentiality**: What damage would be caused by unauthorised knowledge?

  This valuation is typical of data.

- Its **integrity**: What damage would be caused if it was damaged or corrupt?

  This evaluation is typical of data that can be handled and be totally or partially false or even of a lack of data.

- Its **availability**: What damage would be caused if it were not available or could not be used?

  This valuation is typical of services.[13]

In systems dedicated to e-government or e-commerce, knowledge of those involved is fundamental in order to be able to provide the service correctly and to be able to track down failures (accidental or deliberate) that may occur. As well as authenticity, it is interesting to calibrate in these assets:

- The **accountability** of the use of the service: what damage would be caused by not knowing to whom the service is provided? That is, who does what, when?
- The **accountability** of access to the data: what damage would be caused by not knowing who accesses the data and what they do with them?

Usually the basic dimensions are recognised: authenticity, confidentiality, integrity and availability. Authenticity has been refined in this method to discriminate between the use of a service and the access to data. The concept of accountability has also been introduced, taken from the ISO/IEC 13335 guides, equally separated into the accountability of the service and of the data. The aspects of the authenticity and accountability of the data are critical for meeting the regulatory measures for files containing personal data.

Chapter 3 of the “Elements catalogue” provides a list of security dimensions.

[13] There are end services that provide the organisation’s final mission. There are internal services used by the organisation to structure its own distribution of responsibilities. Finally there are services acquired from other organisations: external supplies.

In a tree of dependencies in which the upper assets depend on the lower ones, it is essential to value these upper assets, those that are important in themselves. This value automatically accumulates in the lower ones, which does not mean that these may not also need their own valuation.

How much is the 'health' of the assets worth?

Once it has been determined which security dimensions are of interest in an asset, it must be valued. The valuation is the determination of the cost caused by an incident that destroys the asset. There are many factors to be considered:

- Replacement cost: acquisition and installation.
- Labour cost (specialised) invested in recovering (the value of) the asset.
- Loss of income.
- Operating capacity: the confidence of the users and suppliers which translates into a loss of activity or into worsened economic conditions.
- Penalties due to non-compliance with the law or with contractual obligations.
- Damage to other assets, internal or external.
- Injury to persons.
- Environmental damage.

The evaluation may be quantitative (with a quantity) or qualitative (on a scale of levels). The most important criteria to be respected are:

- **Uniformity**: It is important to be able to compare values even if they are of different dimensions in order to be able to combine own and accumulated values as well as to be able to determine if the damage is more serious in one dimension or in another.
- The **relationship**: It is important to be able to see the relative value of an asset in comparison with other assets.

All these criteria are met with financial valuations (the monetary cost required to "cure" the asset) and it is frequently tempting to put a price on everything. If this is achieved, fine. It is even easy to put a price on the most tangible aspects (equipment, working hours, etc) but when entering into more abstract evaluations (intangible, such as the organisation's credibility) the exact financial valuation can be slippery and the cause of bitter arguments between experts.

Chapter 4 of the "Elements catalogue" gives some guidelines for the systematic valuation of assets.

Qualitative valuation

Qualitative scales allow rapid progress, positioning the value of each asset in the relative order with respect to the others. The scales are frequently provided as "orders of magnitude" for providing estimates of the order of magnitude of the risk.

The limitation of qualitative valuations is that they do not allow values to be compared beyond their relative order - the values cannot be added.

Chapter 8.1 of the "Guide to techniques" describes an analysis model based on qualitative valuations.

Quantitative valuation

Absolute numerical valuations require great effort but do not have the problems of qualitative valuations. Adding numerical values is absolutely "natural" and the interpretation of the results is never the cause of controversy.

If the valuation is monetary, financial studies can also be made comparing what is at risk with what the solution costs by answering the questions:

- Is it worth investing so much money in this safeguard?

- Which group of safeguards optimises the investment?
- Over what period of time will the investment be recovered?
- What is the reasonable cost of an insurance policy?

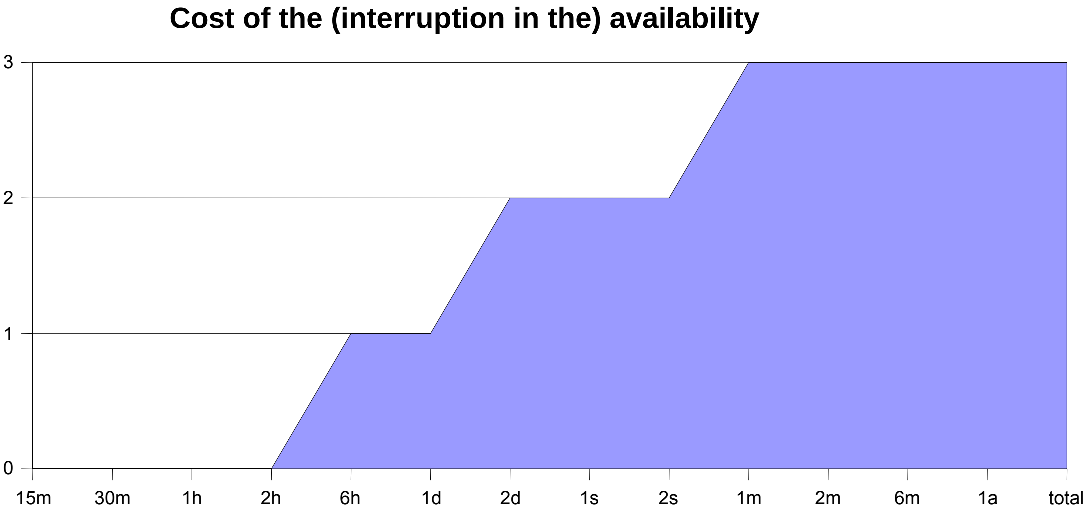
Chapter 8.2 of the “Guide to techniques” gives an analysis model based on quantitative valuations.

The value of an interruption to the service

Nearly all the dimensions described above can be valued simply, qualitatively or quantitatively, but there is one exception: availability.

Interrupting a service for one hour is not the same as interrupting it for a day or for a month. One hour’s stoppage may be irrelevant while a day without service may cause moderate damage; but a month’s stoppage implies the termination of the activity. Unfortunately, there is no proportional relationship between the length of the downtime and its consequences.

Thus, the valuation of the [interruption of the] availability of an asset requires the use of a more complex structure, summarised in the following diagram:



This shows a series of steps of an interruption that end with the total, permanent destruction of the assets. In the above example, stoppages of up to six hours can be withstood without consequences. But after six hours, the alarms start to ring and increase if the stoppage exceeds two days. If the stoppage exceeds one month, it could be said that the organisation has lost its operating capacity: it is dead. From the point of view of cures, the graph directly states that not a single euro must be spent to prevent stoppages of less than six hours. A certain cost is worthwhile to prevent a stoppage from exceeding six hours or two days. When evaluating the cost of preventing the stoppage from exceeding one month, the entire value of the organisation must be weighed against the cost of the safeguards - it may not be worth it.

2.1.2. Step 2: Threats

The next step is to determine the threats that may affect each asset. Threats are “things that happen.” Of all the things that could happen, those that are of interest are those that could happen to our assets and cause damage.

There are natural disasters (earthquakes, floods, etc) and industrial accidents (pollution, electrical failures, etc) of which the information system is a passive victim, but being passive does not necessarily mean remaining defenceless. There are threats caused by persons, either through errors or intentional attacks.

Chapter 5 of the “Elements catalogue” gives a list of typical threats.

Not all threats affect all assets[14] but there is a certain relationship between the type of asset and what could happen to it.

Valuation of threats

When an asset is the victim of a threat, not all of its dimensions are affected and not all to the same degree.

Once it has been determined that a threat may damage an asset, the asset's vulnerability[15] must be estimated considering two aspects:

Degradation: The amount of damage done to the asset.

Frequency: How often the threat appears.

Degradation measures the damage caused by an incident if it occurs.

Degradation is often described as a part of the asset's value and therefore expressions appear such as that an active has been "totally degraded," or "very slightly degraded". When the threats are not intentional, it is probably enough to know the physically damaged part of an asset in order to calculate the proportional loss of value. But when the threat is intentional, one cannot think of proportions since the attacker may cause a great deal of damage selectively.

Frequency[16] puts degradation into perspective since one threat may have terrible consequences but very unlikely to occur while another threat may have very small consequences but be so frequent as to accumulate into considerable damage.

Frequency is modelled as an annual occurrence rate with the following typical values:

100	very frequent	daily
10	frequent	monthly
1	normal	annually
1/10	infrequent	every few years

2.1.3. Step 4: Determination of the impact

Impact is the measurement of the damage to an asset arising from the appearance of a threat. By knowing the value of the assets (in various dimensions) and the degradation caused by the threats, their impact on the system can be derived directly. The only consideration required relates to the dependencies between assets. Frequently, the value of the information system is centred on services it provides and the data it handles while the threats usually appear in the media.

Accumulated impact

This is calculated for an asset taking into account:

- Its accumulated value (its own plus the accumulated value of the assets that depend on it).
- The threats to which it is exposed.

The accumulated impact is calculated for each asset, for each threat and in each evaluation dimension, being a function of the accumulated value and of the degradation caused.

[14] Installations may catch fire but not applications. Persons may be subjected to a bacteriological attack but not services. However, computer viruses affect applications but not persons.

[15] Readers familiar with Magerit v1.0 will notice the absence of the "vulnerability" concept (the potential or possibility that a threat will occur to an asset) which is incorporated using the degradation measurements of the asset and the frequency with which the threat occurs.

[16] Measured as the average number of occurrences of the threat over a specific period. Typically, it is estimated annually. For example, if a fault occurs in a system's air conditioning on an average of five times a year, that is the frequency: 5.

The greater the intrinsic or accumulated value of an asset, the greater the impact.

The greater the degradation of the attacked asset, the greater the impact.

Because the accumulated impact is calculated on the assets that carry the weight of the information system, it allows the determination of the safeguards to be adopted in the working media: protection of equipment, back-up copies, etc.

Deflected impact

This is calculated for an asset taking into account:

- Its intrinsic value.
- The threats to which the assets on which it depends are exposed.

The deflected impact is calculated for each asset, for each threat and in each valuation dimension, being a function of the intrinsic value and of the degradation caused.

The greater the intrinsic value of an asset, the greater the impact.

The greater the degradation of the attacked asset, the greater the impact.

The greater dependency of the attacked asset, the greater the impact.

Because the deflected impact is calculated on assets that have their own value, it allows the determination of the consequences of the technical incidents on the mission of the information system. It is therefore a management presentation that helps in making one of the critical decisions of a risk analysis: accepting a certain level of risk.

Aggregation of impact values

The above paragraphs determine the impact of a threat on an asset in a certain dimension. These single impacts may be aggregated under certain conditions:

- The deflected impact on different assets may be aggregated.
- The accumulated impact on assets that are not inter-dependent and that do not depend on any higher asset may be aggregated.
- The accumulated impact on assets that are not independent must not be aggregated because this would imply overrating the impact by including the accumulated value of the higher assets several times.
- The impact of different threats on the same asset may be aggregated although it is useful to consider to what measure the different threats are independent and may be concurrent.
- The impact of a threat in different dimensions may be aggregated.

2.1.4. Step 5: Determination of the risk

Risk is the measurement of the probable damage to the system. Knowing the impact of the threats to the assets, the risk can be derived directly simply by taking into account the frequency of occurrence.

The risk increases with the impact and with the frequency.

Accumulated risk

This is calculated for an asset taking into account:

- The accumulated impact on an asset arising from a threat.
- The frequency of threats.

The accumulated risk is calculated for each asset, for each threat and each valuation dimension, being a function of the accumulated value, the degradation caused and the frequency of threat.

Because the accumulated risk is calculated on the assets that support the weight of the information system, it allows the determination of the safeguards that must be employed in the work media: protection of equipment, back-up copies, etc.

Deflected risk

This is calculated for an asset taking into account:

- The deflected impact on an asset due to a threat.
- The frequency of the threat.

The deflected risk is calculated for each asset, for each threat and in each valuation dimension, being a function of the intrinsic value, the degradation caused and the frequency of the threat.

Because the deflected risk is calculated on the assets that have intrinsic value, it allows the determination of the consequences of technical incidents on the mission of the information system. It is therefore a management presentation that helps in making one of the most critical decisions in a risk analysis: accepting a certain level of risk.

Aggregation of risks

The above paragraphs determine the risk to an asset of a threat in a certain dimension. These single risks may be aggregated under certain conditions:

- The deflected risk on different assets may be aggregated.
- The accumulated risk on assets that are not inter-dependent and do not depend on any common higher asset may be aggregated.
- The accumulated risk on assets that are not independent must not be aggregated since this would imply overrating the risk by including the accumulated value of higher assets several times.
- The risk of different threats on the same asset may be aggregated although it is useful to consider to what measure the different threats are independent and may be concurrent.
- The risk of a threat in different dimensions may be aggregated.

2.1.5. Step 3: Safeguards

The above steps have not included the safeguards deployed. Thus, the impacts and risks to which the assets would be exposed if they were not protected in any way are measured. In practice, it is unusual to find unprotected systems: the measures described indicate what would happen if the safeguards were removed.

Safeguards or counter-measures are procedures or technological mechanisms that reduce the risk. There are threats that can be removed simply by suitable organisation; others require technical devices (programs or equipment) while others need physical security. Finally, there is the personnel policy.

Chapter 6 of the “Elements catalogue” gives a list of suitable safeguards for each type of asset.

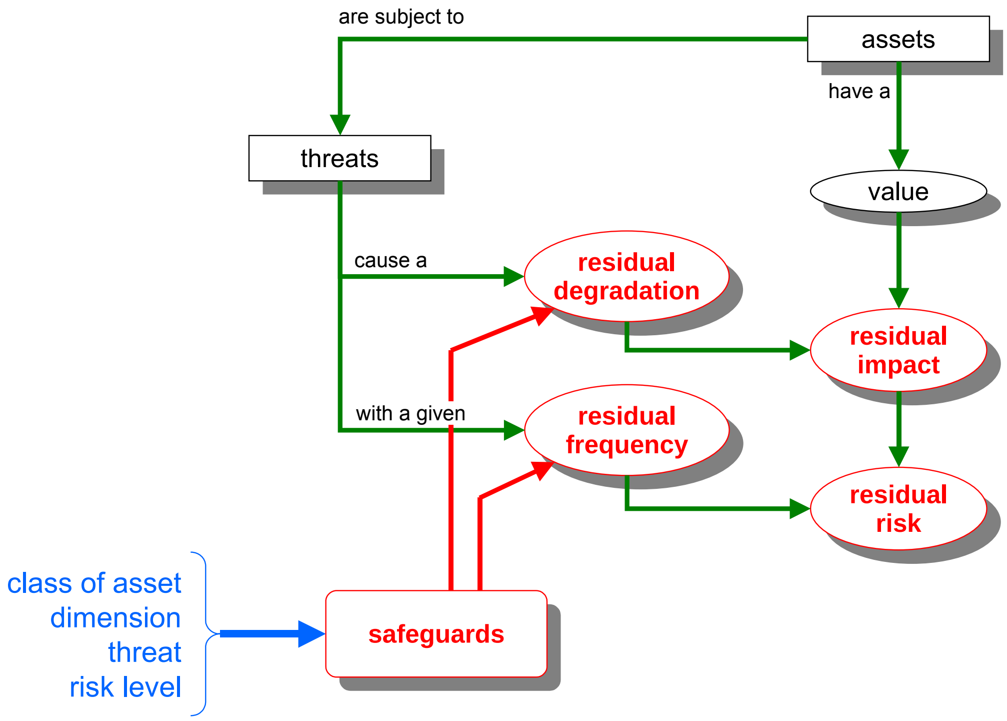
Safeguards enter into the calculation of the risk in two ways:

Reducing the frequency of threats

These are called preventive safeguards. Ideally, they completely prevent a threat from occurring.

Impact limitation

There are safeguards that directly limit any degradation while others allow the immediate detection of the attack to stop the progress of the degradation. There are even some safeguards that are limited to allowing the quick recovery of the system when the threat destroys it. In all of these versions, the threat occurs but the consequences are limited.



As well as being classified by their existence, safeguards are also classified by their effectiveness against the risk that they prevent. The ideal safeguard is 100% effective, which implies that:

- It is theoretically ideal.
- It is perfectly deployed, configured and maintained.
- It is always used.
- There are clear procedures for its normal use and its use in the event of incidents.
- The users are trained and aware.
- There are checks that warn of possible failures.

A level of real effectiveness must be estimated for each specific case, ranging from 0% for those that are just decorative and 100% for those that are perfect.

2.1.6. Revision of step 4: residual impact

If all homework has been carried out perfectly, the residual impact must be minimal.

If some of the work is half done (imprecise standards, incomplete procedures, unsuitable or insufficient safeguards, or controls that do not control) then the system is said to be subject to a residual impact.

The calculation of the residual impact is simple. Since neither the assets nor their dependencies have changed, only the size of the degradation, the impact calculations are repeated with this new degradation level.

The size of the degradation, taking into account the effectiveness of the safeguards, is the proportion that remains between perfect effectiveness and real effectiveness.

The residual impact may be accumulated on the lower assets or deflected on the higher assets.

2.1.7. Revision of step 5: residual risk

If all homework has been carried out perfectly, the residual risk must be minimal.

If some of the work is half done (imprecise standards, incomplete procedures, unsuitable or insufficient safeguards, or controls that do not control) then the system is said to be subject to a residual risk.

The calculation of the residual risk is simple. Since neither the assets nor their dependencies have changed, only the size of the degradation and the frequency of threats, the risk calculations are repeated using the residual impact and the new rate of occurrence.

The size of the degradation is taken into consideration in calculating the residual impact.

The size of the frequency, taking into account the effectiveness of the safeguards, is the proportion that remains between perfect effectiveness and real effectiveness.

The residual risk may be accumulated on the lower assets or deflected on the higher assets.

2.2. Risk management

Risk analysis determines impacts and risks. Impacts include absolute damage, regardless of whether the occurrence of the circumstance is more or less probable. On the other hand, the risk covers the probability of its occurring. The impact reflects the possible damage while the risk reflects the probable damage.

If the impact and the residual risk are minimal, the work is finished; otherwise something must be done.

2.2.1. Interpretation of the values for impact and residual risks

Impact and residual risk are a measurement of the present state, between the potential insecurity (without any safeguard) and the suitable measures that reduce impact and risk to minimal values. They are therefore a measurement of deficiencies.

The following paragraphs refer to impact and risk together.

If the residual value is equal to the potential value, the existing safeguards are worthless, usually not because nothing has been done but because there are fundamental elements that remain undone.

If the residual value is minimal, the task is ended. This does not mean lowering one's guard but it does mean starting the day with a certain degree of confidence.[17].

While the residual value is greater than minimal, there is a certain level of exposure.

It is important to understand that a residual value is only a number. Its correct interpretation requires that it be accompanied by the list of what must be done and what has not been done. Those responsible for making decisions must pay careful attention to this account of pending tasks, called the **deficiencies report**.

2.2.2. Choice of safeguards

Threats must be combated, in principle and while the alternative cannot be justified.

It is necessary to plan the group of appropriate safeguards to prevent both the impact and the risk, either by reducing the degradation of the asset (minimising the damage) or by reducing the frequency of the threat (minimising its opportunities).

All threats must be combated professionally, which means it is necessary to:

1. Set a policy for the organisation in the matter; that is, general directives for who is responsible for each thing.
2. Set a standard; that is, objectives to be met in order to be able to say correctly that the threat has been eliminated.
3. Set up procedures; that is, step by step instructions of what must be done.

[17] Don Quixote (Chapter 10) described the "balsam of Fierabras", which is ""It is a balsam," answered Don Quixote, "with which one need have no fear of death, or dread dying of any wound". The security manager cannot indulge in blind confidence since systems develop, attackers innovate, users are unpredictable in their errors and is always necessary to be aware and react promptly to new realities.

4. Deploy technical safeguards that effectively combat the threats and that can eliminate them.
5. Deploy controls that show that all the above is functioning as planned.

This group of elements is normally called Information Security Management System (SGSI) although it is being managed as well as acting.

The above paragraph may be deceptive if the reader understands that all of the points must be carried out for each threat. No. In practice, it translates into developing a policy, standards and procedures together with the deployment of a series of safeguards and controls to ensure that each threat has a suitable response.

Of the above points, the most "open" is that of determining the appropriate safeguards. This is really an art that requires specialised personnel although in practice the most usual situations are perfectly documented in the literature and it is sufficient to choose from a catalogue according to the size of the risk.

Types of safeguards

As a priority, the system must consider preventive safeguards that ensure that the threat does not occur or that its damage is minimal; that is, they must prevent incidents or attacks.

In practice, not everything can be foreseen, and not everything that can be foreseen can be eliminated in its origins within financial reason. Both to face the unknown and to protect against a threat to which the system is exposed, it is necessary to have elements available that detect when an incident occurs and allow a fast reaction to prevent its becoming a disaster.

Both preventive and emergency measures allow a certain degradation of the assets so it is necessary to have available means for recovery that retrieve the value lost by the assets.

Here, it is common sense to act preventively so that things cannot occur or so that not much damage is caused, but this is not always possible[18] and it is necessary to be prepared for what might happen. But an attack must never be allowed to occur unseen: it must be detected, recorded and acted against, firstly with an emergency plan (which stops the incident and limits it) and then with a plan for continuity and recovery to return to the original state.

Finally, and without wanting to overwhelm the reader, it must be remembered that a certain balance should be reached between:

Technical safeguards: in applications, equipment and communications.

Physical safeguards: protecting the working environment for persons and equipment.

Organisational measures: for preventing and managing incidents.

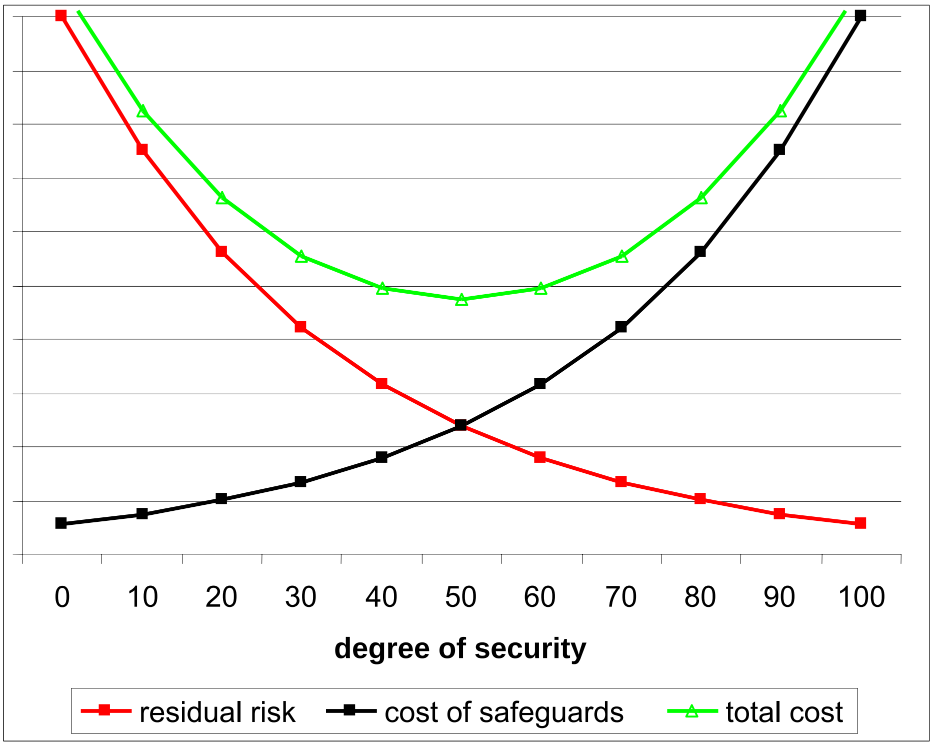
Personnel policy: which at the end of the day is the essential and most delicate step: a policy for hiring, permanent training, incident reporting organisation, reaction plans and disciplinary measures.

2.2.3. Profit and loss

Common sense dictates that the investment in safeguards cannot exceed the value of the assets to be protected.

In practice there are graphs such as the following one that compare the cost of insecurity (the cost of not being protected) and the cost of the safeguards.

[18] There are a thousand reasons that prevent absolute protection: cost, technical difficulty, legal limits, etc. However, one of the strongest reasons for not being able to prevent is mere lack of knowledge of what could happen. Something that occurred in the past can be prevented but it is difficult to foresee the next intentional attack since there is a creative component on the part of the attacker.



This type of graph tries to show how, in the progress from a security level of 0 towards a level of 100%, the cost of insecurity (the risk) reduces while the cost of investment in safeguards increases. It is intentional that the risk drops strongly with small investments[19] and that the cost of investments soars on reaching security levels close to 100%[20]. The central curve sums the cost for the organisation either from the risk (low security) or from the investment in protection. Somehow, there is a balance point between what is at risk and what is invested in defence - the critical point if the only consideration is financial.

But putting common sense into practice is not evident, neither in the part for calculating the risk nor in the part of calculating the cost of the safeguards. In other words, the above curve is a concept and cannot be applied to a real case.

In practice, there are various hypothetical scenarios when protecting oneself against a risk that is considered important:

E0: Nothing is done.

E1: A certain group of safeguards is applied.

E2: Another group of safeguards is applied.

And so forth for N scenarios with different combinations of safeguards.

The financial analysis must decide between these options, where E0 (not doing anything) is a possible option that may be financially justified.

The cost involved over time must be estimated for each scenario. To aggregate costs, financial losses are accounted as negative values and financial inputs as positive values. Consider the following components:

- (recurrent) residual risk [21]
- (once) cost of the safeguards [22]

[19] Basic security measures provide an important drop in the risk, which is why they are indispensable.

[20] Showing yet again that absolute security (zero risk) does not exist.

[21] If the frequency of threats has been estimated as an annual rate, the data for the residual risk must automatically be annual. If another scale has been used, it must be converted into annual terms.

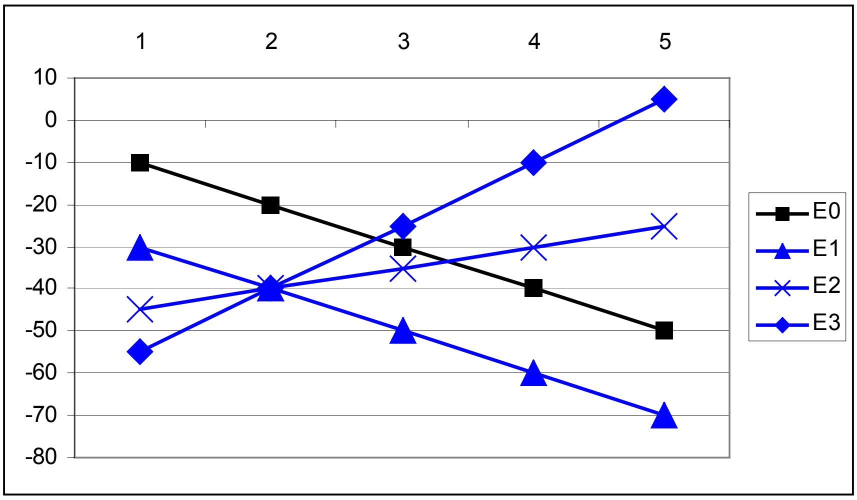
− (recurrent) annual cost of maintaining the safeguards.

+ (recurrent) improvement in productivity.[23]

+ (recurrent) improvement in the organisation's capability for providing new services, achieving better conditions from suppliers, entering into association with other organisations, etc.

The E0 scenario is very simple: each year there is a cost caused by the risk, which accumulates year after year.

In the other scenarios, there are things to be added and things to be subtracted, giving rise to various situations.[24]:



- In E0 it is known what (is estimated) to have been lost each year.
- The E1 scenario looks like a bad idea since it involves an added cost in the first year which is not recovered in the following years.
- The E2 scenario is different since it involves a greater initial outlay that starts to become profitable from the fourth year.
- The E3 scenario is even more attractive, in which the cost of an even larger initial outlay results in savings from the third year and even provides operational profits from the fifth year. The E3 scenario could be said to be a good investment.

2.2.4. Management attitude

The management of the organisation undergoing the risk analysis must determine the acceptable level of impact and risk. Put more correctly, it must accept responsibility for the deficiencies. This is not a technical decision; it may be a political or management decision or may be determined by law or by contractual undertakings with suppliers or users. These levels of acceptance can be set per asset or group of assets (in a specific department, in a specific service, in a specific dimension, etc).

[22] Cost of improvement if the safeguard already exists, otherwise, cost of acquisition and installation. In both cases, the costs of training for operators, users, etc, must be imputed.

[23] This section may be positive if the organisation improves its productivity or negative if it worsens. A typical example of safeguards that improve productivity would be the use of authentication devices instead of the classical password. A typical example of safeguards that reduce productivity would be the classification of documentation with restricted access control.

[24] The X axis shows years, referenced to year 0 in which the risk analysis is carried out; the costs are shown in arbitrary units.

Any level of impact and/or risk is acceptable if it is known and formally accepted by the management 25.

If the impact and/or risk is above the acceptable level, it is possible to:

1. Remove the asset. This is a strong measure but sometimes there are assets which, simply, are not worth keeping.[26]
2. Introduce new safeguards or improve the effectiveness of the existing ones.

2.2.5. Revision of step 1: assets

Some safeguards, especially technical ones, involve the deployment of more equipment[27] which, in turn, becomes an asset in the system. These assets support part of the system's value and are in turn subject to threats that may damage the valuable assets.

It is therefore necessary to repeat the risk analysis, enlarging it with the new deployment of media and, of course, ensuring that the risk to the enlarged system is less than that to the original system, that is, that the safeguards effectively reduce the organisation's risk status.

[25] To talk of management is to simplify reality. The term "stakeholders" is used to refer to those affected by the strategic decisions of an organisation: owners, managers, users, employees and even society in general, because at the end of the day, if unwisely high risks are accepted, those damaged may not only be the managers but everyone who puts confidence in the organisation whose sad performance obscures their legitimate expectations. In the final instance, the confidence in a sector or in a technology may be affected by the unwise actions of some of its members.

[26] Is it really necessary to maintain this personal and high-level data? Is the wireless network really necessary in the office?

[27] Typical examples would be a firewall, a system for managing private virtual networks, intelligent identification cards for users, a PKI, etc.

3. Structuring the project

The previous chapter described the concept of carrying out risk analysis and management; this chapter describes those concepts as parts of a risk analysis and management project (AGR) [28]. The steps are divided into three large processes (preparation, analysis and management). Each process is organised into activities which are structured into tasks to be carried out. For each task, what has to be done as well as the possible difficulties in doing it and the form of carrying it out successfully are described[29]. In each process, the milestones are given that show the progress of the project until its end.

Magerit covers a very wide spectrum of interests for its users. A “maximums” criterion has been used in planning these guides, reflecting all types of assets, all types of security aspects, all types of situations. In practice, the user may face situations in which the analysis is more restricted, the following being some frequent practical cases:

- A study is only required of files affected by legislation regarding personal data.
- A study is only required of the information confidentiality guarantees.
- A study is only required of communications security.
- A study is only required of perimeter security.
- A study is only required on the availability of services (typically because a contingency plan is to be developed).
- Approval or accrediting is required for the system or for a product.
- A security metrics project is to be launched, involving identification of which points should be controlled and at what frequency and in what detail.
- Etc.

These frequent situations are formally included in the tasks in activity A1.2 with the informal comments that it is constructive to concentrate on a reduced domain and then enlarge it according to needs rather than tackling the entirety.

As well as covering a more or less extensive domain, situations may arise that require a different type of analysis:

- An urgent analysis to determine the critical assets.
- An overall analysis to determine general measures.
- A detailed analysis to determine specific safeguards for certain elements in the information system.
- A detailed quantitative analysis to determine the opportunity for a high cost.
- Etc.

To summarise, the tasks described below must be adapted:

1. Horizontally to the required scope (activity A1.2).
2. Vertically to the appropriate depth.

3.1. Participants

The following groups[30] are involved in the AGR project from start to finish:

[28] Corresponds to the “Processes model” in Magerit version 1.0.

[29] Chapter 6 includes additional practical advice.

[30] It is important to formalise the roles of those participating in the project. This section identifies those roles and gives them standard names. Later, the moment (task) in a project at which they are formally constitu-

Management committee

This group of participants must include persons at a high level in the organisation's management who know the strategic and business objectives to be achieved and have the authority to validate and approve each process carried out during the project's evolution.

The responsibilities of this committee are:

- To assign the resources needed to carry out the project.
- To approve the final results of each process.

The Management Committee formalises its functions in task T1.3.2.

Tracking Committee

This consists of the persons responsible for the units affected by the project as well as by those responsible for computing and for management within these units. It is also important that services common to the organisation (planning, budget, human resources, government, etc) participate. In any case, the make-up of the committee will depend on the properties of the units affected.

The responsibilities of this committee are:

- To resolve incidents during the evolution of the project.
- To ensure the availability of human resources with suitable qualifications and their participation in those activities in which their collaboration is necessary.
- To approve the intermediate and final reports of each process.
- To prepare the final reports for the Management Committee.

The Tracking Committee is created in task T1.1.1 and its functions are formalised in T1.3.2.

Project team

This consists of experts in technologies and information systems and technical personnel with qualifications in the affected domain, with knowledge of security management in general and of the application of the risk analysis and management methodology specifically. If the project is carried out with technical assistance through external contractor, persons specialising in information systems security must form part of this project team.

The responsibilities of this team are:

- To carry out the project tasks.
- To compile, process and consolidate data.
- To prepare the reports.

The project team is determined in task T1.3.2.

Delegates' groups

This is formed of representative users from within the units affected by the project and consists of various possible sub-groups:

- Those responsible for the service and who are aware of the organisation's mission and its medium and long term strategies.
- Those responsible for internal services.
- Computer services operational personnel who are aware of the media deployed (production and safeguards) and of usual incidents.

The units affected are determined in tasks T1.2.2 and T1.2.3. The delegates are identified in task T1.3.1.

Some other individual roles must be identified as well as these groups:

ted is described.

Promoter

A person who leads the first tasks in the project, defining its opportunity and scope to launch the AGR project itself.

This must be a person with an overview of the information systems and their role in the organisation's activities without needing to know the details but aware of the incidents.

The promoter's role is defined in task T1.1.1.

Project manager

This must be a high-level manager with responsibilities within the organisation for security, information systems or planning, co-ordination or materials, services or similar areas.

This is the visible head of the project team.

The project manager is designated in task T1.2.2.

Operational link

This must be a person in the organisation with a good knowledge of the persons and units involved in the AGR project and who can connect the project team to the users group.

He is the visible face of the Tracking Committee.

The operational link is designated in task T1.3.2.

It should be remembered that an AGR project is always mixed because of its very nature; that is, it requires the permanent involvement of specialists and users in both the preparatory phases and during its undertaking. The operational link has a permanent relevance that is not as usual in other types of more technical projects.

3.2. Project undertaking

This section describes and formalises the actions to be carried out during an AGR project, setting a standardised development framework that defines:

1. A project structure that serves as a guide for the work team and that allows the involvement in it of managers and users.
2. A group of products to be obtained.
3. A group of techniques to obtain the products.
4. The functions and responsibilities of the participants.

The project is divided into three large processes, each broken down into a series of activities and these, in turn, into tasks which are as detailed as required.

Each task specifies the following items:

- Actions to be carried out.
- Input data.
- Output data: products and documents to be obtained as a result of the actions.
- Recommended techniques for successfully terminating the task's objectives.
- Participants who are involved in or are affected by the undertaking of the actions.

An AGR project involves three processes:

Process P1: Planning

- Consider the approach needed to start the AGR project.
- Investigate the opportunity for carrying it out.
- Define the objectives to be met and the domain (reach) covered.
- Plan the material and human resources needed for its undertaking.
- Launch the project.

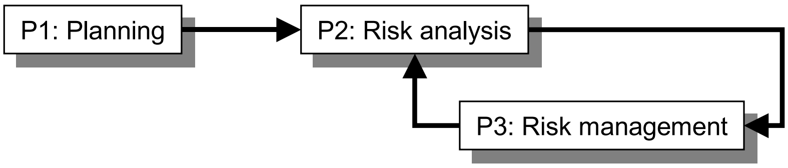
Process P2: Risk analysis

- Identify the assets to be dealt with, the relationships between them and their valuation.
- Identify the important threats to those assets and their value in terms of frequency of occurrence and the degradation they cause to the value of the affected asset.
- Identify the existing safeguards and evaluate the effectiveness of their implementation.
- Estimate the impact and risk to which the assets in the system are exposed.
- Interpret the meaning of the impact and risk.

Process P3: Risk management

- Choose a strategy to mitigate the impact and risk.
- Determine the appropriate safeguards for the above objective.
- Determine the quality needed for these safeguards.
- Design a security plan (action plan or master plan) to reduce the impact and risk to acceptable levels.
- Carry out the security plan.

These three processes are not necessarily sequential. Process P1 is clearly the project trigger. Process P2 supports process P3 in the sense that Risk management (P3) is a continuous task supported by the analysis techniques (P2). Risk management always involves alterations to the group of safeguards either because new safeguards appear or because some are replaced with others or the existing ones are improved. Risk management may involve the alteration of the group of assets[31], either because new assets appear (safeguard elements that become part of the system) or because assets are removed from the system. In short, tasks from process P2 appear throughout the P3 process.



A series of documents of general interest is generated throughout these processes[32]:

P1: Planning

- Types of assets.
- Relevant security dimensions.

[31] Formally, it is said that the introduction of safeguards to reduce certain risks may introduce new risks to the system.

[32] Without including the working documents for the AGR project itself, which are detailed in the tasks.

- Evaluation criteria.

P2: Risk analysis

- Value model.
- Risk map.
- Safeguard evaluation.
- Risk status.
- Deficiencies report.

P3: Risk management

- Security plan.

3.2.1. Overview

Without prejudice to a detailed discussion later, the following lists the complete tree of processes, activities and tasks in an AGR project.

Processes, activities and tasks
Process P1: Planning Activity A1.1: Opportunity study: Task T1.1.1: Determine the opportunity. Activity A1.2: Determine the scope of the project. Task T1.2.1: General objectives and restrictions. Task T1.2.2: Determination of the domain and limits. Task T1.2.3: Identification of the environment. Task T1.2.4: Estimate of dimensions and costs. Activity A1.3: Project planning: Task T1.3.1: Evaluate loads and plan interviews. Task T1.3.2: Organise the participants. Task T1.3.3: Plan the work. Activity A1.4: Launch the project: Task T1.4.1: Adapt the questionnaires. Task T1.4.2: Evaluation criteria. Task T1.4.3: Resources needed. Task T1.4.4: Awareness.
Process P2: Risk analysis Activity A2.1: Characterisation of assets: Task T2.1.1: Identification of assets. Task T2.1.2: Dependencies between assets. Task T2.1.3: Valuation of assets. Activity A2.2: Characterisation of threats: Task T2.2.1: Identification of threats. Task T2.2.2: Valuation of threats. Activity A2.3: Characterisation of safeguards: Task T2.3.1: Identification of existing safeguards. Task T2.3.2: Valuation of existing safeguards. Activity A2.4: Estimate of the risk status: Task T2.4.1: Estimate of the impact. Task 2.4.2: Estimate of the risk. Task 2.4.3: Interpreting the results.
Process P3: Risk management Activity A3.1: Decision making: Task A3.1.1: Classification of risks. Activity A3.2: Security plan: Task T3.2.1: Security programmes. Task T3.2.2: Undertaking plan. Activity A3.3: Carrying out of plan: Task T3.3.*: Carrying out of each security programme.

3.3. Process P1: Planning

The main objective of this process is to set a general reference framework for the entire project.

The following can be identified as complementary objectives:

- To motivate, make aware and involve the organisation's management.
- To explain the opportunity of carrying out an AGR project.
- For the management to confirm and announce its wish to carry it out.
- To create the human and material conditions to successfully carry out the project.

This process is carried out using the following activities and tasks:

Activity A1.1: Opportunity study

The opportunity for carrying out the AGR project now is described, framed within the evolution of the other activities of the organisation.

The result of this activity is the "preliminary" report.

Tasks:

Task T1.1.1: Determine the opportunity.

Activity A1.2: Determine the scope of the project

The final objectives, domain and limits of the project are defined. A preliminary identification of the environment and the general restrictions to be considered is made. And finally, the cost involved is estimated.

The result of this activity is an AGR project profile.

Tasks:

Task T1.2.1: General objectives and restrictions.

Task T1.2.2: Determination of the domain and limits.

Task T1.2.3: Identification of the environment.

Task T1.2.4: Estimate of dimensions and costs.

Activity A1.3: Project planning

The work load in carrying out the project is determined. The interviews to be made for collecting information are planned: who is to be interviewed. A working plan is prepared for carrying out the project.

In this activity, the participants are determined and the groups and committees to carry out the project are structured.

The result of this activity consists of:

- A working plan for the AGR project.
- Procedures for managing the information generated.

Tasks:

Task T1.3.1: Evaluate loads and plan interviews.

Task T1.3.2: Organise the participants.

Task T1.3.3: Plan the work.

Activity A1.4: Launch the project

The questionnaires for collecting information are adapted to the current project. The main techniques to be used for evaluating the risk are chosen and the resources needed to start the project are assigned. An awareness campaign is also carried out for those affected on the purposes and requirements of their participation.

The result of this activity consists of:

- The questionnaires for the interviews.
- The interviews plan.
- The catalogue of types of assets.
- The list of security dimensions.
- The evaluation criteria.

Tasks:

Task T1.4.1: Adapt the questionnaires.

Task T1.4.2: Evaluation criteria.

Task T1.4.3: Resources needed.

Task T1.4.4: Awareness.

3.3.1. Activity A1.1: Opportunity study

This consists of a single task:

T1.1.1: Determine the opportunity.

P1: Planning
A1.1: Opportunity study
T1.1.1: Determine the opportunity

Objectives

- To identify or arouse the interest of the organisation’s management in carrying out an AGR project.

Input products

Output products

- **Preliminary report** recommending the preparation of the AGR project.
- Awareness and support from the management for carrying out the AGR project.
- Creation of the Tracking Committee.

Techniques, practices and guidelines

1. Interviews (see “Guide to techniques” 3.6.1)

- Meetings (see “Guide to techniques” 3.6.2)

Participants

- The promoter.

Management is usually very aware of the advantages of electronic, computer and telematic techniques for its operations but not so aware of the new security problems that these techniques imply or the legal or regulatory obligations that affect them.

In all public and private organisations, it is important to transform the growing preoccupation with the lack of security in information systems, with the media and environment, into specific measures since their effects do not only affect the systems but also the very functioning of the organisation and, in critical situations, its mission and capacity for survival.

Development

The initiative for carrying out an AGR project comes from a promoter inside or outside the organisation who is aware of the problems related to security in information systems such as:

- Continuous security-related incidents.
- The lack of provisions in matters related to the evaluation of needs and means to reach an acceptable level of security in information systems that is compatible with the correct undertaking of the organisation’s mission and functions.
- Restructuring in the products or services provided.
- Changes in the technology used.
- Development of new information systems.

The promoter may prepare a **framework questionnaire** (a document that is difficult to systematise and that must be created for each specific case) to encourage thought on security aspects in the information systems by:

Those responsible for the operational units (responsible for services)

The questionnaire allows the situation regarding security in their information systems to be examined formally. They must be able to express their opinions on the security projects already carried out (with their degree of satisfaction or with the limits of these) and their expectations with regard to the preparation of an AGR project[33]. This high-level approach provides a first view of the specific objectives and options that must underlie the preparation of the project.

Those responsible for computing

The questionnaire provides a technical panorama for the preparation of the project and also the opportunity for studying its undertaking after including the above options.

The answers from the framework questionnaire and the interviews with the above managers and groups gives the promoter a first approach to the functions, services and products involved in security matters in the information systems, their geographical location, the technical means, human means, etc.

With these elements, the promoter prepares the **preliminary report**, recommending the preparation of the AGR project and including these items:

- A discussion of the basic arguments.
- A list of the antecedents regarding security in information systems (strategic plan, action plan, etc).
- A first approach to the domain to be included in the project depending on:
    - The purposes of the units or departments.
    - The management orientations and techniques.
    - The organisational structure.
    - The technical environment.
- A first approach to the human and material means for carrying out the AGR project.

The promoter presents this preliminary report to the management, which may decide to:

- Approve the project, or,
- Change its domain and/or objectives, or,
- Delay the project.

[33] They probably do not know what this means and it is necessary to include a short explanation in the framework questionnaire of what an AGR project is and what its objectives are.

3.3.2. Activity A1.2: Determine the scope of the project

Once the opportunity of carrying out an AGR project is clear and has the support of management, this activity estimates the project planning elements, that is, the participants and their work loads.

This estimate must take into account the possible existence of other plans (for example, a strategic information systems plan or general security plan in the units that may be affected or in the organisation) and the period considered for putting the AGR project into practice. Specifically, the existence of a strategic information systems plan for the units that may be affected within the organisation may greatly determine the scope and extension of the activities carried out in this activity.

This activity consists of four tasks:

T1.2.1: General objectives and restrictions.

T1.2.2: Determination of the domain and limits.

T1.2.3: Identification of the environment.

T1.2.4: Estimate of dimensions and costs.

P1: Planning ***A1.2: Determine the scope of the project*** ***T1.2.1: General objectives and restrictions***
Objectives • To determine the project’s short and medium term objectives. • To determine the general restrictions on the project.
Input products • Compilation of the organisation’s relevant documentation.
Output products • Detailed specification of the project’s objectives. • List of general restrictions.
Techniques, practices and guidelines • Interviews (see “Guide to techniques” 3.6.1). • Meetings (see “Guide to techniques” 3.6.2).
Participants • The Tracking Committee

An AGR project may have short term objectives such as ensuring a specific system or specific business process or may have wider objectives such as the overall analysis of the organisation’s security. In both cases this must be determined.

Especially when implementing corrective actions, it must be remembered that “not everything goes” but that the project has a series of restrictions, not necessarily technical, that set a framework to be adhered to. In order to include the restrictions in the risk analysis and management, they are grouped by different concepts, typically:

Political or management restrictions:

Typical of governmental organisations or those strongly related with governmental organisations, either as suppliers or as suppliers of services.

Strategic restrictions:

Arising from the forecast development of the organisation’s structure or objectives.

Geographical restrictions:

Arising from the organisation’s physical location or its dependence on physical means of communication: islands, sites beyond frontiers, etc.

Time restrictions:

Taking into consideration collateral situations: labour conflicts, international crises, change of ownership, re-engineering of processes, etc.

Structural restrictions:

Taking the internal organisation into consideration: decision-making procedures, dependency on international parent companies, etc.

Functional restrictions:

Taking the organisation’s objectives into account.

Legal restrictions:

Laws, regulations, sector regulations, external and internal contracts, etc.

Restrictions relating to personnel:

Working profiles, contractual undertakings, trade union undertakings, professional careers, etc.

Methodological restrictions:

Arising from the nature of the organisation and its working habits or abilities that may impose a certain way of doing things.

Cultural restrictions:

The “culture” or internal way of working may be incompatible with certain theoretically ideal safeguards.

Budgetary restrictions:

The amount of money is important but so is the way of planning the cost and managing the budget.

P1: Planning
A1.2: Determine the scope of the project
T1.2.2: Determination of the domain and limits

Objectives

- To determine the domain, scope or perimeter of the AGR project.

Input products

- Results of task T1.2.1, General objectives and restrictions.
- General profile of the units within the project's domain.

Output products

- List of units in the organisation that will be affected as part of the project's domain.
- List of relevant roles in the units within the domain.
- Designation of the project manager.

Techniques, practices and guidelines

- Process charts (see "Guide to techniques" 3.3).

Participants

- Those responsible for the units in the organisation.
- The Tracking Committee

This task identifies the units that form the target of the AGR project and specifies their general features with regard to persons responsible, services provided and geographical locations. It also identifies the main relationships of the units in the project with other entities such as the exchange of information on various media, access to common computer media, etc.

The task involves a basic principle: risk analysis and management must be centred on a limited domain that may include various units or be kept within a single unit (depending on the complexity and type of problem to be handled) since a project with a reach that is too wide or indeterminate may be impractical because it is excessively generalised or too long, to the prejudice of the estimates of the elements in the analysis.

P1: Planning
A1.2: Determine the scope of the project
T1.2.3: Identification of the environment

Objectives

- To define the perimeter of the domain.
- To define the relationships between the interior of the domain and the environment.

Input products

- Results of task T1.2.1, General objectives and restrictions.
- Results of task T1.2.2, Determination of the domain and limits.
- Diagram of the relationships of the units in the domain with the environment.
- Data flow charts.

Output products

- List of the units in the organisation that will be affected as the perimeter of the domain.
- List of relevant roles in other units to be considered for defining the environment.

P1: Planning
A1.2: Determine the scope of the project
T1.2.3: Identification of the environment

Techniques, practices and guidelines

- Data flow charts (see “Guide to techniques” 3.2).
- Process charts (see “Guide to techniques” 3.3).
- Interviews (see “Guide to techniques” 3.6.1).
- Meetings (see “Guide to techniques” 3.6.2).

Participants

- Those responsible for the units in the domain.
- The Tracking Committee

This task carries out an overall study of the information systems in the units in the project’s domain to identify their main functions and purposes and their relationships with the environment as well as their development trends. The general profile of the units - obtained in the previous task - is enlarged in this task with the information provided by those responsible for the areas in these units.

P1: Planning
A1.2: Determine the scope of the project
T1.2.4: Estimate of dimensions and costs

Objectives

- To determine the volume of resources needed to carry out the AGR project: human, time and financial.

Input products

- Results of task T1.2.1, General objectives and restrictions.
- Results of task T1.2.2, Determination of the domain and limits.
- Results of task T1.2.3, Identification of the environment.

Output products

- Size of the project.
- Costs and benefits of the project.

Techniques, practices and guidelines

- Cost/benefit analysis (see “Guide to techniques” 3.1).
- Project planning (see “Guide to techniques” 3.5).

Participants

- The project manager.

This task enables the dimensioning of the project (size, complexity, areas of uncertainty) based on knowledge of its objectives, domain and the profile of the units included in the study. The techniques to be used in the project are chosen according to the estimated dimension and objectives. For example, if the purpose of the project is to carry out an initial generic analysis, the technique for calculating the risks will be based on a discrimination in two blocks of the risks depending on whether or not more detailed analysis applications are required.

The task also dimensions the project with regard to its cost and the return or benefits it may provide so that management has a basis for deciding on its undertaking and for assigning the resources needed for its development.

- The study of the project’s cost is carried out by estimating the times and profiles of the personnel assigned to the stages of the previously dimensioned project.
- The study of the return can only be very imprecise in this initial process since it is still not possible to take into account the real return of a security project, which is precisely the cost of not having this security in the domain under study, that is, the result of the AGR project itself.

3.3.3. Activity A1.3: Project planning

In this activity the participants in the project, their work loads, their structuring into groups and their mode of acting are determined.

This activity consists of three tasks:

T1.3.1: Evaluate loads and plan interviews.

T1.3.2: Organise the participants.

T1.3.3: Plan the work.

P1: Planning ***A1.3: Project planning*** ***T1.3.1: Evaluate loads and plan interviews***
Objectives • To define the groups of delegates: the users affected in each unit. • To plan the interviews for collecting information.
Input products • Results of activity A1.2, Determine the scope of the project.
Output products • List of participants in the delegates' groups. • Plan of interviews. • Loads report.
Techniques, practices and guidelines • Project planning (see "Guide to techniques" 3.5).
Participants • The project manager. • The Tracking Committee.

The plan of interviews must detail who is to be interviewed, when and with what purpose. This plan allows the determination of the load that the project will imply for the affected units, either in the domain or in the environment.

The plan of interviews is especially important when the subjects to be interviewed are in different geographical locations and the interviewing requires the movement of one or other of the parties.

It is also useful to arrange interviews so that the most technical opinions are collected first and then those of management so that the interviewer can develop questions using facts (historical experience) before valuations and perspectives of the service to third parties.

P1: Planning
A1.3: Project planning
T1.3.2: Organise the participants

Objectives

- To determine the entities participating in the management, undertaking, tracking and maintenance of the project.
- To define the functions and responsibilities of the participating entities.
- To set the operating rules and modes.
- To set the classification of the information generated.

Input products

- Results of activity A1.2, Determine the scope of the project.

Output products

- Formalisation of the Management Committee.
- Formalisation of the Tracking Committee.
- Criteria and procedures for classifying and managing the information generated.
- Designation of the operational link.
- Creation of the work team.

Techniques, practices and guidelines

Not applicable.

Participants

- Tracking Committee.
- Project manager.

Although all AGR projects involve basically the same committees, in this case the generic approach is moulded to the specific case; it can follow the general case or a specific one.

It is particularly relevant to determine the classification of the documents produced during the project. If there is a classification standard, it should be adhered to in order to take advantage of the procedures already set up for handling documents; otherwise, it is necessary to prepare both the classification criteria and the handling procedures. The default classification will be “confidential,” it being particularly important to maintain the confidentiality of the documentation for the evaluation of safeguards and of deficiencies.

P1: Planning
A1.3: Project planning
T1.3.3: Plan the work

Objectives

- To prepare the schedule for carrying out the stages, activities and tasks in the project.
- To set a tracking schedule that defines the tentative dates for meetings of the Management Committee, the plan for delivering the project's products, possible changes to the objectives set, etc.

Input products

- Results of activity A1.2, Determine the scope of the project.
- Results of task T1.3.1, Evaluate loads and plan interviews.
- Results of task T1.3.2, Organise the participants.

Output products

- Project schedule.
- Participants' dedication.
- Specification of the necessary material resources.
- Description of milestones.

Techniques, practices and guidelines

- Project planning (see "Guide to techniques" 3.5).

Participants

- The project team.

3.3.4. Activity A1.4: Launch the project

This activity completes the preparatory tasks for launching the project, starting with choosing and adapting the questionnaires used to collect data and specifying the criteria and techniques to be used, and ending by assigning the resources needed to carry out the project and carrying out the awareness campaign for those involved.

This activity consists of four tasks:

T1.4.1: Adapt the questionnaires.

T1.4.2: Evaluation criteria.

T1.4.3: Resources needed.

T1.4.4: Awareness.

P1: Planning ***A1.4: Launch the project*** ***T1.4.1: Adapt the questionnaires***
Objectives • To identify the relevant information to be obtained, grouped according to the structure of the units and the participants' roles.
Input products • Results of activity A1.3, Project planning.
Output products • Adapted questionnaires.
Techniques, practices and guidelines • Questionnaires (see "Elements catalogue" in general and specifically Appendix 2).
Participants • The project team.

The task adapts the questionnaires to be used to collect information in process P1 to the project's objectives, the domain and the matters to be discussed with the users.

The questionnaires are adapted in order to identify the work elements correctly - assets, threats, vulnerabilities, impact, existing safeguards, general restrictions, etc - in preparation for the needs of activities A2.1 (characterisation of assets), A2.2 (characterisation of threats) and A2.3 (characterisation of safeguards).

Adaptation is always necessary (because of the very wide range of security problems that can and must be handled by Magerit) but the degree of adaptation depends also on the conditions in which these questionnaires are used. Interviews guided by the security specialist would not require the same degree of adaptation as those self-administered by the person responsible for the domain or by the users of the information systems.

P1: Planning
A1.4: Launch the project
T1.4.2: Evaluation criteria

Objectives

- To determine the catalogue of types of assets.
- To determine the dimensions of the valuation of assets.
- To determine the levels of the valuation of assets including a unified guide of criteria for assigning a certain level to a certain asset.
- To determine the levels of the evaluation of threats: frequency and degradation.

Input products

- Elements catalogue.
- Results of activity A1.3, Project planning.

Output products

- Catalogue of types of assets.
- List of security dimensions.
- Valuation criteria.

Techniques, practices and guidelines

- See “Elements catalogue” chapters 2, 3 and 4.

Participants

- The project team.

This task is preparation for process P2 (Risk Analysis) and sets the choice of the criteria and techniques to be used throughout the process. In fact the Risk management in process P3 is conditioned by the type of analysis carried out in process P2. If a type of criteria and techniques for evaluating the risks has been chosen, the same technique should be applied to evaluate the reduction of risks when the proposed safeguards are implemented. The choice of these criteria and techniques depends on:

- The project’s objectives (T1.2.1).
- The project’s domain (T1.2.2).

The proposals in the “Elements catalogue” book, attached to this guide, should be used.

P1: Planning
A1.4: Launch the project
T1.4.3: Resources needed

Objectives

- To assign the resources needed (human, organisational, technical, etc) for carrying out the AGR project.

Input products

- Results of activity A1.3, Project planning.

Output products

- Communications to the participating personnel of their assignation to the project.
- Availability of the necessary material resources.

Techniques, practices and guidelines

- Project planning (see “Guide to techniques” 3.5).

Participants

- The Tracking Committee.

P1: Planning ***A1.4: Launch the project*** ***T1.4.4: Awareness***
Objectives • To inform the affected units. • To create an atmosphere of general knowledge of the objectives, those responsible and the schedules.
Input products • Results of activity A1.3, Project planning.
Output products • Information note from the management. • Material and report presenting the project.
Techniques, practices and guidelines • Presentations (see “Guide to techniques” 3.6.3).
Participants • The project manager. • The Tracking Committee. • The operational link. • The project team.

This task reports the launch of the AGR project to the affected units by various means and at least:

- An information note from management to the units involved, giving their support for carrying out project.
- The presentation of the project, its objectives and the methodology to be used, carried out by the project team in the units involved.

3.3.5. Synthesis of process P1

3.3.5.1. Control milestones

Control milestone H1.1:

Management must approve or not the undertaking of the AGR project on the basis of the opportunity study carried out by the promoter.

Control milestone H1.2:

The project Management Committee must validate the “Risk analysis and management project planning” report containing a synthesis of the products from the activities carried out in the P1 process.

3.3.5.2. Results

Intermediate documentation

- Results of the interviews.
- Documentation from other sources: statistics, comments from experts and comments from the analysts.
- Additional documentation: drawings, organisational charts, requirements, specifications, functional analysis, work books, user manuals, operating manuals, flow charts for information and processes, data models, etc.
- Analysis of the results, with the detection of the critical key areas.
- Existing information that can be used for the project (for example, assets inventory).
- Results of any applications of risk analysis and management methods carried out previously (for example, cataloguing, grouping and valuation of assets, threats, vulnerabilities, impacts, risk, safeguard mechanisms, etc).

Final documentation

- Types of assets.
- Relevant security dimensions.
- Evaluation criteria.
- “Risk analysis and management project planning” report containing a synthesis of the products from the activities carried out in process

3.3.6. Process P1 checklist[34]

Project organisation

√ Management approval (P1).

√ Explicit commitment from management (P1).

√ Management support (P1).

√ Tracking Committee (T1.3.2).

√ Project team (T1.3.2).

√ Project manager (T1.2.2).

√ Operational link (T1.3.2).

[34] This list provides a check that all the objectives, sub-objectives and output products detailed in the tasks have been achieved.

- √ Groups of delegates (T1.3.1).
- √ Functions and working method (T1.3.2).
- √ Criteria for documentation classification and procedures for handling it (T1.3.2).

Project planning

- √ Preliminary report recommending and justifying the opportunity for launching an AGR project (T1.1.1).
- √ Specific and unambiguous objectives (T1.2.1).
- √ Estimate of dimensions and costs (T1.2.4).
- √ Plan of interviews: persons and dates (T1.4.3).
- √ Work plan: milestones (T1.3.3).
- √ Assignation of resources (T1.4.3).
- √ Awareness of the organisation (T1.4.4).
- √ Risk analysis and management project plan (P1).

Technical aspects

- √ General project limitations (T1.2.1).
- √ Project domain: units included in the analysis (T1.2.2).
- √ Project environment: other units related in some way (T1.2.3).
- √ Adapted questionnaires (T1.4.1).
- √ Catalogue of types of assets (T1.4.2).
- √ List of relevant security dimensions (T1.4.2).
- √ Evaluation criteria (T1.4.2).

3.4. Process P2: Risk analysis

This process is the central core of Magerit and its correct application governs the validity and usefulness of the entire project. The identification and estimation of the assets and any threats to them is a complex task.

This process has the following objectives:

- To provide a model of the system's value, identifying and valuing the relevant assets.
- To provide a Risk map of the system, identifying and valuing the threats to those assets.
- To provide knowledge of the current safeguards situation.
- To evaluate the possible impact to the system under study, both the potential impact (without safeguards) and the residual impact (including the effect of the safeguards implemented, if dealing with a current system, otherwise of a planned system).
- To evaluate the possible risk to the system under study, both the potential risk (without safeguards) and the residual risk (including the effect of the safeguards implemented, if dealing with a current system, otherwise of a planned system).
- To show the Management Committee the areas of the system with the greatest impact and/or risk.

The starting point for this process is the documentation from the previous one referring to the project's objectives, the plans for interviews, evaluation of work loads, the composition and rules for action for the team of participants, the work plan and the report presenting the project.

This process is carried out using the following activities and tasks:

Activity 2.1: Characterisation of assets

This activity identifies the relevant assets in the system to be analysed, classifying them by type of asset, identifying the relationships between the assets, determining which security dimensions are important and valuing this importance.

The result of this activity is the "Value model" report.

Tasks:

Task T2.1.1: Identification of assets.

Task T2.2.2: Dependencies between assets.

Task T2.3.3: Valuation of assets.

Activity 2.2: Characterisation of threats

This activity identifies the relevant threats to the system being analysed, classifying them by their estimated frequency of occurrence and the estimate of the damage (degradation) that they would cause to the assets.

The result of this activity is the "Risk map" report.

Tasks:

Task T2.2.1: Identification of threats.

Task T2.2.2: Valuation of threats.

Activity 2.3: Characterisation of safeguards

This activity identifies the safeguards deployed in the system being analysed, classifying them by their effectiveness against the threats they are designed to prevent.

The result of this activity is the "Safeguards evaluation" report.

Tasks:

Task T2.3.1: Identification of existing safeguards.

Task T2.3.2: Valuation of existing safeguards.

Activity 2.4: Estimate of the risk status

This activity processes all the data compiled in the previous activities in order to:

- Prepare a risk status report: estimate of impact and risk.
- Prepare a deficiencies report: deficiencies or weaknesses in the safeguards system.

Tasks:

Task T2.4.1: Estimate of the impact.

Task T2.4.2: Estimate of the risk.

Task T2.4.3: Interpreting the results.

3.4.1. Activity A2.1: Characterisation of assets

This activity consists of three tasks:

T2.1.1: Identification of assets.

T2.1.2: Dependencies between assets.

T2.1.3: Valuation of assets.

The objective of these tasks is to recognise the assets in the processes and to define the dependencies between them. Based on the information compiled in the previous activity, this activity deepens the study of the assets with a view to obtaining the necessary information for estimating the risk.

Frequently, the tasks relating to the assets are carried out concurrently with those relating to the threats to them (A2.2) and the identification of current safeguards (A2.3) simply because the persons tend to coincide and it is difficult for them to avoid treating each asset “vertically,” seeing everything that affects it before moving on to the next one.

P2: Risk analysis
A2.1: Characterisation of assets
T2.1.1: Identification of assets

Objectives

- To identify the assets in the domain, determining their features, attributes and classification in the specific types.

Input products

- Inventories of the data handled by the organisation.
- Business processes.
- Use diagrams.
- Data flow charts.
- Inventories of logical equipment.
- Inventories of physical equipment.
- Functional classification of the work posts.
- The organisation’s premises and sites.

Output products

- List of assets to be considered.
- Characterisation of assets.

Techniques, practices and guidelines

- Data flow charts (see “Guide to techniques” 3.2).
- Process charts (see “Guide to techniques” 3.3).
- Interviews (see “Guide to techniques” 3.6.1).
- Meetings (see “Guide to techniques” 3.6.2).
- See also section 2.1.1.

Participants

- The project team.
- The delegates’ groups.

This task is critical. Good identification is important from various points of view:

- It precisely defines the scope of the project.
- It enhances communication with the user groups: everyone speaks the same language.
- It allows the determination of the precise dependencies between assets.
- It allows the assets to be valued precisely.
- It allows the threats to be identified and valued precisely.

Characterisation of assets

It is necessary to determine a series of features that define each asset:

- Code, typically from the inventory.
- Name (short).
- Description (long).
- Type (or types) of the asset.

- Unit responsible. Sometimes there is more than one unit. For example, in the case of applications, it is necessary to differentiate between the unit that maintains it and the one that uses it.
- Person responsible. Especially relevant in the case of data. Sometimes more than one person is responsible. For example, in the case of personal data, it is necessary to differentiate between the person responsible for the data and the operator who handles it.
- Location: technical (in intangible assets) or geographical (in material assets).
- Quantity, if relevant, such as in the case of personal computing (for example, 350 desktop systems).
- Other features that are specific to the type of asset.

P2: Risk analysis ***A2.1: Characterisation of assets*** ***T2.1.2: Dependencies between assets***
Objectives • To identify and value the dependencies between assets, that is, the measure to which a higher order asset can be prejudiced by a threat occurring in a lower order asset.
Input products • Results of task T1.2.1, Identification. • Business processes. • Data flow charts. • Use diagrams.
Output products • Diagram of dependencies between assets.
Techniques, practices and guidelines • Data flow charts (see “Guide to techniques” 3.2). • Process charts (see “Guide to techniques” 3.3). • Interviews (see “Guide to techniques” 3.6.1). • Meetings (see “Guide to techniques” 3.6.2). • Delphi evaluation (see “Guide to techniques” 3.7). • See also section 2.1.1.
Participants • The project team. • The delegates’ groups.

It is useful to record the following information for each dependency:

- An estimate of the degree of dependency: up to 100%.
- An explanation of the valuation of the dependency.
- Interviews which support the above estimate.

P2: Risk analysis
A2.1: Characterisation of assets
T2.1.3: Valuation of assets

Objectives

- To identify the dimension in which the asset is valuable.
- To evaluate the cost to the organisation of the destruction of the asset.

Input products

- Results of task T1.4.2, Evaluation criteria.
- Results of task T2.1.1, Identification of assets.
- Results of task T2.1.2, Dependencies between assets.

Output products

- **Value model**: reports of the assets’ value.

Techniques, practices and guidelines

- Interviews (see “Guide to techniques” 3.6.1).
- Meetings (see “Guide to techniques” 3.6.2).
- Delphi evaluation (see “Guide to techniques” 3.7).
- See also section 2.1.1.

Participants

- The project team.
- The delegates’ groups.
- The Tracking Committee.
- Management.

It may be necessary to interview different groups within the organisation to acquire this knowledge:

- Management, which knows the consequences for the organisation’s mission.
- Those responsible for the services, who know the consequences of not providing a service or of providing a degraded service.
- Those responsible for the data, who know the consequences of data degradation.
- Those responsible for the information systems and their operation, who know the consequences of an incident.

It is useful to record the following information for each valuation:

- The dimensions in which the asset is relevant.
- An estimate of the value in each dimension.
- An explanation of the valuation.
- Interviews from which the above estimates have been deduced.

3.4.2. Activity A2.2: Characterisation of threats

This activity is usually carried out concurrently with activities A2.1 and A.2.3, given that the people to be interviewed are the same.

This activity consists of two tasks:

T2.2.1: Identification of threats.

T2.2.2: Valuation of threats.

P2: Risk analysis ***A2.2: Characterisation of threats*** ***T2.2.1: Identification of threats***
Objectives • To identify the relevant threats to each asset.
Input products • Results of task T1.4.2, Evaluation criteria. • Results of activity A2.1, Characterisation of assets.
Output products • List of possible threats.
Techniques, practices and guidelines • Catalogue of threats (see “Elements catalogue”, chapter 5). • Attack trees (see “Guide to techniques” 2.3). • Interviews (see “Guide to techniques” 3.6.1). • Meetings (see “Guide to techniques” 3.6.2). • Delphi evaluation (see “Guide to techniques” 3.7). • See also section 2.1.2.
Participants • The project team. • The delegates’ groups.

In this task, the important threats to the assets are identified, taking into consideration:

- The type of asset.
- The dimensions in which the asset is valuable.
- The organisation’s experience.

It is useful to record the following information for each threat to each asset:

- An explanation of the effect of the threat.
- Interviews from which the above estimate has been deduced.
- Background, if any, either within the organisation itself or in other organisations considered relevant.

P2: Risk analysis
A2.2: Characterisation of threats
T2.2.2: Valuation of threats

Objectives

- To estimate the frequency at which each threat occurs to each asset.
- To estimate the degradation that the threat would cause in each of the asset's dimensions if it occurs.

Input products

- Results of task T1.4.2, Evaluation criteria.
- Results of task T2.2.1, Identification of threats.
- Incident logs.
- Background: incidents in the organisation.

Output products

- **Risk map**: Report on possible threats, according to their frequency of occurrence and the degradation they would cause to the assets.

Techniques, practices and guidelines

- Attack trees (see "Guide to techniques" 2.3).
- Interviews (see "Guide to techniques" 3.6.1).
- Meetings (see "Guide to techniques" 3.6.2).
- Delphi evaluation (see "Guide to techniques" 3.7).
- See also section 2.1.2.

Participants

- The project team.
- The delegates' groups.

The threats identified in the previous task are evaluated in this task, taking into consideration:

- Universal experience (history).
- Experience (history) in the activity sector.
- Experience (history) in the environment in which the systems are located.
- Experience (history) of the organisation itself.

Knowing that there is a series of possible problems as described in Section X,

it is useful to record the following information for each threat to each asset:

- An estimate of the frequency of the threat.
- An estimate of the damage (degradation) that its occurrence would cause.
- An explanation of the estimates of frequency and degradation.
- Interviews from which the above estimates have been deduced.

3.4.3. Activity A2.3: Characterisation of safeguards

This activity usually occurs concurrently with activities A2.1 and A2.2, given that the persons to be interviewed are the same.

This activity consists of two tasks:

T2.3.1: Identification of existing safeguards.

T2.3.2: Valuation of existing safeguards.

P2: Risk analysis
A2.3: Characterisation of safeguards
T2.3.1: Identification of existing safeguards

Objectives

- To identify the safeguards of all types that have been planned and deployed by the date of the study.

Input products

- Inventory of operating procedures.
- Inventory of hardware and software products and/or developments that support the systems’ security.
- Training plan.
- Definition of the work posts.
- Agreements.
- Agreements for outsourcing services.

Output products

- List of safeguards deployed.

Techniques, practices and guidelines

- Catalogues of safeguards (see “Elements catalogue” chapter 6).
- Attack trees (see “Guide to techniques” 2.3).
- Interviews (see “Guide to techniques” 3.6.1).
- Meetings (see “Guide to techniques” 3.6.2).
- See also section 2.1.5.

Participants

- The project team.
- The delegates’ groups.

It is useful to record the following information for each safeguard:

- A description of the safeguard and its implementation status.
- A description of the threats it is to face.
- Interviews from which the above information has been deduced.

P2: Risk analysis *A2.3: Characterisation of safeguards* *T2.3.2: Valuation of existing safeguards*
Objectives • To determine the effectiveness of the safeguards deployed.
Input products • Inventory of safeguards (Elements catalogue).
Output products • **Safeguards evaluation**: Report on the safeguards deployed, according to their degree of effectiveness.
Techniques, practices and guidelines • Interviews (see "Guide to techniques" 3.6.1). • Meetings (see "Guide to techniques" 3.6.2). • Delphi evaluation (see "Guide to techniques" 3.7). • See also section 2.1.5.
Participants • The project team. • The delegates' groups. • Specialists in specific safeguards.

The effectiveness of the safeguards identified in the previous task is evaluated in this task, taking into consideration:

- The suitability of the safeguard for its purpose.
- The quality of the implementation.
- The training of those responsible for configuring and operating it.
- The training of the users, if they have an active role.
- The existence of controls for measuring its effectiveness.
- The existence of procedures for regular revisions.

It is useful to record the following information for each safeguard:

- An estimate of its effectiveness in dealing with those threats.
- An exploration of the effectiveness estimate.
- Interviews from which the above estimate has been deduced.

3.4.4. Activity A2.4: Estimate of the risk status

In this activity, information from the previous activities (A2.1, A2.2 and A2.3) is combined to provide estimates of the organisation's risk status.

This activity consists of three tasks:

T2.4.1: Estimate of the impact.

T2.4.2: Estimate of the risk.

T2.4.3: Interpreting the results.

P2: Risk analysis ***A2.4: Estimate of the risk status*** ***T2.4.1: Estimate of the impact***
Objectives • To determine the potential impact to which the system is subjected. • To determine the residual impact to which the system is subjected.
Input products • Results of activity A2.1, Characterisation of assets. • Results of activity A2.2, Characterisation of threats. • Results of activity A2.3, Characterisation of safeguards.
Output products • Report on the impact (potential) per asset. • Report on the residual impact per asset.
Techniques, practices and guidelines • Analysis using tables (see "Guide to techniques" 2.1). • Algorithmic analysis (see "Guide to techniques" 2.2). • See also section 2.1.3 and 2.1.6.
Participants • The project team.

In this task, the impact to which the system's assets are exposed is estimated:

- The potential impact to which the system is exposed, taking into account the value of the assets and the valuation of threats but not the safeguards currently deployed.
- The residual impact to which the system is exposed, taking into account the value of the assets and the valuation of threats and the effectiveness of the safeguards currently deployed.

P2: Risk analysis ***A2.4: Estimate of the risk status*** ***T2.4.2: Estimate of the risk***
Objectives • To determine the potential risk to which the system is subjected. • To determine the residual risk to which the system is subjected.
Input products • Results of activity A2.1, Characterisation of assets. • Results of activity A2.2, Characterisation of threats. • Results of activity A2.3, Characterisation of safeguards.
Output products • Report on the risk (potential) per asset. • Report on the residual risk per asset.
Techniques, practices and guidelines • Analysis using tables (see “Guide to techniques” 2.1). • Algorithmic analysis (see “Guide to techniques” 2.2). • See also section 2.1.4 and 2.1.7.
Participants • The project team.

In this task, the risk to which the system’s assets are exposed is estimated:

- The potential risk to which the system is subjected, taking into account the value of the assets and the valuation of threats but not the safeguards currently deployed.
- The residual risk to which the system is subjected, taking into account the value of the assets and the valuation of threats and the effectiveness of the safeguards currently deployed.

P2: Risk analysis

A2.4: Estimate of the risk status

T2.4.3: Interpreting the results:

Objectives

- To interpret the above results for impact and risk.
- To establish priorities regarding assets or groups of assets, either by order of impact or by order of risk.

Input products

- Results of activity A2.1, Characterisation of assets.
- Results of activity A2.2, Characterisation of threats.
- Results of activity A2.3, Characterisation of safeguards.
- Results of task T2.4.1, Estimate of the impact.
- Results of task T2.4.2, Estimate of the risk.

Output products

- Prioritised report on assets subjected to greatest impact.
- Prioritised report on assets subjected to greatest risk.
- **Risk status:** Report summarising the impact and potential and residual risks to which each asset in the domain is exposed.
- **Deficiencies report**: A report that describes the inconsistencies between the safeguards required and those that exist and the inconsistencies between the size of the risk and the current effectiveness of the safeguards.

Techniques, practices and guidelines

- Graphical techniques (see “Guide to techniques” 3.4).
- Meetings (see “Guide to techniques” 3.6.2).
- Presentations (see “Guide to techniques” 3.6.3).
- See also section 2.2.1.

Participants

- The project team.
- The Tracking Committee.

3.4.5. Synthesis of process P2

3.4.5.1. Control milestones

Control milestone H2.1

Acceptance of the “Value model” report.

Control milestone H2.2

Acceptance of the “Risk map” report.

Control milestone H2.3

Acceptance of the “Safeguards evaluation” report.

Control milestone H2.4

Acceptance of the “Risk status” report.

Control milestone H2.5

Acceptance of the “Deficiencies report” report.

3.4.5.2. Results

Intermediate documentation

- Results of the interviews.
- Documentation from other sources: statistics, comments from experts and comments from the analysts.
- Existing information that can be used by the project (for example, inventory of assets).
- Additional documentation: drawings, organisational charts, requirements, specifications, functional analysis, work books, user manuals, operating manuals, information and processes flowcharts, data models, etc.

Final documentation

- **Value model**

  A report that details the assets, their dependencies, the dimensions in which they are valuable and an estimate of their value in each dimension.
- **Risk map**

  A report that details the important threats to each asset, according to their frequency of occurrence and the degradation they could cause to the asset if they occur.
- **Safeguards evaluation**

  A report that details the existing safeguards, according to their effectiveness for reducing the risk they face.
- **Risk status**

  A report that details the impact and residual risks for each asset for each threat.
- **Deficiencies report**

  A report that details the safeguards needed that are absent or insufficiently effective.

This documentation is a faithful picture of the risk status and of the reasons why this risk is not to be disregarded. It is fundamental to understand the reasons that lead to a specific risk evaluation as a prior step to the following process, P3, designed to remove the risk or to reduce it to acceptable levels.

3.4.6. P2 process checklist

√ Identification of assets (T2.1.1).

√ Characterisation of assets (T2.1.1).

√ Dependencies between assets (T2.1.2).

√ Dimensions regarding security per asset (T2.1.3).

√ Valuation of assets (T2.1.3).

√ Value model (A2.1).

√ Identification of relevant threats (T2.2.1).

√ Estimate of the frequency of occurrence (T2.2.2).

√ Estimate of the damage (degradation) arising from the appearance of a threat (T2.2.2).

√ Risk map (A2.2).

√ Identification of existing safeguards (T2.3.1).

√ Estimate of the effectiveness of the existing safeguards (T2.3.2).

√ Safeguards evaluation (A2.3).

√ Estimate of the impact and residual impact (T2.4.1).

√ Estimate of the risk and residual risk (T2.4.2).

√ Risk status (P2).

√ Deficiencies report (P2).

3.5. Process P3: Risk Management

The impact and risks identified in the previous process are processed, either by assuming them or by facing them. To face those risks considered unacceptable, a security plan must be carried out to correct the current situation. A security plan consists of a collection of security programmes. Some programmes will be simple while others will reach a sufficient level of complexity and cost that their undertaking becomes a project in itself. The series of programmes (and, where appropriate, projects) is planned over time using the so-called security plan that describes and organises the actions to bring the risk status to an acceptable level that is accepted by management.

This process is carried out with the following activities and tasks:

Activity A3.1: Decision making

In this activity, the technical conclusions from process P2 are turned into action decisions.

Tasks:

Task T3.1.1: Classification of risks.

Activity A3.2: Security plan.

In this activity, action decisions are translated into specific actions: projects to improve security, planned over time.

Tasks:

Task T3.2.1: Security programmes.

Task T3.2.2: Undertaking plan.

Activity A3.3: Carrying out of plan

This activity takes the series of projects in the security plan and carries them out.

Tasks:

Task T3.3.*: Carrying out of each security programme

3.5.1. Activity A3.1: Decision making

This activity consists of a single task:

T3.1.1: Classification of risks.

P3: Risk management
A3.1: Decision making
T3.1.1: Classification of risks

Objectives

To classify the risks on a scale: critical, serious, appreciable or acceptable.

Input products

- Results of process P1, Risk analysis.
- Applicable legislation, laws and jurisprudence.
- Sector regulations.
- Agreements and contracts.
- Environmental reports.
- Market studies.

Output products

- A report classifying impacts and risks, including directives on the schedule for solving them.

Techniques, practices and guidelines

- Meetings (see “Guide to techniques” 3.6.2).
- Delphi evaluation (see “Guide to techniques” 3.7).
- See also section 2.2.1.

Participants

- The project team.
- The Tracking Committee.
- The Management Committee.

Given the impacts and the risks to which the system is exposed, a series of decisions - management, not technical - must be taken, conditioned by various factors:

- The seriousness of the impact and/or risk.
- The organisation’s legal obligations.
- The organisation’s obligations under sector regulations.
- The organisation’s contractual obligations.

Within the area of movement allowed by this framework, additional considerations may appear regarding the organisation’s capacity for accepting certain intangible impacts[35] such as:

- Public image within society.
- Internal policy: relationships with the employees themselves such as the capacity to hire suitable persons, the ability to keep the best ones, capacity to support personnel turnover, capability to offer an attractive professional career, etc.

[35] Because the risks analysis and management methodology is centred on damage evaluation, it does not fully capture the benefits of the absence of damage which generates an atmosphere of confidence and improves the undertaking of the organisation’s functions in its operating environment.

- Relationships with suppliers, such as the capability of reaching advantageous agreements over short, medium and long terms, capability to obtain priority treatment, etc.
- Relationships with clients or users such as the capability to win them over, capability to increase the offer, capability to stand out amongst the competition, etc.
- Relationships with other organisations, such as the capability to reach strategic agreements, alliances, etc.
- New business opportunities, such as ways to recover the investment in security.
- Access to recognised security certificates or qualifications.

All the above considerations result in the classification of each important security risk, determining whether:

1. It is **critical** in the sense that it requires urgent attention.
2. It is **serious** in the sense that it requires attention.
3. It is **appreciable** in the sense that it could be the subject of a study for handling it.
4. It is **acceptable** in the sense that action will not be taken against it.

Option four, accepting the risk, is always risky and must be taken with care and justification. The reasons that could lead to this acceptance are:

- When the residual impact is negligible.
- When the residual risk is negligible.
- When the cost of the suitable safeguards is out of proportion when compared to the residual impact and risks.

All the decisions are proposed by the Tracking Committee after hearing of the opinion of the project manager. All the decisions are adopted by the Management Committee.

This classification will have consequences in the following tasks and is a basic factor for establishing the relative priority of the actions.

3.5.2. Activity A3.2: Preparation of the information security plan

Action decisions are turned into specific actions.

This activity consists of two tasks:

T3.2.1: Security programmes.

T3.2.2: Undertaking plan.

P3: Risk management
A3.2: Preparation of the information security plan
T3.2.1: Security programmes

Objectives

- To prepare a set of security programmes.

Input products

- Results of task T3.1.1, Classification of risks.
- Knowledge of security techniques and products.
- Catalogues of security products and services.

Output products

- List of security programmes.

Techniques, practices and guidelines

- Risk analysis (see process P2).
- Cost/benefit analysis (see “Guide to techniques” 3.1).
- Project planning (see “Guide to techniques” 3.5).
- See also section 2.2.2 and 2.2.3.

Participants

- The project team.
- Security specialists.
- Specialists in specific areas of security.

Basically, two steps are involved:

1. All the impact and risk scenarios considered critical or serious as a result of the previous task are taken into consideration.
2. A set of security programmes is prepared that provide a response to all of the above scenarios, knowing that one programme may attack different scenarios and that one scenario may be handled by different programmes.

The final purpose is to implement or improve the implementation of a series of safeguards that reduce the impact and risk to residual levels accepted by the management. This handling of the safeguards becomes a series of tasks to be carried out.

A security programme is a group of tasks. The grouping is made for convenience, either because the tasks by themselves lack effectiveness or because they are tasks with a common objective, or because they are tasks that involve a single action unit.

Each security programme must detail:

- Its generic objective.
- The specific safeguards to be implemented or improved, detailing their objectives for quality, effectiveness and efficiency.
- The list of impact and/or risk scenarios to be faced: assets affected, types of asset, threats

faced, valuation of assets and threats and levels of impact and risk.

- The unit responsible for carrying them out.
- An estimate of costs, both financial and in terms of effort, for carrying them out, considering:
  - Cost of acquisition (of products) or of contracting (of services) or of development (of turn-key systems); it may be necessary to evaluate various alternatives.
  - Cost of initial implementation and maintenance over time.
  - Cost of training, both of operators and users, depending on the case.
  - Operating costs.
  - Impact on the organisation's productivity.
- A list of sub-tasks to be carried out, considering:
  - Changes in the regulations and development of procedures.
  - Technical solution: programs, equipment, communications and installations.
  - Deployment plan.
  - Training plan.
- An estimate of the undertaking time from start-up to putting into operation.
- An estimate of the risk status (impact and residual risk on completion).
- A system of effectiveness and efficiency indicators that continuously show the quality of the security function required and its evolution over time.

The above estimates may be very precise in simple programmes but may be just guidelines in complex programmes that involve carrying out a specific security project. In the latter case, each project will develop the latter details through a series of tasks for each project which, in general lines, will involve the following points:

- Study of the market offer: products and services.
- Cost of a specific development, either in-house or sub-contracted.
- If a specific development is considered suitable, it is necessary to determine:
  - The functional and non-functional specification of the development.
  - The development method that guarantees the security of the new component.
  - The mechanisms for measurement (controls) that must be built in.
  - The acceptance criteria.
  - The maintenance plan: incidents and evolution.

P3: Risk management

A3.2: Preparation of the information security plan

T3.2.2: Undertaking plan

Objectives

- To prepare a schedule of the security programmes.

Input products

- Results of task T3.1.1, Classification of risks.
- Results of task T3.2.1, Security programmes.

Output products

- Schedule for carrying out the plan.
- **Security plan.**

Techniques, practices and guidelines

- Risk analysis (see process P2).
- Project planning (see “Guide to techniques” 3.5).

Participants

- Development department.
- Purchasing department.

A schedule must be prepared for the security programmes, taking the following factors into account:

- The critical nature, seriousness or convenience of the impacts and/or risks being faced, giving maximum priority to those programmes that handle critical situations.
- The cost of the programme.
- The availability of in-house personnel to take responsibility for the management (and, where appropriate, the undertaking) of the scheduled tasks.
- Other factors such as the preparation of the organisation’s annual budget, relationships with other organisations, development of the legal, regulatory or contractual framework, etc.

Typically, a security plan it is prepared at three levels:

Master plan (one)

Often called the “action plan”, this covers a long period (typically three to five years) and sets the directives for action.

Annual plan (a series of annual plans)

Covers a short period (typically, between one and two years) and sets the planning of the security programmes.

Project plan (a group of projects with their planning)

Covers a short period (typically, less than one year) and sets the detailed plan for carrying out each security programme.

One single, master plan must be prepared which gives perspective and unity of objectives to the individual actions. This master plan allows annual plans to be developed which structure the assignation of resources for carrying out the tasks within the strategic framework, especially budgetary items. And, finally, there will be a series of projects that provide the security programmes.

3.5.3. Activity A3.3: Carrying out of plan

This activity consists of a number of tasks that depend on the security plan determined in activity A3.2, since it involves carrying out the programmes planned in it.

This activity consists of N tasks - as many as a have been set in the security plan.

T3.3.*: Carrying out of each security programme[36].

P3: Risk management
A3.3: Carrying out of plan
T3.3.*: Carrying out of each security programme

Objectives

- To attain the objectives described in the security plan for each programme.

Input products

- Results of activity A3.2, Security plan.
- Current security programme.
- Risk analysis before carrying out the plan.

Output products

- The implemented safeguard.
- Standards for use and operation.
- A system of indicators for effectiveness and efficiency in attaining the required security objectives.
- Updated value model.
- Updated Risk map.
- Updated risk status (impact and residual risks).

Techniques, practices and guidelines

- Risk analysis (see process P2).
- Project planning (see “Guide to techniques” 3.5).

Participants

- The project team: development of the risk analysis.
- Personnel specialising in the relevant safeguard.

[36] This activity consists of an unknown number of tasks, to be determined in each project; thus the reference use of the symbol *.

3.5.4. Synthesis of process P3

3.5.4.1. Control milestones

Control milestone H3.1

Management will approve or not the security plan including a list of security programmes and the proposed schedule for carrying them out.

Control milestone H3.*

Completion of each security programme, meeting the acceptance criteria described in the security plan.

3.5.4.2. Results

Intermediate documentation

- Decisions for classifying the impact and risk scenarios.

Final documentation

- Security plan.

3.5.5. Checklist for process P3

- √ Classification of risks (T3.1.1).
- √ Identification of the required security programmes (T3.2.1).
- √ Security programmes:
  - √ Objectives.
  - √ Estimate of effort.
  - √ Estimate of cost.
  - √ Acceptance plan.
  - √ Operation plan.
  - √ Maintenance plan.
  - √ Training plan.
  - √ System for checking effectiveness.
  - √ System for checking efficiency.
  - √ Estimate of impact and residual risks.
- √ Undertaking schedule (T3.2.2).
- √ Strategic security plan: long term (A3.2).
- √ Tactical security plan: medium term (A3.2).
- √ Operational plans: individual projects (A3.2).

4. Development of information systems

Applications *(*software*)* are a frequent and core type of asset for treating information in general and for providing the services based on that information. The presence of applications in an information system is always a source of risk in the sense that it is a point at which threats may appear. On the other hand, sometimes, the applications appear as part of the answer in the sense that they safeguard the system against potential risks. In any case, the risk arising from the presence of applications must be under control.

The analysis of the risks is a fundamental part of the design and development of secure information systems. It is possible -and imperative- to incorporate functions and mechanisms that strengthen security in a new system and in the development process, ensuring its consistency and security, following the organisation's security plan. It is a recognised fact that considering the security of a system before and during its development is more effective and economic than considering it afterwards. Security must be embedded in the system from its initial conception.

There are two types of activities:

- **SSI**: Activities related to the very security of the information system.
- **SPD**: Activities related to security during the process of developing the information system.

4.1. Start of the processes

There are various reasons that can lead to the development of a new application or the modification of an existing one:

New services and/or data

- Requires the development of new applications or the modification of operational applications. May involve the disappearance of operational applications.
- The initiative may be taken by the development manager, with the security manager acting as a subsidiary.

Technological development. Information technologies are continually developing, with changes appearing in techniques for developing systems, in languages, in development platforms, operating platforms, operating services, communications services, etc.

- It requires the development of new applications or the modification of operational applications. Might involve the disappearance of operational applications.
- The initiative may be taken by the development manager, with the security manager acting as a subsidiary.

Modification of the security classification of services or data

- Typically requires the modification of operational applications. Rarely implies the development of new applications or the disappearance of operational applications.
- The initiative may be taken by the security manager, with the systems manager acting as a subsidiary.

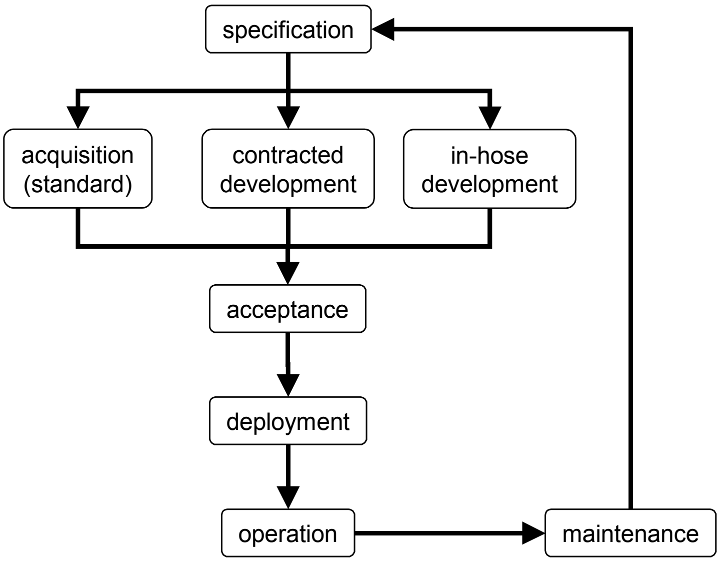
Consideration of new threats. The development of communications technologies and services may enable new threats or convert formerly unimportant threats into important ones in the future.

- It typically requires the modification of operational applications, either to their coding or, more frequently, in their operating conditions. Rarely implies the development of new applications or the disappearance of operational applications.
- The initiative may be taken by the security manager, with the systems manager acting as a subsidiary.

Modification of the risk classification criteria. May be caused by operational quality criteria, by changes to applicable legislation, in sector regulations or by agreements or contracts with third parties.

- Typically requires the modification of operational applications. Rarely implies the development of new applications or the disappearance of operational applications.
- The initiative may be taken by the security manager, with the systems manager acting as a subsidiary.

4.2. Life cycle of applications



Typically, the life cycle of an application involves several phases or stages:

Specification. In this phase, the requirements to be met by the application are determined and a plan is prepared for the following phases.

Acquisition or development. To turn a specification into a reality, a product may be acquired or developed, either in-house or through outsourcing.

Acceptance. Neither a new application nor a modification of an existing one must be allowed to enter into operation without being formally accepted.

Deployment. This consists of installing the code in the system and configuring it so that it enters into operation.

Operation. The users use the application, and users and/or operators attend to incidents.

Maintenance. Either because new requirements appear or because a failure has been discovered, the application may require maintenance that requires returning to any of the previous stages - in the final resort, to the basic specification.

4.2.1. Systems plan

Computer applications are one component of information systems. The applications are embedded in the information system to take care of part of the services required. A systems plan determines the framework for the development and operation of the computer applications, specifically:

The services required, both for the internal users and to support the internal users or internal applications.

The functional data used.

The applications that handle these data.

The equipment: computers and communications services.

From the security point of view, a systems plan allows:

- The essential services to be identified and valued.

- The essential data to be identified, classified and valued.
- The organisation's security policy to be determined, that is:
  - The legal context within which the organisation operates.
  - The criteria for excellence in service provision.
  - The roles of the personnel related with the information systems.

The systems plan allows the value model to be established, that is, the large sections (assets) and the first valuations of what will become a detailed risk analysis.

4.3. Risk analysis

Being part of an information system, the risks associated with an application must be known and managed, whether they are supported by the application or are risks that affect higher assets or risks to lower assets accumulated.

Magerit allows the application to be modelled directly with an asset, establishing its dependencies, whether of higher assets that depend on it or of lower ones that support it. The method allows threats and safeguards to be identified and valued, providing information on the impact and risk to the application itself and to the assets related with it.

Self-contained AGR. If the organisation has not carried out an AGR project, it will be necessary to do so, incorporating at least the assets that are directly or indirectly related with the application.

Marginal AGR. If the organisation has already carried out an AGR project, it is sufficient to revise the results of the project, incorporating the new assets. The appearance of a new application may imply new services, new data, new equipment, new premises and new personnel. It may also imply the disappearance of old assets that have been replaced by the new application and its possibilities. For each specific case, it is necessary to determine what must be added and what must be removed, following activities A2.1, A2.2 and A2.3 of process P2, Risk analysis.

Regardless of the approach used, the result will be a list of impacts and risks to both the application and to its environment. These data are obtained by following the steps in activity A2.4 of process P2. The results are interpreted using task A2.4.3 of process P2, Interpreting the results.

4.4. Risk management

The P3 Risk management process recommends safeguards and evaluates the effect of the safeguards deployed against the impact and risk. The decisions made will depend on the criteria set in the organisation's security policy and other considerations specific to each case. Although the security policy sets a reference framework that cannot be broken, usually not all the technical and operation details of the service to make precise decisions are covered.

Due to the relationship between the elements in a system, it is not sufficient to protect a certain type of asset in order to protect the whole. However, this chapter concentrates on the measures that must be applied to applications so that they do not compromise the system's security.

Always following the initiative and corroboration of the risk management process, the following aspects must be considered:

During the specification:

- Dimensioning.
- User profiles.
- Requirements for user identification and authentication.
- Encryption requirements.
- Monitoring and logging requirements:
  - Of input data.

  - Of output data.
  - Of intermediate data.
  - Of access to the application.
  - Of activity (use).

If standard software is acquired:

- Acquisition and maintenance contracts.

If software development is sub-contracted:

- Acquisition and maintenance contracts.
- Development environment: space, persons, platforms and tools.
- Secure programming techniques.
- Source code management:
  - Access control.
  - Version control.

If software is developed in-house:

- Maintenance conditions:
- Development environment: space, persons, platforms and tools.
- Secure programming techniques.
- Source code management:
  - Access control.
  - Version control.

For acceptance:

- Acceptance tests:
  - Test data.
  - If they are not real, they must be realistic.
  - If the use of real data is unavoidable, copies and access to them must be controlled.
  - Functional tests (of the security services).
  - Simulation of attacks.
  - Test under load.
  - Controlled intrusion (ethical hacking).
  - Inspection of services/code.
  - Information leaks: covert channels, through the records, etc.
  - Access via back doors.
  - Privilege escalation.
  - Buffer overflow problems.
  - Accrediting.

For the deployment:

- Inventory of applications in operation.
- Change management: standards and procedures.
- Setting of passwords.

During operation:

- Standards and procedures for:
  - User management.
  - Password management.
  - Log management.
  - Incident management: recording evidence, escalation, emergency and recovery plans.
- Log analysis: tools, criteria, procedures, etc.
- User manuals: administrators, operators and users.
- Training: Initial and continuous: administrators, operators and users.

In the maintenance cycles:

- Standards and procedures for:
  - Requests.
  - Approval, including the differential analysis of risks and the approval of new measures, where relevant.

End

- Destruction of operational data.
- Copying and safekeeping of data when required by law or internal policy.
- Elimination of operating code: executable, configuration data and user accounts.
- Revision of back-up copies.

4.5. Development security

As described above, a distinction can be made between the security of the development process (SPD tasks) and the security of the information system (SSI). The tasks in the interface are arranged according to whether they belong to one security objective or the other.

4.5.1. SPD – Development process security

Assets to be considered

Each development stage requires an analysis of the specific risk involved:

- The data being handled:
  - Systems specifications and documentation.
  - Source code.
  - Operator and user manuals.
  - Test data.
- The software development environment:
  - Tools for handling the documentation: generation, publication, documentation control, etc.
  - Tools for handling the code: generation, compiling, version control, etc.
- The hardware development environment: central equipment, work posts, filing equipment, etc.
- The communications development environment.
- The installations.
- The personnel involved: developers, maintenance personnel and users (for tests).

Activities

Involves the following steps:

1. The development team describes the elements involved via the project manager.
2. The analysis team receives the information on the assets involved via the security manager.
3. The risk analysis team analyses the risks.
4. The risk analysis team describes the risk status via its manager, proposing a series of measures to be taken.
5. The development team prepares a report on the cost of the recommended measures, including development costs and the costs of deviations in the delivery schedule.
6. Management classifies the risk and decides the safeguards to be implemented on the basis of the joint reports of the risk and cost analysis for the proposed solutions.
7. The risk analysis team prepares the report for the solutions adopted.
8. The security team prepares the relevant security standard.
9. Management approves the plan for carrying out the process with the required security.

Results of the risk analysis and management

In all cases:

- Recommended safeguards.
- Information handling standards and procedures.

Other considerations

Although each stage requires its specific risk analysis, it is true that the models are very similar so that the greatest efforts are made in the first one and the others are adaptations of it.

During system planning, high-level contributions may appear that affect the organisation's security standards and even the corporate security policy itself.

Notable among the standards and procedures generated is the need for a standard for classifying documentation and procedures for its handling.

Special attention must be paid in all processes to the personnel involved; as basic rules, it is useful to:

- Identify the roles and the persons.
- Determine the security requirements for each post and incorporate them into the selection criteria and hiring conditions.
- Limit access to the information: by necessity only.
- Segregate tasks, especially preventing the concentration of those applications or parts of application that involve a high risk in one person.

4.5.2. SSI – Information system security

The entire existence of an information system can be seen as stages of growing concretion from a very overall perspective during the planning processes to a detailed vision during development and operation. However, this life cycle is not linear: it is frequently necessary to examine other options and review the decisions made.

The impact and risk estimates in the risk analysis must be based on the actual systems, concentrating on their assets. Thus, the value model can be understood as an evolution, constantly collecting the level of detail available. As a methodology, Magerit allows the systematic and uniform treatment of what is essential to be able to compare options and to manage the systems' development.

The use of support tools must allow:

1. An initial model to be captured (during system specification).
2. Variations to be studied (during system feasibility and architectural analysis).
3. A movement from generalisations to specifics, forecasting potential threats and the preparation of detection and reaction mechanisms (during system detailed design and development).
4. Their acceptance and use to be managed (during system deployment and acceptance).
5. The proposed changes to be periodically checked (during system maintenance).

Use of Magerit methodology tasks

Process P1: Planning

Activity A1.1: Opportunity study

Task T1.1.1: Determine the opportunity

This task involves the internal decision to develop the information system, taking security into account.

Activity A1.2: Determine the scope of the project

Task T1.2.1: General objectives and restrictions

Those of the information system under development.

Task T1.2.2: Determination of the domain and limits

Those of the information system under development.

Task T1.2.3: Identification of the environment

Those of the information system under development.

Task T1.2.4: Estimate of dimensions and costs

Part of the project (or projects) for developing the information system.

Activity A1.3: Project planning

Task T1.3.1: Evaluate loads and plan interviews

This task is carried out as in any AGR project. The task must be carried out along with the very early system planning, preparing a list of interviews for the rest of the processes, except for occasional adjustments as deemed necessary.

Task T1.3.2: Organise the participants

This task is carried out as in any AGR project. Along with system planning, a list of participants to be interviewed must be prepared, without going into greater detail than their roles. As the system is developed, the persons that meet the planned roles are identified.

Task T1.3.3: Plan the work

Part of the project (or projects) for developing the information system.

Activity A1.4: Launch the project

Task T1.4.1: Adapt the questionnaires

This task is carried out as in any AGR project. This task must be carried out along with the very early system planning, being established for the rest of the processes, except for occasional adjustments.

Task T1.4.2: Evaluation criteria

This task is carried out as in any AGR project. This task must be carried out along with the very early system planning, being established for the rest of the processes.

Task T1.4.3: Resources needed

Part of the project (or projects) for developing the information system.

Task T1.4.4: Awareness

Part of the project (or projects) for developing the information system.

Process P2: Risk analysis

Activity A2.1: Characterisation of assets

Task T2.1.1: Identification of assets

During system planning, the generic assets are identified. As the development progresses, identification is tightened so that the generic assets become specific assets. Concretion must be at its maximum on reaching the development stage.

Task T2.1.2: Dependencies between assets

During system planning, general relationships appear. As the development progresses, dependencies are tightened as the generic assets become specific assets. Concretion must be at its maximum on reaching the development stage.

Task T2.1.3: Valuation of assets

The evaluation of the end services and the essential data can be made along with the very early system planning, although as the development progresses, the services and/or data can be segmented, requiring individual valuation which must never exceed the valuation of the aggregated services or data. In other words, the services and/or data can be separated in fractions of lower value.

Typically, the evaluation of the rest of the assets can be analysed as a simple accumulated value from the higher assets, using the dependency relationships.

Activity A2.2: Characterisation of threats

Task T2.2.1: Identification of threats

Threats to generic assets can be incorporated from the very early system planning, but as the detailed group of components is concreted, specific threats to the technology used must be incorporated.

Task T2.2.2: Valuation of threats

This task is carried out as in any AGR project.

Activity A2.3: Characterisation of safeguards

Task T2.3.1: Identification of existing safeguards

Many safeguards may be identified from the very early system planning.

However, the technical safeguards must be specified as the detailed group of components and the technology used is specified.

Task T2.3.2: Valuation of existing safeguards

This task is carried out as in any AGR project.

Activity A2.4: Estimate of the risk status

Task T2.4.1: Estimate of the impact

This task is carried out as in any AGR project.

Task T2.4.2: Estimate of the risk

This task is carried out as in any AGR project.

Task T2.4.3: Interpreting the results:

This task is carried out as in any AGR project.

Process P3: Risk Management

Activity A3.1: Decision making

Task T3.1.1: Classification of risks

This task is carried out as in any AGR project.

Both the development team and the risk analysis team must take part in the decision-making.

Activity A3.2: Preparation of the overall information security plan

Task T3.2.1: Security programmes

This task is included in the development tasks.

Task T3.2.2: Undertaking plan

This task is included in the development tasks.

Activity A3.3: Carrying out of plan

Task T3.3.*: Carrying out of each security programme

These tasks are included in the development tasks.

Other considerations

It is important to carry out the risk analysis progressively, incorporating greater detail as the development progresses but never starting again from zero.

During system planning, high-level contributions may appear that affect the organisation's security standards and even the corporate security policy itself.

The standards and procedures derived from each development stage form a group of standards and procedures that will be used during the operation of the system.

- Typically, the standards must be completed in the early stages: system planning, feasibility study, and architectural design; they are rarely changed in the following stages.
- On the other hand, the procedures cannot be obtained until the details are specified in the detailed design, development, and deployment stages; they must not be changed, except for adjustments and corrections, in the following stages.
- During deployment and acceptance stages, standards and procedures are moved into operation.
- The maintenance stage may involve the correction of erroneous standards and procedures or the extension of incomplete standards and procedures that have not included all the practical circumstances.

The specification of safeguards must include both the mechanisms for action and for the configuration, monitoring and control of their effectiveness and efficiency. Frequently, some developments appear that are specifically designed to configure the group of safeguards and to monitor their operation.

4.6. References

- NIST Special Publication 800-64, "Security Considerations in the Information System Development Life Cycle", Rev.1. June 2004.
- NIST Special Publication 800-27 Rev. A, "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)", Rev. A, June 2004.
- "Seguridad de las Tecnologías de la Información. La construcción de la confianza para una sociedad conectada", E. Fernández-Medina y R. Moya (editors). AENOR, 2003.

5. Practical advice

All of the above is somewhat abstract and may not allow the analyst to progress easily through the steps described. Therefore, it has been considered appropriate to include some comments that may serve as a guide for progress.

It is also recommended that the user consults the “Elements catalogue” containing types of assets, valuation dimensions, valuation guides and catalogues of threats and safeguards.

5.1. Identifying assets

It is useful to repeat that only those information systems resources that have value to the organisation, either in themselves or because they support valuable assets, are of interest.

As an example, a Web server is an asset with little value in itself. This can be assured because it is not normal for an organisation to deploy a Web server except when it needs to provide a service. All of its value is imputed:

- The non-availability of the server implies the interruption of the service. The cost involved in the interruption of the service is the availability value to be imputed to the server.
- Uncontrolled access to the server puts at risk the secrecy of its data. The cost involved in the loss of confidentiality of the data is the confidentiality value to be imputed to the server.
- And so on with the dimensions under consideration.

The intangibles

Certain elements of value in organisations are intangible:

- Credibility or good image.
- Accumulated knowledge.
- Independence of criterion or action.
- Personal privacy.
- Physical well-being of persons.

These elements can be included in the risk analysis as assets[37] or as evaluation elements[38]. The quantification of these items is often difficult but somehow it must never be forgotten that what is to be protected finally is the organisation’s mission and the value of this lies in these intangibles, as recognised in Magerit version 1.0[39].

Identification of assets

Perhaps the best approach to identify the assets is to ask directly:

- Which assets are fundamental to your achieving your objectives?
- Are there more assets that must be protected due to legal obligations?
- Are there assets that are related to the above?

It is not always clear what an asset is individually. If, for example, your unit has 300 PC work posts, all with identical configurations and handling identical data, it is not useful to analyse 300 identical

[37] Not all authors agree that it is a good idea to identify intangible assets. It is true that they are assets in the financial sense but it is questionable that they are actual resources of the information system. What happens is that if delegates are asked during the interviews in terms of the organisation’s intangible values, the daily perspective is lost since most of the members of the organisation have more specific and closer objectives on which a considered opinion can be given.

[38] See “Catalogue of Elements”, chapter 4. Valuation criteria”.

[39] See Magerit version 1.0, “Procedures guide” / “3. Elements sub-module” / “3.4. Impacts” / ”3.4.3. Types”.

assets. It is sufficient to analyse a generic PC that represents them all; grouping simplifies the model.

On other occasions, the opposite occurs: a central server with a thousand functions - file server, mail server, intranet server, document management system server, etc. In these cases it is useful to segregate the services provided as independent (internal) services. Only on reaching the level of the physical equipment need all the services be converged in a single piece of equipment. If services are shared out among various servers in the future, it is then easy to revise the value model and dependencies.

5.2. Discovering and modelling the dependencies between assets

Sometimes this is more difficult than expected because those responsible for the assets are usually more concerned about the functional chaining between the assets than about the dependence in the value propagation sense.

It is necessary to tell the delegate that, instead of searching for what is necessary for the system to function, he should do the reverse: look for where the system may fail or, more precisely, where the assets' security could be compromised.

- If there are data that are important because of their confidentiality, it is necessary to know in which places they will be stored and through which places they will travel; they could be revealed in these points.
- If there are data that are important because of their integrity, it is necessary to know in which places they will be stored and through which places they will travel; they could be altered in these points.
- If a service is important because of its availability, it is necessary to know which elements are used to provide it: the failure of these elements would stop the service.

These considerations could be made as questions of the type:

- If you wanted to access these data, where would you attack?
- If you wanted to stop this service, where would you attack?

This approach of "putting yourself in the attacker's place" gives rise to the techniques known as "attack trees" [40] which in this methodology are associated with what are called dependencies. An asset may be attacked directly or indirectly through another asset on which it depends.

The above considerations can be shown in a "flat" dependencies diagram which can (and should, for practical purposes) be converted into a more compact tree. As a result, it is normal to say that the services depend on the equipment which in turn depends on the premises in which the equipment is located, without the need to state that the services depend on the premises[41]. It is normal to identify "internal services" or "horizontal services" which are groups of assets for a specific function. These intermediate services are effective for compacting the dependencies graph because the dependencies of these services are interpreted unambiguously as dependencies of all the elements that provide the service.

When data flow charts or process charts are used, the route followed by the data is not as important as the (unorganised) whole of the elements involved. The process depends on all the assets that appear in its diagram. Some data depend on all the sites through which they pass. In both diagrams, it is usual to find hierarchical descriptions where a process is subdivided into levels of greater detail. These hierarchical diagrams may help to prepare the dependencies graph.

Typical mistakes

It is not true to state that an application depends on the data it handles. The reasoning of those who say so is that "the application does not function without data", which is correct, but it is not the

[40] See "Guide to techniques", section 2.3.

[41] The "Guide to techniques" contains the algorithmic model for calculating the total dependencies between assets on the basis of the direct dependencies.

interesting point. It is the opposite: the data depend on the application. In value terms, it could be said that the application has no value without data. Because the value is a property of the data, it is this value that is inherited by the application. Thus, the data depend on the application. From the other point of view, the data can be accessed through the application, making the application the means to attack the data.

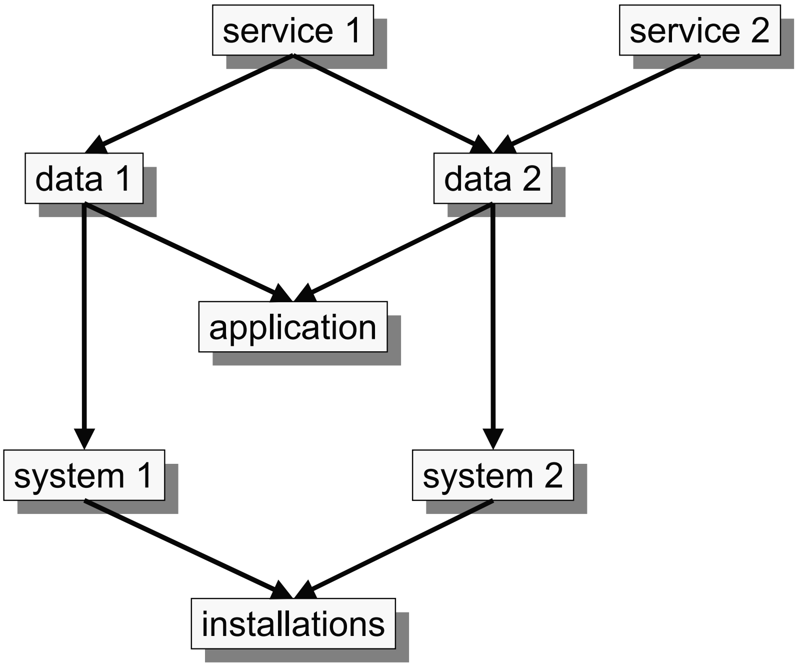
Given that data and applications usually join forces to provide a service, the value of the service is transmitted to both the data and to the applications involved.

Bad	***Good***
• service → application • application → data	• service → data • data → application • service → application

It is not true to say that an application depends on the equipment in which it runs. The reasoning of those who state this is that “the application does not function without equipment”, which is correct but is not the interesting point. If both the application and the equipment are necessary to provide a service, this must be stated explicitly, without searching for more complex paths.

Bad	***Good***
• service → application • application → equipment	• service → application • service → equipment

These mistakes sometimes pass unnoticed while the system is very small (only one service, one application and one piece of equipment) but they appear when the system grows. For example, application X may run on different equipment with different data to provide different services. It is then impossible to relate the application with one or more pieces of equipment, other than by considering each case.



Are the dependencies well modelled?

Establishing dependencies is a delicate task that can have a bad ending. Before a dependencies model can be considered good, it is necessary to trace for each asset all the assets that it depends on directly or indirectly and the following questions must be answered positively:

- Have all the assets through which the asset being valued may be attacked been identified?
- Can the asset being valued really be attacked in all the assets on which it depends?

The dependency list propagates the accumulated value so that if an asset without accumulated value is found, this means that the dependencies are badly modelled or, simply, that the asset is irrelevant.

5.3. Valuing assets

It is always useful to value the information or data that forms the reason for the information system's existence.

If end services (provided to users beyond the analysis domain) have been modelled, they should also be valued.

It is easy to identify data or information type assets and value them according to guideline classifications such as their personal nature or their security classification but it is much more delicate to value commercial or operational type data because it is necessary to look at the consequences of the damage suffered.

The rest of the assets can often be left unvalued because their most important value is to support the data and/or services and the dependencies relationships take care of this calculation.

However, it may be useful to value other types of assets.

The simplest assets to value are those acquired in a shop. If one is faulty, another one must be installed. This costs money and time (that is, more money). This is known as a replacement cost. Apart from some notable exceptions, the cost of the physical assets is often minimal compared to other costs and can be overlooked.

It is generally difficult to value persons but if a post involves a slow and laborious period of training, it must be remembered that the person filling this post becomes very valuable because his “replacement cost” is high.

In any case, to value an asset, the person responsible must be identified - the suitable person to value the asset. This person must be helped with valuation tables such as those in chapter 4 of the “Elements catalogue” which, when adapted to the specific case, allow the perception of the value to be converted into a qualitative or quantitative measurement.

Often, there is no single person responsible for an asset and/or service; instead, several persons within the organisation have qualified opinions on the matter. It is necessary to listen to them all and to reach a consensus. If there is no obvious consensus, the following may be required:

A meeting: Bring the opinion holders together and try to reach a common opinion.

A Delphi[42]**:** Send questionnaires to the opinion holders and try to converge on a common opinion.

The assets evaluation processes frequently require the help of different persons to value different assets and often all those interviewed consider their assets as having the greatest importance, this being more frequent the more specialised the person interviewed. Since many evaluations are estimates of value, care must be taken that everyone uses the same estimating scale. It is therefore important to use a table such as that in chapter 4 of the “Elements catalogue”, directly or adapted to the specific case, and it is important that after asking those who are familiar with each asset, they all receive a copy of the overall valuation of the system so that they can appreciate the relevant relative value of “their” assets and provide an opinion in context.

Personal data

Personal data are controlled by laws and regulations and require the organisation to adopt a series of protection measures that are independent of the assets' value[43].

[42] See "Guide to techniques”, chapter 3.7.

[43] The evaluation of personal assets can be approached by quantifying the fine that would be imposed by the Data Protection Agency. This approach is not valid in a qualitative analysis. In a quantitative analysis, the approach starts from the hypothesis that the worst that could happen with this data is for it to be the

The most realistic form of handling personal data is to classify them as such in the appropriate level and to determine their value: the damage that would be caused if they were wrongfully revealed or altered. With this approach, the analysis of impact and risks allows the data to be protected both by legal obligation and because of their own value.

5.4. Identifying threats

The task seems impossible: identify the threats to each asset, in each dimension.

One starting point is past experience, either in-house or that of similar organisations. What has happened may repeat itself and in any case it would be unthinkable not to take it into account.

As a complement, a catalogue of threats such as that in the “Elements catalogue” helps to locate what should be considered, depending on the type of assets and on the dimensions in which it has its own or an accumulated value.

Often, attack scenarios are invented that are dramatisations of how an attacker would attack our systems. This technique is sometimes known as “attack trees”. Put yourself in the place of the attackers and imagine what they would do with their knowledge and financial capability. Different situations may have to be considered, depending on the technical profile of the attacker or on his technical and human resources. The dramatisations are interesting for being able to calculate impacts and risks but are also very useful when convincing senior management and users that a threat is not theoretical but very real. When the safeguards are evaluated, it may be useful to revise these attack scenarios.

5.5. Valuing threats

The task is demoralising: determine the degree of degradation that would be caused and the probable frequency of occurrence for each asset in each dimension.

Whenever possible, it is useful to start with standard data. In the case of natural disasters or industrial accidents, an historical or generic series may be available or one from the place in which the equipment for the information system being studied is located. A log that shows which events are frequent and which “never happen” may also be available.

Classifying human errors is more complicated but experience allows realistic values to be obtained.

The most complex is classifying deliberate attacks because these depend on good or bad luck. There are many reasons that increase the danger of a threat:

- The attacker does not need great technical knowledge.[44]
- The attacker does not need a great investment in equipment.[45]
- There is a very large financial benefit in play (the attacker may get rich).
- There is an enormous benefit in play (the attacker may be strongly benefited, in terms of esteem, popularity, etc) so that challenges must be avoided and it is important never to boast about how invulnerable your information system is - it isn’t and having this demonstrated is not amusing.
- There is a bad atmosphere at work, giving rise to discontented employees who take their revenge via the systems, simply to cause damage.
- There is a bad relationship with the external users, who take their revenge via our systems.

cause of a fine.

[44] Attention should be paid to the “sale” of attack tools. An attack may require a real expert to carry it out manually (that is, it is infrequent) but if the expert packages his attack in a tool with a simple graphical interface, using that tool becomes a game that requires nothing more from the attacker than an absence of scruples (that is, the threat becomes very frequent).

[45] It must be remembered that the Internet is an immense network of computing power. If someone knows how to get organised, it is not difficult to put the Net to “work for me” which means that the attacker has vastly more effective means than the system being attacked.

Starting from a standard value, it is necessary to increase or reduce the classifications for frequency and degradation until they describe the specific case as closely as possible. Often, the correct value cannot be determined and it is necessary to use simulations as guidelines. The use of some type of tool is very useful for studying the consequences of a certain value, which some authors call the sensitivity of the model to certain data. If it appears that the results change drastically due to small alterations in an estimate of frequency or degradation, it is necessary to: (1) Be realistic; and (2) Pay great attention to why the system is so sensitive to something so specific and to take measures designed to make the system independent, that is, to stop a certain threat from being critical.

Remember that the frequency does not affect the impact so that studying the impact allows the degradation to be adjusted and then studying the risk allows the frequency to be adjusted. An unjustified degradation value must never be accepted in the hope of its being compensated with the frequency since the estimate of the impact is important in itself as well as that of the risk.

Whatever the final decision made for estimating a value, it must be documented because explanations will be required sooner or later, above all if costly safeguards are to be recommended as a consequence.

5.6. Choosing safeguards

Probably the only way is with a catalogue. Use an expert (system) to help see which solution is suitable for each combination of:

- Type of asset.
- Threat to which it is exposed.
- Dimension of value that is the cause of the concern.
- Risk level.

Often, many solutions with different qualities are found for a problem. In these cases, a solution must be chosen that corresponds with the calculated impact and risk levels.

Many safeguards are of low cost: it is sufficient to configure the systems suitably or organise standards so that people carry out tasks suitably. But some counter-measures are very expensive (to acquire, to deploy, to maintain periodically, to train the personnel in charge of them, etc). In these cases, it is useful to decide whether the cost of the safeguard does not exceed that of the potential risk, that is, always make spending decisions that involve a net saving.

Last and by no means least, when safeguards are deployed it is necessary to consider their ease of use. Ideally, the safeguard should be transparent so that the user needs to do nothing or as little as possible. A safeguard that is complex to use and requires specialised personnel adds the threat implied by its erroneous use to the threats already in the system.

5.7. Successive approximations

The reader will already have realised that risk analysis may be very laborious, requiring time and effort. It is also necessary to introduce many elements that are not objective but that are analysts' estimates, which implies the need to explain and agree what each thing means to avoid being exposed to unknown or undervalued impacts or risks and to avoid turning paranoia into a waste of unjustified resources.

In order to be practical and effective, it is useful to make successive approximations. Start with a high level superficial analysis, quickly identifying the most critical parts: assets of great value, clear vulnerabilities or, simply, textbook recommendations because there is nothing more prudent than learning from the experience of others. This risk analysis is evidently imperfect but it is enough to be confident in its correct handling. The following paragraphs describe how to quickly move towards the final objective: having impacts and risks under control.

Note that these imperfect approximations allow the quick deployment of systems that are reasonably protected when there is no time for a full-scale risk analysis. When, after time, the risk management phase is reached after an exhaustive analysis, very probably many safeguards will be found to be already available, requiring only the introduction of some new ones and/or the improvement to the effectiveness of those that already exist. Following these informal approximations is therefore not a waste of work.

5.7.1. Baseline protection

Basic (baseline) protection measures are frequently heard of that must be implemented in all systems unless it is shown that they are not relevant in a specific case.

Don’t argue or hesitate. Your information systems must not be accessible to just anyone at any moment. They can be protected physically or logically, placing them in a room to which not just anyone has access or using logical access identification. But protect them!

This type of reasoning can be applied frequently and leads to the deployment of a minimum of “purely common sense” safeguards. Once the obvious has been carried out and must never be argued over, more elaborate levels can be reached, that are specific to each system.

A catalogue of safeguards is required to apply a baseline treatment. There are numerous sources, including:

- International standards, for example ISO/IEC 17799:2005.
- National standards, for example the “Security criteria”.
- Sector standards.
- Corporate standards, especially frequent in small branches of large organisations.

The advantages of protection by catalogue are:

- It is very quick.
- It requires almost no effort.
- It provides a uniform level with other, similar organisations.

The disadvantages of protection by catalogue are:

- The system may be protected against threats from which it does not suffer, implying an unjustified cost.
- The system may be unsuitably protected against real threats.

In general terms, one does not know what is being done with baseline protection and although on the right track, there is no measurement of lacks or excesses. However, it can be a useful starting point for later refinement.

Protection by catalogue can be refined somewhat by considering the value of the assets or quantifying the threats.

Based on the classification of the assets

If you have personal data classified as high level, they must be encrypted.

If you have data classified as confidential, they must be labelled and encrypted.

Apart from complying with specific laws and standards, a type of “preventive vaccination” of important assets must be carried out.

If you have a local area network connected to the outside world you must put a firewall at the connection point.

Based on the value of the assets

If you have all the operational data on computer media, you must make back-up copies.

If you have computer equipment, keep it up-to-date with the manufacturer’s updates.

Anything valuable must be taken care of in case something happens, without going into details of what exactly may happen.

Based on threats

When dealing with a so-called electronic government system (remote bureaucratic procedures) or if the systems are used for electronic trading (remote purchasing and sales), record who does what at all times in case of incidents with users, in which it is necessary to determine who is right and who pays for the damage. This will also show who is using the services without authorisation (fraud).

What may be necessary is necessary and part of the responsibilities of the security manager is to have available the correct information when it is needed.

Based on vulnerabilities

If you have a network of old equipment and it is connected to the Internet, you must install a firewall.

If you have a production application, it must keep it up to date by applying the improvements and correcting the defects announced by the manufacturer.

When it is known that computer systems are vulnerable, they must be protected.

5.8. References

- ISO/IEC 17799:2005, “Information technology – Security techniques – Code of practice for information security management”, June 2005.
- “Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades”, MAP, 2004.
- C. Alberts and A. Dorofee, “Managing information Security Risks. The OCTAVE Approach”, Addison Wesley, 2003.
- UNE-ISO/IEC 17799:2002, “Tecnología de la Información. Código de Buenas Prácticas de la Gestión de la Seguridad de la Información”, 2002.
- United States General Accounting Office, Accounting and Information Management Division, “Information Security Risk Assessment -- GAO Practices of Leading Organizations.
- Ministerio de Administraciones Públicas, “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”, MAP, versión 1.0, 1997.

Appendix 1. Glossary

Different authors or organisations define the same terms in different ways. The following tables contain definitions as they are used in this guide, in both Spanish and English. Of the many definitions, those preferred in Magerit v2 have been chosen and are shown in bold. When the definition comes from a source, this is quoted.

1.1. Terms

Accrediting	The action of allowing an information system or network to process sensitive data, determining both the degree to which the design and the implementation of the system meet the pre-set security and technical requirements. [CESID:1997] Accreditation: Formal declaration by the responsible management approving the operation of an automated system in a particular security mode using a particular set of safeguards. Accreditation is the official authorization by management for the operation of the system, and acceptance by that management of the associated residual risks. Accreditation is based on the certification process as well as other management considerations. [15443-1:2005]
Accountability	**Assurance that who did what and when can be determined at all times.** Accountability: A quality that allows all the actions carried out to an information technology system to be associated unequivocally with an individual or entity. [CESID:1997] Accountability: The property that ensures that the actions of an entity may be traced uniquely to the entity. [13335-1:2004] Accountability: Process of tracing information system activities to a responsible source. [CNSS:2003]
Accumulated risk	The calculated risk taking into consideration the value of an asset and the value of the assets that depend on it. This value is combined with the degradation caused by a threat and its estimated frequency.
Accumulated value	**Considers the value of the asset itself and that of the assets that depend on it.** Inherited goods: Those inherited from the grandparents. [DRAE]
AGR	Risk analysis and management
Asset	**Resources of the information system or related with it that are necessary for the organisation to operate correctly and to attain the objectives proposed by its management.** Resources of the information system or related with it that are necessary for the organisation to operate correctly and to attain the objectives proposed by its management. [Magerit:1997] Goods: In terms of values, an element with a positive value making it estimable. [DRAE] Asset: Anything that has value to the organisation. [13335-1:2004] Asset: A component or part of the total system. Assets may be of four types: physical, application software, data, or end user services. [CRAMM:2003] Asset: Something of value to the enterprise. [Octave:2003] Asset: Any information resource with value that is worth protecting or preserving. [TDIR:2003] Assets: Information or resources to be protected by the countermeasures of a Target of Evaluation. [CC:1999]
Attack	Any deliberate action designed to break through the security mechanisms

	in an information system. [CESID:1997]
Authenticity	**Assurance of identity or origin.** Authentication: The property of giving and recognising the authenticity of the assets in the domain (of information type) and/or the identity of those involved and/or the authorisation by those issuing it as well as the checking of these three matters. [Magerit:1997] Authenticity: Having an undisputed identity or origin. [OPSEC] Authenticity: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. [800-53:2004] Authenticity: The property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems, and information. [13335-1:2004]
Availability	**Assurance that the authorised users have access when they require it to the information and its associated assets.** Assurance that the authorised users have access when they require it to the information and its associated assets. [17799:2002] Property that prevents the unauthorised denial of access to assets in the domain. [Magerit:1997] Availability: The assurance that data transmissions, computer processing systems, and/or communications are not denied to those who are authorized to use them (JCS 1997) [OPSEC] Availability: Ensuring timely and reliable access to and use of information. [800-53:2004] Availability: The extent to which, or frequency with which, an asset must be present or ready for use. [Octave:2003] Availability: Timely, reliable access to data and information services for authorized users. [CNSS:2003] [TDIR:2003] [CIAO:2000] Availability: The property of being accessible and usable upon demand by an authorized entity. [7498-2:1989]
Certification	Confirmation of the result of an evaluation and that the evaluation criteria used were applied correctly.
Confidentiality	**Assurance that the information is accessible only to those authorised to have access.** Assurance that the information is accessible only to those authorised to have access. [17799:2002] A property that prevents the unauthorised disclosure of assets in the domain. [Magerit:1997] Confidentiality: An assurance that information is not disclosed to unauthorized entities or processes (DOD JP 1994; JCS 1997) [OPSEC] Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [800-53:2004] Confidentiality: The requirement of keeping proprietary, sensitive, or personal information private and inaccessible to anyone that is not authorized to see it. [Octave:2003] Confidentiality: Assurance that information is not disclosed to unauthorized persons, processes, or devices. [CNSS:2003] [TDIR:2003] Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [7498-2:1989]
Control	See safeguard.
Controls selection document	A formal document for a group of safeguards that shows whether they apply to the information system being studied or whether they are meaningless.
Countermeasure	See safeguard.

Deficiencies report	**Report: Absence or weakness of safeguards that appear suitable for reducing the risk to the system.**
Deflected risk	The calculated risk taking into consideration the value of an asset. This value is combined with the degradation caused by a threat and its estimated frequency, both measured on the assets on which it depends.
Degradation	The loss of the value of an asset as a result of the appearance of a threat.
Dimension	**(Of security) An aspect, different to other possible aspects, that allows the value of an asset to be measured in the sense of the damage that would be caused by its loss of value.**
Frequency	**The rate at which a threat occurs.**
Impact	**The effect that the appearance of a threat has on an asset.** The effect that the appearance of a threat has on an asset. [Magerit:1997] Impact: The result of an information security incident. [13335-1:2004] Impact: The effect of a threat on an organisation's mission and business objectives. [Octave:2003] Impact: The effect on the organisation of a breach in security. [CRAMM:2003]
Impact analysis	Study of the consequences to the organisation of a stoppage of X time.
Incident	**Event with negative consequences for the information system security.** Information security event: An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant. [17799:2005] Information security incident: Any unexpected or unwanted event that might cause a compromise of business activities or information security. [13335-1:2004] Incident: A successful or unsuccessful action attempting to circumvent technical controls, organizational policy, or law. This is often called an attack. [TDIR:2003]
Information system	**Computers and electronic communications networks as well as the electronic data stored, processed, retrieved or transmitted by them for their operation, use, protection and maintenance.** A group of physical and logical elements, communications elements, data and personnel that allow the storage, transmission and processing of information. [Magerit:1997] Any system or product designed to store, process or transmit information. [CESID:1997] Information System: Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. [CNSS:2003] Information System: Any procedure or process, with or without IT support, that provides a way of acquiring, storing, processing or disseminating information. Information systems include applications and their supporting infrastructure. [CRAMM:2003]
Integrity	**Guarantee of the exactness and completeness of the information and the methods for processing it.** Guarantee of the exactness and completeness of the information and the methods for processing it. [17799:2002] Property that prevents the unauthorised modification or destruction of assets in the domain. [Magerit:1997] Information integrity: The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed (NSC EO 1995; JCS 1997). [OPSEC]

Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [800-53:2004]

Integrity: the property of safeguarding the accuracy and completeness of assets. [13335-1:2004]

Integrity: the authenticity, accuracy, and completeness of an asset. [Octave:2003]

Data integrity: A condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed. [CNSS:2003] [TDIR:2003] [CIAO:2000]

Data integrity: The data quality that exists as long as accidental or malicious destruction, alteration, or loss of data does not occur. [CRAMM:2003]

Integrity: Condition existing when an information system operates without unauthorized modification, alteration, impairment, or destruction of any of its components. [CIAO:2000]

Residual impact

The impact remaining in the system after the implementation of the safeguards described in the information security plan.

Residual risk

The risk remaining in the system after the implementation of the safeguards described in the information security plan.

Risk remaining after applying safeguards in a simulation scenario or in the real world. [Magerit:1997]

Residual risk: The risk that remains after risk treatment. [13335-1:2004]

Residual risk: Portion of risk remaining after security measures have been applied. [CNSS:2003] [CRAMM:2003]

Residual Risk: The potential for the occurrence of an adverse event after adjusting for the impact of all in-place safeguards. [TDIR:2003]

Risk

Estimate of the degree of exposure to a threat appearing to one or more assets, causing damages or prejudices to the organisation.

The possibility of a specific impact occurring on an asset, a domain or the entire organisation. [Magerit:1997]

The probability that a vulnerability in the information system will be used by the threats to that system in order to penetrate it. [CESID:1997]

Risk: combination of the probability of an event and its consequence. [17799:2005][Guide 73:2002]

Risk: A measure of the potential degree to which protected information is subject to loss through adversary exploitation. [OPSEC]

Risk: the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation. [13335-1:2004]

Risk: Possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability. [CNSS:2003]

Risk: A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting adverse impact. Reducing either the threat or the vulnerability reduces the risk. [TDIR:2003]

Total risk: The potential for the occurrence of an adverse event if no mitigating action is taken (i.e., the potential for any applicable threat to exploit a system vulnerability). [TDIR:2003]

Risk: A measure of the exposure to which a system or potential system may be subjected. [CRAMM:2003]

Risk analysis

The systematic process for estimating the size of the risks to which an organisation is exposed.

Identification of threats to the components belonging or relating to the information system (known as “assets”) to determine the system’s vulnerability to these threats and to estimate the impact or degree of damage that insufficient security may have for the organisation, obtaining a certain knowledge of the risk being run. [Magerit:1997]

Risk analysis: Systematic use of information to identify sources and to estimate the risk. [17799:2005][Guide 73:2002]

Risk assessment: Process of evaluating the risks of information loss based on an analysis of threats to, and vulnerabilities of, a system, operation or activity. [OPSEC]

Risk analysis: The systematic process of estimating the magnitude of risks. [13335-1:2004]

Risk Analysis: Examination of information to identify the risk to an information system. [CNSS:2003]

Risk Assessment:: Process of analyzing threats to and vulnerabilities of an information system, and the potential impact resulting from the loss of information or capabilities of a system. This analysis is used as a basis for identifying appropriate and cost-effective security countermeasures. [CNSS:2003]

Risk Analysis: An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence. [TDIR:2003]

Risk Assessment: A study of vulnerabilities, threats, likelihood, loss or impact, and theoretical effectiveness of security measures. The process of evaluating threats and vulnerabilities, known and postulated, to determine expected loss and establish the degree of acceptability to system operations. [TDIR:2003]

Risk management

Selection and implementation of safeguards to know, prevent, reduce or control the identified risks.

Selection and implementation of the security measures or “safeguards” that are suitable to know, prevent, reduce or control the identified risks and to reduce their potential or possible damage to the minimum. Risk management is based on the results of analysing the risks. [Magerit:1997]

Risk management: Coordinated activities to direct and control an organisation with regard to risk. [17799:2005][Guide 73:2002]

Risk management: A security philosophy which considers actual threats, inherent vulnerabilities, and the availability and costs of countermeasures as the underlying basis for making security decisions (JSCR 1994). [OPSEC]

Risk management: Process of identifying and applying countermeasures commensurate with the value of the assets protected based on a risk assessment. [CNSS:2003]

The identification, assessment, and mitigation of probabilistic security events (risks) in information systems to a level commensurate with the value of the assets protected. [CIAO:2000]

Risk map

Report: List of the threats to which the assets are exposed.

Threat Analysis: The examination of all actions and events that might adversely affect a system or operation. [TDIR:2003]

Threat Assessment: An evaluation of the nature, likelihood, and consequence of acts or events that could place sensitive information and assets as risk. [TDIR:2003]

Risk status

Report: Characterisation of assets by their residual risk; that is, what could happen, taking into consideration the safeguards deployed.

Safeguard

Procedure or technological mechanism that reduces the risk.

Control: Means of managing risks, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management or legal nature. [17799:2005]

Countermeasure: Anything which effectively negates or mitigates an adversary’s ability to exploit vulnerabilities. [OPSEC]

Safeguard: Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management

	constraints, personnel security, and security of physical structures, areas, and devices. [800-53:2004] Safeguard: a practice, procedure or mechanism that treats risk. [13335-1:2004] Countermeasure: Action, device, procedure, technique, or other measure that reduces the vulnerability of an information system. [CNSS:2003] Security safeguard: Protective measures and controls prescribed to meet the security requirements specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. [CNSS:2003] Countermeasure: Any action, device, procedure, technique, or other measure that mitigates risk by reducing the vulnerability of, threat to, or impact on a system. [TDIR:2003]
Safeguards evaluation	**Report: Evaluation of the effectiveness of the existing safeguards in relation to the risks they face.**
Security	**The capability of networks or information systems to resist accidents or illegal or malicious actions that compromise the availability, authenticity, integrity and confidentiality of the data stored or transmitted and of the services that these networks or systems make available with a specific level of competence.** Information system security: Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. [CNSS:2003]
Security audit	Independent study and examination of the history and activities of an information system in order to check the suitability of the system's controls, and to ensure their compliance with the security structure and operational procedures to detect breaches in security and to recommend changes in procedures, controls and security structures.
Security plan	**Group of security programs that put Risk management decisions into practice.**
Security programme	**Grouping of tasks defined to face the risk to the system. The grouping is made by convenience either because the tasks by themselves lack effectiveness or because the tasks have a common objective or because the tasks involve a single unit of action.**
Security project	**Security programme whose scope is such that it requires a specific plan.**
Threat	**Events that may cause an incident in the organisation, producing material damage or immaterial losses in its assets.** Events that may cause an incident in the organisation, producing material damage or immaterial losses in its assets. [Magerit:1997] Condition in the information system's environment which may cause a security violation, given the opportunity. [CESID:1997] Threat: A potential cause of an incident which may result in harm to a system or organisation. [17799:2005][13335-1:2004] Threat: Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [800-53:2004] Threat: Any circumstance or event with the potential to adversely impact an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. [CNSS:2003] Threat: An activity, deliberate or unintentional, with the potential for causing

	harm to an automated information system or activity. [TDIR:2003] Threat: Any circumstance or event that could harm a critical asset through unauthorized access, compromise of data integrity, denial or disruption of service, or physical destruction or impairment. [CIAO:2000] A threat is an indication of a potential undesirable event. [NSTISSI:1998] Threat: A potential violation of security. [7498-2:1989]
Value	**Of an asset. An estimate of the cost of the appearance of a threat.** Quality of some realities, considered goods, which makes them estimable. [DRAE]
Value model	**Report: A description of the value of the assets to the organisation as well as the dependencies between the assets.**
Vulnerability	**Estimate of the effective exposure of assets to a threat. It is determined by two measurements: frequency of occurrence and the degradation caused.** The vulnerability of an asset is the potential or possibility of the appearance of a threat to it. [Magerit:1997] Weakness in the security of an information system. [CESID:1997] Vulnerability: A weakness of an asset or group of assets that can be exploited by one or more threats. [17799:2005][13335-1:2004] Vulnerability: The susceptibility of information to exploitation by an adversary. [OPSEC] Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited. [CNSS:2003] Vulnerability: A weakness or lack of controls that would allow or facilitate a threat actuation against a specific asset or target. [CRAMM:2003]

1.2. ISO/IEC Guide 73:2002

ISO/IEC Guide 73:2002 uses the following structuring of terms:

Risk management:
coordinated activities to direct and control an organization with regard to risk.

Risk assessment:
overall process of risk analysis and risk evaluation.

Risk analysis:
systematic use of information to identify sources and to estimate risk.

Source identification:
process to find, list and characterize sources[46].

Risk estimation:
process used to assign values to the probability[47] and consequences of a risk.

Risk evaluation:
process of comparing the estimated risk against given risk criteria to determine the significance of the risk.

Risk treatment:
process of selection and implementation of measures to modify risk.

The following tables shows the alignment between Guide 73 and Magerit v2:

[46] Source: item or activity having a potential for a consequence.
Consequence: outcome of an event.
Event: occurrence of a particular set of circumstances.

[47] Probability: extend to which an event is likely to occur.

Guide 73:2002	Magerit v2	
Risk management	Risk análisis and management	P1 + P2 + P3
Risk assessment		
Risk analysis	Risk analysis	P2
Source identification		
Risk estimation		
Risk evaluation		A3.1
Risk treatment	Risk management	A3.2 + A3.3

1.3. References

[DRAE]
Real Academia Española. Diccionario de la Lengua Española. 22.ª edición, 2001.
http://buscon.rae.es/diccionario/drae.htm

[OPSEC]
OPSEC Glossary of Terms,
http://www.ioss.gov/docs/definitions.html

[17799:2005]
ISO/IEC 17799:2005, “Information technology -- Code of practice for information security management”, 2005.

[15443-1:2005]
ISO/IEC TR 15443:2005, “Information technology -- Security techniques -- A framework for IT security assurance -- Part 1: Overview and framework”, 2005.

[800-53:2004]
NIST, “Recommended Security Controls for Federal Information Systems”, National Institute of Standards and Technology, special publication 800-53, 2004.

[13335-1:2004]
ISO/IEC 13335-1:2004, “Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management”, 2004.

[CRAMM:2003]
“CCTA Risk Analysis and Management Method (CRAMM)”, Version 5.0, 2003.

[Octave:2003]
C. Alberts and A. Dorofee, “Managing information Security Risks. The OCTAVE Approach”, Addison Wesley, 2003.

[TDIR:2003]
Texas Department of Information Resources, “Practices for Protecting Information Resources Assets“, Revised September 2003.

[CNSS:2003]
Committee on National Security Systems, Instruction No. 4009, “National Information Assurance (IA) Glossary“, May 2003.

[17799:2002]
UNE ISO/IEC :2002, “Tecnología de la Información – Código de Buenas Prácticas para la Gestión de la Seguridad de la Información”, 2002.

[CIAO:2000]
Critical Infrastructure Assurance Office, “Practices for Securing Critical Information Assets”,

January 2000.

[CC:1999]
ISO/IEC 15408:1999, “Information technology — Security techniques — Evaluation criteria for IT security”, 1999.

[NSTISS:1998]
National Security Telecommunications and Information Systems Security Committee, “Index of National Security Telecommunications Information Systems Security Issuances”, NSTISSI no. 4014, NSTISSC Secretariat, 1998.

[CESID:1997]
Centro Superior de Información de la Defensa, “Glosario de Términos de Criptología”, Ministerio de Defensa, 3ª edición, 1997.

[Magerit:1997]
Ministerio de Administraciones Públicas, “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”, MAP, versión 1.0, 1997.

[Ribagorda:1997]
A. Ribagorda, “Glosario de Términos de Seguridad de las T.I.”, Ediciones CODA, 1997.

[7498-2:1989]
ISO 7498-2:1989, “Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture”, 1989.

Appendix 2. References

Some of the chapters and appendices contain bibliographic references that are specific to the matter under discussion. This appendix contains the references to methods that consider risk analysis and management as an integral activity. The references are sorted by date, from the most recent to the oldest.

- Federal Office for Information Security (BSI). “IT Baseline Protection Manual”, October 2003 Germany.
  http://www.bsi.de/gshb/english/etc/index.htm
- “The Vulnerability Assessment and Mitigation Methodology”, P.S. Antón et al., RAND National Defense Research Institute, MR-1601-DARPA, 2003.
- “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/
- “Information Security Risk Analysis”, T.R. Peltier, Auerbach Pub; 1st edition (January 23, 2001)
- “Risk Management: Multiservice Tactics, Techniques, and Procedures for Risk Management”, Air Land Sea Application Center, FM 3-100.12, MCRP 5-12.1C, NTTP 5-03.5, AFTTP(I) 3-2.30. February 2001.
- Air Force Pamphlet 90-902, “Operational Risk Management (ORM) Guidelines and Tools”, December 2000.
- KPMG Peat Marwick LLP, “Vulnerability Assessment Framework 1.1“, October 1998
- 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
- GMITS, ISO/IEC TR 13335-2:1997, “Information technology - Security techniques - Guidelines for the management of IT security - Part 2: Managing and planning IT security”.

Finally, mention must be made of a tool that implicitly contains a methodology. Because it is a product, the date is that of the latest version on the market.

- CRAMM, “CCTA Risk Analysis and Management Method (CRAMM)”, Version 5.0, 2003.

Appendix 3. Legal framework

This section is only available in Spanish.

Appendix 4. Evaluation and certification framework

The complexity of information systems requires a great deal of effort to determine the quality of the security measures with which it has been equipped and their trustworthiness. Frequently, third parties appear to independently issue judgments on these aspects, judgments which are issued after a rigorous evaluation and contained in a recognised document.

This chapter describes two frameworks in which the process of evaluation and certification (or registry) has been formalised:

- In information security management systems.
- In security products.

The opportunity, the way of organising oneself to reach certification and the administrative and standards framework in which the activities are carried out are described for both of these frameworks.

4.1. Information security management systems (SGSI)

The problems of security in information systems have a technical origin but are so complex that the solution can not be exclusively technical. Technology is too rich in opportunities and therefore it must be kept under control, ensuring that it works for the organisation's objectives.

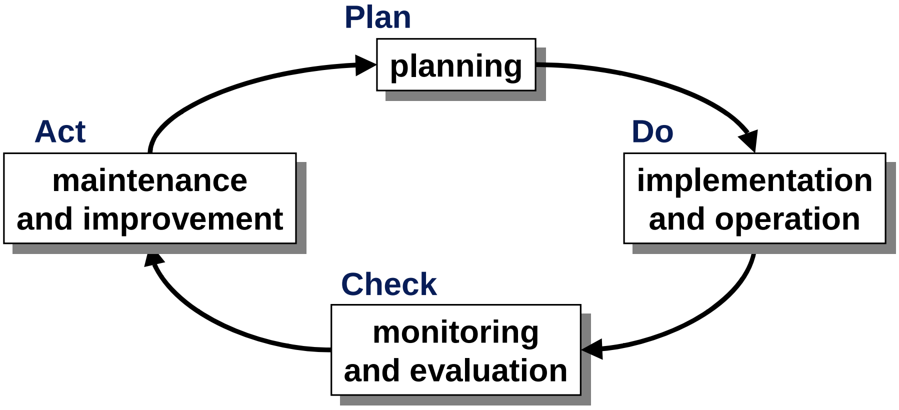
Security means being prepared (beforehand), prepared to react to foreseen or unforeseen emergencies and to know how to recover after the disaster. None of this is free: it costs money, time and effort. It is therefore necessary to use financial criteria to reach a balanced solution between preventing what happens, what is done to detect failures and what is done to prepare for the time when something occurs, something which, theoretically, should never occur. This must be done without forgetting the time dimension because cost and investments must be rationalised so that we know today what we may discover tomorrow.

There is therefore a management component that is as necessary as the technical components.

Information security management system

This is a management system which includes the policy, organisational structure, procedures, processes and resources needed to implement the management of information security. This system is the tool for the management of organisations to carry out the security policies and objectives (integrity, confidentiality and availability, assignation of responsibilities, authentication, etc). It provides mechanisms to safeguard the information assets and those of the systems which process them according to the organisation's security policies and strategic plans. [UNE 71502:2004]

This is the essence of the PDCA model (plan, do, check, act) used in quality management models.


Plan
planning
Do
implementation and operation
Check
monitoring and evaluation
Act
maintenance and improvement

The planning (P for plan) must include a security policy that sets objectives and a risk analysis that models the system's value, its exposure to threats and what it has (or needs) to keep the risk under control. It is natural that these bases are used to generate a security plan for Risk management.

The action (D for do) means carrying out a plan in its technical and organisational aspects, involving those persons in charge of the system or related with it. A plan is successful when daily operations are carried out without surprises.

The monitoring (C for check) of the system's operation begins with the fact that one cannot blindly confide in the effectiveness of the measures but must continually evaluate whether they respond as expected with the desired effectiveness. It is necessary to measure both what occurs and what would occur if measures had not been taken. Sometimes one speaks of the "cost of insecurity" as a justification for spending money and effort. It is also necessary to be aware of novelties that arise in both modifications to the information system itself and in the form of new threats.

The reaction (A for act) is knowing how to obtain consequences from experience, one's own and that of similar systems, repeating the PDCA cycle.

The evaluation of a security management system starts with the supposition that the above scheme guides the organisation's actions in security matters and judges the effectiveness of the implemented controls to reach the proposed objectives.

4.1.1. Certification

The certification of a security management system consists of somebody who is competent affirming that a system is healthy and guarantees it with his word (in writing) with all the precautions of scope and time that are considered appropriate (and that are included explicitly), knowing that what is assured today must be revised over the medium term because everything changes.

A series of processes must be followed to obtain a certificate. Without going into excessive detail, we will describe how the team sent by the certification organisation evaluates the equipment to be judged.

The first thing to be done is to delimit the scope of what is to be evaluated as the "information security management system". This is a delimitation for each organisation which reflects its mission and its internal organisation. It is important to delimit clearly. If the perimeter is unclear, what needs to be done in the following steps is unclear, especially with regard to the persons or departments from whom the relevant information must be obtained. Note that this may not be evident. Currently, it is rare to find an organisation that is closed from the point of view of its information systems: the outsourcing of services, electronic government and electronic commerce have diluted frontiers. Additionally, the internal organisational chart rarely shows security responsibilities.

The next thing which must be clear, written and maintained is the corporate security policy. Often, the security policy includes a list of the legislation that affects it. It is absolutely necessary to delimit the legal and regulatory framework to be followed.

Everything must be in writing, and well written: it must be understandable, coherent, published, known to those involved and kept up-to-date. A certification process always includes a strong documentation revision component.

A picture of the organisation's risk status must be taken before the evaluation team arrives. In other words, a risk analysis must be made, identifying assets, valuing them, identifying and valuing the significant threats. This process includes determining which safeguards the system requires and with which quality. Each case is a separate world: not everyone has the same assets, and not all assets have the same values and are interconnected in the same way, and not everyone is subject to the same threats and neither does everyone adopt the same protection strategy. The important point is to have a strategy, marked by the policy and the detail on the Risk map.

A risk analysis is an essential management tool. Preparing or not preparing a risk analysis does not mean greater or lesser security; it simply means knowing where you are.

The results of the risk analysis allow the preparation of a statement of applicability and provides a justification for the quality required. All this must be checked by the evaluation team which, if satisfied, will issue the certificate.

The evaluation team inspects the information system to be certified, comparing it with a recognised reference that allows the objective evaluation to avoid any type of arbitrariness or subjectivity and allows the universal use of the certificates issued. A "certification scheme" is used (for example, in Spain we have the UNE 71502 standard).

The UNE 71502:2004 standard is designed to specify the “requirements to establish, implement, document and evaluate an information security management system according to the UNE ISO/IEC 17799:2002 standard within the context of the risks identified by the organisations. It specifies the requirements of the security controls according to the organisations’ requirements independently of their type, size or area of activity.”

The UNE 71502:2004 standard is based on a list of controls which are in turn based on the UNE-ISO/IEC 17799:2002 standard. The list must be adjusted to the organisation to be evaluated, removing those elements that are not relevant. If considered necessary, additional specific controls are chosen beyond UNE-ISO/IEC 17799 for each organisation that match its specific business model as well as the objectives to be obtained with them, justifying the selection.

The basic list is:

Security policy

Periodic revision and evaluation of the security policy.

Control and management of the documentation.

Organisational aspects for security

Assignation of responsibilities for information security.

Identification of the risk through access by third parties.

Contracting of services.

Contracting of outsourcing.

Contracting of collaborating companies.

Classification and control of assets

Inventory of assets.

Classification of assets.

Classification of the information.

Periodic revision and classification of assets.

Periodic revision of the risk analysis.

Marking and handling of the information.

Security connected with personnel

Contracting of personnel.

Training.

Reporting of incidents.

Physical and environment security

Installation and protection of equipment.

Maintenance of equipment.

Management of communications and operations

Operational processes.

Control of changes.

Management of incidents.

Measures and controls against harmful software.

Recovery of information.

Management of removable media.

Elimination of media.

E-mail security.

Availability of public systems.

Control of input, storage and output of information.

Analysis and management of records.

System capacity planning.

Physical exchange of information.

Logical exchange of information.

Authorisation for the output of material and/or information.

Back-up copies and restoration.

Access control

Identification and authentication of users.

Restriction of access to the information.

Control of access to the network.

Control of access to the operating system.

Control of logical access to the information.

Management of passwords.

Remote equipment management.

Development and maintenance of systems

Control of move from development to tests.

Control of move from tests to production.

Control of changes to operating system.

Control of changes to the software.

Selection, control and approval of external software.

Control of the design of applications.

Specification of security requirements.

Control of operational software.

Management of business continuity

Management of business continuity.

Maintenance and evaluation of the continuity plans.

Conformity

Identification of the applicable legislation.

Revision of compliance with legislation.

Internal audits.

4.1.2. Accrediting by the certification organisation

The credibility of the certification amounts to the trustworthiness of the organisation providing the certification. How is this confidence achieved?

One essential component is the credibility of the certification scheme. A second component is the credibility of the organisation that issues the certificates. This organisation is responsible for the competence of the evaluation team and for carrying out the evaluation process. To certify that these responsibilities are complied with, an "accrediting process" is used in which a new organisation evaluates the evaluator. In Spain, the organisation responsible for accrediting certification organisations is ENAC which follows internationally recognised standards for certificates issued by certification authorities in different countries.

4.1.3. Terminology

The following lists the terms used in information systems certification activities, as understood in this context.

Accrediting

A procedure in which an authorised organisation formally recognises that an organisation is competent to carry out a specific conformity evaluation activity.

Auditing

See "evaluation".

Certification

The purpose of certification is "to publicly declare that a product, process or service complies with the set requirements."

Certification: A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. [NIST SP 800-37]

Certification document (or record)

A document that confirms that the information security management system (SGSI) in an organisation conforms to the reference standards adapted to the features of the certified organisation.

Control selection document

A document that describes the objectives of control and the relevant and applicable controls for the information security management system in the organisation. This document must be based on the results and conclusions of the risk analysis and management process.

Certification scheme

A technical and administrative framework that sets the working reference for comparing the conformity of the organisation being evaluated, issues the certificate or record and keeps it updated and valid.

Evaluation

A group of activities that allow the determination of whether an organisation meets the applicable criteria within a certification scheme. It includes preparatory activities, revision of the documentation, inspection of the information system and preparation of the relevant documentation for issuing the conformity certificate, if applicable.

Certification (or record) organisation

An organisation which uses the evaluation report to certify (or record) that the organisation satisfies the requirements set in the certification scheme.

Conformity evaluation organisations

These are responsible for evaluating and providing an objective declaration that the services and products comply with specific requirements, either regulatory or voluntary.

Security policy

A group of regulatory standards, rules and practices that determine the way in which the assets - including the information considered as sensitive - are managed, protected and distributed within an organisation.

4.1.4. References

- ISO/IEC 17799:2005, *"Information technology -- Code of practice for information security management",* 2005.
- UNE 71502:2004, *"Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI)",* 2004.
- UNE-ISO/IEC 17799:2002, *"Tecnología de la Información. Código de Buenas Prácticas de la Gestión de la Seguridad de la Información",* 2002.
- ISO Guide 72:2001, *"Guidelines for the justification and development of management system standards",* 2001.
- European Co-Operation for Accreditation, "Guidelines for the Accreditation of Bodies Operating Certification/Registration of Information Security Management Systems", *EA-7/03, February 2000.*

4.2. Common evaluation criteria (CC)

The need to evaluate the security of an information system appeared very early in the processes for acquiring equipment by the Department of Defense in the USA which, in 1983, published the so-called "Orange Book" (TCSEC – Trusted Computer System Evaluation Criteria). The objective was to specify unambiguously what the purchaser needs and what the seller offers so that there are no misunderstandings; instead, there is a transparent scheme for evaluation, guaranteeing the objectivity of the acquisitions.

The same need caused the appearance of European initiatives such as ITSEC *(*Information Technology Security Evaluation Criteria*)*. During the 1990s, evaluation criteria proliferated world wide, greatly hindering international trade, and bringing about an agreement for convergence, called "Common Criteria for Information Technology Security Evaluation*"*, normally known as "Common Criteria" or by its initials, CC.

As well as the need for a universal understanding, the CC include the changing nature of information technologies which, since 1980, have moved from being centred on computer equipment to include much more complex information systems.

The CC allow:

1. The definition of security functions[48] in products and systems (in information technologies).
2. The determination of the criteria for evaluating [the quality] of these functions.

It is essential that the CC be open to allow the evaluation to be objective and to be carried out by a third party (neither by the supplier nor by the user) so that the choice of suitable safeguards is notably simplified for organisations that need to mitigate their risks.

The Spanish administration - and many others - recognises the security certificates issued in other countries on the basis of the "Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology" [49].

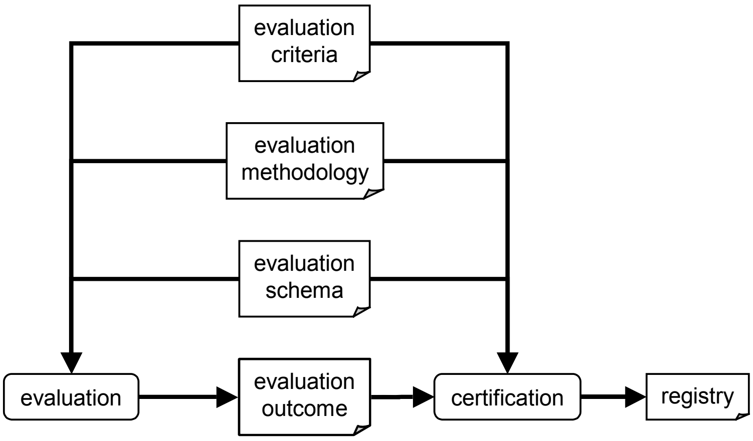
The evaluation of a system is the basis for its certification. Certification requires the availability of:

1. Criteria that define the meaning of the elements to be evaluated.
2. A methodology that defines how the evaluation is carried out.
3. A certification scheme[50] that sets the administrative and regulatory framework under which the certification is carried out.

[48] CC use their own terminology, which is rigorous but not always obvious. The precise definition of each term in the context of the CC is defined below.

[49] On 23 May 2000 in Baltimore (Maryland, USA) Germany, Australia, Canada, Spain, the United States, Finland, France, Greece, Italy, Norway, New Zealand, the Netherlands and the United Kingdom ratified their adherence to the Arrangement on the Recognition of the Common Criteria Certificates in the field of Information Technology Security (hereinafter, the Arrangement). Later, they were joined by Israel, Sweden, Austria, Turkey, Hungary, Japan, the Czech Republic, Korea, Singapore and India. See http://www.csi.map.es/csi/pg3433.htm.

[50] Royal Decree 421/2004, 12 March, regulates the functions of the National Cryptological Centre, which include that of "forming the certification organisation of the national scheme for evaluating and certifying security in information technologies applied to products and systems within its sphere". The national scheme can be found at http://www.oc.ccn.cni.es/.



This allows the objectivity of the process to be guaranteed, that is, it encourages confidence that the results of a certification process are universally valid, regardless of where the certification was carried out.

Given that [the quality of] the security required in a system is not always the same but depends on its use, the CC set a scale of assurance levels[51]:

EAL0: No guarantees.

EAL1: Functionally tested.

EAL2: Structurally tested.

EAL3: Methodically tested and checked.

EAL4: Methodically designed, tested and reviewed.

EAL5: Semi-formally designed and tested.

EAL6: Semi-formally verified, designed and tested.

EAL7: Formally verified, designed and tested.

The higher levels require greater effort in development and evaluation but in exchange offer great guarantees to the users. For example, in the area of electronic signatures, secured signature devices are usually certified with a profile at level EAL4+[52].

4.2.1. Beneficiaries

CC are aimed at a wide audience of potential beneficiaries of the formalisation of the concepts and elements for evaluation: consumers (users of security products), developers and evaluators. A common language between all of these provides appreciable advantages:

For consumers

- They can express their requirements before acquiring the services or products that they need. This characterisation can be useful both for individual acquisitions and in identifying the needs of groups of users
- They can analyse the features of the services or products offered on the market.
- They can compare different offers.

For developers

They know what will be required of them and how their developments will be evaluated.

They know objectively what the users require.

[51] EAL: Evaluation Assurance Level

[52] When a product falls between two levels, the lower level is shown followed by a “+” which is read as “enhanced”. Thus, a product evaluated EAL4+ means that it meets all the quality levels of Level 4 and some of those in the higher levels.

They can express what their developments do unambiguously.

For evaluators

They have a formalised framework for knowing what they have to evaluate and how they must classify it.

For everyone

They have objective criteria that allow the acceptance of certificates issued anywhere.

All of these participants converge on an object to be evaluated called **TOE** *(*Target Of Evaluation), which is simply the (security) service or product whose (security) properties are to be evaluated.

When a risk analysis provides a list of suitable safeguards, these can be expressed in CC terminology which allows it to connect with the above mentioned advantages, and become a standardised specification.

4.2.2. Security requirements

Given a system, a risk analysis allows the determination of which safeguards are required and with what quality. This analysis can be carried out on a generic system or on a specific one. In the CC, the group of requirements for a generic system is called the **protection profile (PP)**. When not dealing with a generic system but with a specific one, the group of requirements is known as the **security target (ST).**

Given their generic nature, the PPs cover different specific products. They are usually prepared by groups of users or international organisations that wish to model the market [53].

Because of their specific nature, the STs cover a specific product. They are usually prepared by the manufacturers themselves in order to formalise their offer [54].

CC determine the sections into which a PP or an ST must be structured. The index of these documents is a good indicator of their scope:

[53] A typical example of a PP is one that sets the security features to be required from a firewall.

[54] A typical example of an ST is one that sets the security features for Model 3000 from manufacturer XXL, SA, a model that allows telephone communications to be encrypted.

PP- protection profile	***ST – security target***
• Introduction • TOE description • Security environment: • Assumptions • Threats • Organizational security policies • Security objectives: • For the TOE • For the environment • Security requirements: • For the environment • TOE functional requirements • TOE assurance requirements • Application notes • Rationale	• Introduction • TOE description • Security environment: • Assumptions • Threats • Organizational security policies • Security objectives: • For the TOE • For the environment • Security requirements: • For the environment • TOE functional requirements • TOE assurance requirements • TOE summary specification • PP claims: • PP reference • PP tailoring • PP additions • Rationale

The PPs and STs may in turn be subjected to a formal evaluation that checks their completeness and integrity. The PPs evaluated in this way may be placed in public records for sharing by different users.

When preparing an ST, reference is made to the PPs that it includes.

4.2.3. Creation of protection profiles

The generation of a PP or an ST is basically a risk analysis process in which the analyst, having determined the domain of the analysis (the TOE in CC terminology) identifies threats and uses the impact and risk indicators to determine the required safeguards. In CC terminology, the required safeguards are called **security requirements** and are subdivided into two large groups:

Functional security requirements

- What must be done?
- They define the functional behaviour of the TOE.

Security functionality assurance requirements

- Is the TOE well built?
- Is it effective? Does it satisfy the objective for which it is required?
- Is it efficient? Does it achieve its objectives with a reasonable consumption of resources?

It is important to note that CC establish a common language for expressing the functional and assurance objectives. It is therefore necessary that the risk analysis uses this terminology in choosing safeguards. The CC standard provides, in part 2, the standardised catalogue of functional objectives while part 3 provides the standardised catalogue of assurance objectives.

Part 2: Functional requirements	*Part 3: Assurance requirements*
FAU: Security audit	ACM: Configuration management
FCO: Communication	ADO: Delivery and operation
FCS: Cryptographic support	ADV: Development
FDP: User data protection	AGD: Guidance documents
FIA: Identification and authentication	ALC: Life cycle support
FMT: Security management	ATE: Tests
FPR: Privacy	AVA: Vulnerability assessment
FPT: Protection of the TOE security functions	APE: PP evaluation
FRU: Resource utilisation	ASE: ST evaluation
FTA: TOE access	
FTP: Trusted path / channels	

4.2.4. Use of certified products

When a TOE has been certified according to a PP or an ST, depending on the case, it is certain that it meets the requirements and, further, that it meets them with the required quality (for example, EAL4).

The certification of a system or product is not a blind guarantee of suitability: it is necessary to ensure that the PP or ST with respect to which it has been certified meets the requirements of our system. The risk analysis has allowed us to prepare the PP or ST or, sometimes, to choose a group that is appropriate to our risk map. It is essential that from the risk analysis some security requirements have been obtained whose satisfaction will allow the residual impact and risks to be kept under control.

As a certified product matches a PP or ST that meets our needs, risk management is reduced to acquiring the product, installing it and operating it in suitable conditions.

It is important to note that both the PPs and STs include a section called “assumptions” setting a series of pre-requirements that must be met by the operational environment in which the TOE is installed. It must be realised that the best product is unable to guarantee the meeting of the overall objectives if it is unsuitably installed or operated. As a result, certified products are very solid components in a system but it is also necessary to ensure their environment to assure the complete system.

4.2.5. Terminology

Because their objective is to serve as an international reference for evaluations and certifications, the common criteria must be very precise in their terminology. In the above text, the terms have been introduced, as they were needed; these terms are explained formally below:

Assurance

grounds for confidence that an entity meets its security objectives.

Evaluation

assessment of a PP, an ST or a TOE against defined criteria.

Evaluation Assurance Level (EAL)

a package consisting of assurance components from CC part 3 that represents a point on the predefined assurance scale.

Evaluation authority

a body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community.

Evaluation scheme

the administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.

Formal

expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal

expressed in natural language.

Organisational security policies

One or more security rules, procedures, practices, or guidelines imposed by an organisation upon its operations.

Product

a package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.

Protection Profile (PP)

an implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security objective

a statement of intent to counter identified threats and/or satisfy identified organisation security policies and assumptions.

Security Target (ST)

a set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semi-formal

expressed in a restricted syntax language with defined semantics.

System

a specific IT installation, with a particular purpose and operational environment.

Target of Evaluation (TOE)

an IT product or system and its associated guidance documentation that is the subject of an evaluation.

TOE Security Functions (TSF)

a set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy (TSP)

a set of rules that regulate how assets are managed, protected and distributed within a TOE.

4.2.6. References

- "Arreglo sobre el Reconocimiento de los Certificados de Criterios Comunes en el campo de la Seguridad de las Tecnologías de la Información", Mayo, 2000.
- CC, "Common Criteria for Information Technology Security Evaluation", Versión 2.3, 2005.
  - Part 1: Introduction and general model
  - Part 2: Security functional requirements
  - Part 3: Security assurance requirements

  Also published as international standard ISO/IEC 15408:2005, part -1, -2 and -3.
- ITSEC, European Commission, "Information Technology Security Evaluation Criteria", version 1.2, 1991.

- TCSEC, Department of Defense, “Trusted Computer System Evaluation Criteria”, DOD 5200.28-STD, Dec. 1985.

Appendix 5. Tools

The undertaking of an AGR project involves working with a certain amount of assets that are rarely fewer than several dozen and normally numbered in the hundreds. The number of threats is typically in the order of several dozen while safeguards are in the thousands. All this tells us that it is necessary to handle a multitude of data and data combinations, leading, logically, to a search for automatic support tools.

As general requirements, a support tool for AGR projects must:

- Allow working with a wide group of assets, threats and safeguards.
- Allow the flexible treatment of a group of assets to accommodate a model that is close to the organisation's actual situation.
- Be used throughout the three processes in the project, especially to support process P2, Risk analysis.
- Not hide the reasoning that leads to conclusions from the analyst.

Tools can handle the information qualitatively or quantitatively. The choice between these modes has been the cause of a long debate. Qualitative models offer useful results compared to quantitative models, simply because the capture of qualitative data is more agile than the capture of quantitative data[55]. Qualitative models are more effective in relating that which is more important with that which is not so important but they form the conclusions into large groups. Quantitative models, on the other hand, achieve a more precise location of each aspect.

Residual impact and risk can be qualitative until large investments appear and it is necessary to determine their financial rationality - which is of more interest? At this point, numbers are needed.

A mixed option is useful: a qualitative model for the complete information system with the ability to enter into a quantitative model for those components whose protection will require large outlays.

It is also true that an organisation's value model must be used for a long time, at least during the years for which the security plan lasts, in order to analyse the effect of carrying out the programmes. It is notably more difficult to generate a value model from zero than to adapt an existing one to the development of the system's assets and to the evolution of the services provided by the organisation. This continuous evolution may involve the progressive migration from an initially qualitative model to an increasingly quantitative one.

It must be stressed that the data characterising the possible threats are tentative in the first models but experience allows the valuations to be matched to the actual situation.

Whether the tools are qualitative or quantitative, they must:

- Handle a reasonably complete catalogue of types of assets. This is shown in chapter 2 of the "Elements catalogue".
- Handle a reasonably complete catalogue of valuation dimensions. This is shown in chapter 3 of the "Elements catalogue".
- Help to value the assets by offering valuation criteria. This is shown in chapter 4 of the "Elements catalogue".
- Handle a reasonably complete catalogue of threats. This is shown in chapter 5 of the "Elements catalogue".
- Handle a reasonably complete catalogue of safeguards. This is shown in chapter 6 of the "Elements catalogue".
- Evaluate the residual impact and risks.

[55] Assets must be valued and this task requires consensus. Both the valuation and the search for consensus are notably quicker if an order of magnitude must be determined than if an absolute number must be determined.

It is interesting that the tools can import and export data handled in formats that can easily be processed by other tools such as:

XML – Extended Mark-up Language.

which is the option used in this guide, which sets XML formats for exchange.

CSV – Comma Separated Values.

5.1. PILAR

PILAR, the Spanish acronym for "Logical Computer Procedure for Risk Analysis", is a tool developed to the specifications of the National Intelligence Centre to support risk analysis in information systems using the Magerit methodology.

The tool has been completely developed in Java and can be used on any platform that supports this programming environment without requiring third party product licences. The result is a single user graphical application.

The tool supports all the Magerit method phases:

- Characterisation of assets: identification, classification, dependencies and valuation.
- Characterisation of threats.
- Evaluation of safeguards.

The tool includes the "Elements catalogue" to allow uniformity in the results of the analysis:

Types of assets.

Valuation dimensions.

Valuation criteria.

Catalogue of threats.

To incorporate this catalogue, PILAR differentiates between the risk calculation engine and the elements library, which can be replaced to follow the development over time of the elements catalogues.

The tool evaluates the impact and the risk - accumulated and deflected, potential and residual - displaying it in a way that allows the analysis of the reason for a certain impact or risk.

The safeguards are classified by phases, allowing different time situations to be incorporated in the same model. Typically, the result of the different security programmes during the undertaking of the security plan can be incorporated and the improvement to the system can be monitored.

The results are shown in various formats: RTF reports, charts and tables for incorporation in a spreadsheet. It is thus possible to provide different types of reports and presentations of the results.

Finally, the tool calculates security ratings according to the usual *de iure* or *de facto* standards, including:

- Security criteria, standardisation and conservation.
- UNE-ISO/IEC 17799:2002: Security management systems.
- RD 994/1999: Personal data.

It should also be noted that PILAR includes both qualitative and quantitative models with the ability to switch between them to obtain the maximum benefit of theoretical possibilities of each.

5.2. References

CARVER

"Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability", National Infrastructure Institute's Center for Infrastructure Expertise, USA.

COBRA

“Security Risk Analysis & Assessment, and ISO 17799 / BS7799 Compliance”, C&A Systems Security Ltd, UK.

CRAMM

“CCTA Risk Analysis and Management Method”. Insight Consulting. UK.

The CRAMM Risk Analysis and Management Method is owned, administered and maintained by the Security Service on behalf of the UK Government.

EBIOS

“Méthode pour l’Expression des Besoins et l’Identification des Objectifs de Sécurité”. Service Central de la Sécurité des Systèmes d'Information. France.

RIS2K

Basis for Magerit v1.0. Ministerio de Administraciones Públicas. España.

PILAR

“Procedimiento Informático-Lógico para el Análisis de Riesgos”. Centro Nacional de Inteligencia. Ministerio de Defensa. España.

Appendix 6. Evolution from Magerit version 1

This section is only available in Spanish.

Appendix 7. Study case

As an example, this appendix studies the case of an administrative unit that uses its own and third-party information systems for its internal tasks and for providing public information services (electronic government).

The example is only an illustration; the reader shall not derive greater consequences or conclusions that must be complied with. Even when faced with the same impact and risks, the solutions may be different without being able to be extrapolated blindly from one circumstance to another. Specially, it must be stressed the critical role that corresponds to the organisation's management as the last decision point with regard to the policy to be adopted for maintaining the impacts and risks under control.

Most of the following text presents the situation in "normal" words as it becomes initially known to to the working team during the interviews. It is the mission of this team to translate the knowledge acquired into the formal terms defined for this methodology

7.1. The history

The unit under study is not new, but has been handling documents for years, first manually and now with its own computer system. Recently, a connection has been added between its system and a central archive which behaves as a "historical memory" - it allows data to be recovered on start, and filed upon termitation. The latest novelty is to offer its own electronic government service in which users may carry out operations via the Web, using their identity card number as an identification together with a personal password. A civil servant who attends persons who visit the unit's premises, uses the same system locally.

The electronic government project manager, alarmed by news in the media regarding the lack of security on the Internet and knowing that a failure in the service would cause serious damage to his unit's image, takes on the role of promoter. In this role, he writes an internal report[56] for the unit manager, describing:

- The computer resources being used and to be installed.
- The incidents that have occurred since the unit has existed.
- His concerns regarding the use of the Internet for providing the service.

On the basis of this report, he presses for the launch of an risk analysis and management project.

Convinced of the need to take measures before a disaster occurs, management creates a Tracking Committee consisting of the managers of the services involved: user service, legal advice, computer services and physical security.

It is decided that the scope of the project (activity A1.2) will be the personal and remote electronic processing service. The security of the information handled will also be studied: files. With regard to the equipment, both equipment and communications networks will be analysed. The decision is made to leave elements that may be relevant in a more detailed analysis out of this study, such as systems' user identification and authentication data, the work areas of the personnel who handle them, the equipment room (data processing centre) and the persons related with the process. A future, more detailed project is planned for these aspects.

The evaluation of the security of the subcontracted services used is explicitly excluded. The analysis is local, confined to the unit concerned. These remote services were considered to be of "opaque" for the purposes of this analysis; that is, it is nor analysed how they are provided.

The project to launch (activity A1.4) includes a management meeting with the Tracking Committee in which the main points of the analysis are explained by the promoter who was appointed AGR project manager, in which two persons of his development team will take part with a consulting

[56] As usual in these initial phases, the project is not formalised. However, it is providing the "Preliminary Report" of activity "A1.1. Opportunity study".

contract with an external consulting company. One of the members of the internal team will have a technical profile: systems engineer. The external consultancy company is required to identify the persons who will participate and to sign a confidentiality agreement.

The project is announced internally by a general communication to all the personnel in the unit and personal notification to those persons directly involved. These communications identify the people responsible for the project.

7.2. Process P2: Risk analysis

The risk analysis phase starts with a series of interviews with the managers designated by the Tracking Committee, interviews in which the following participate:

- The link person as introducer.
- The external consultant as leader of the interview.
- The internal employee as the secretary: minutes of meeting and data collection.

Public service to the citizens

The service is provided by a computer database application developed in the past. The application is accessed via a local user identification that controls access privileges. For providing the service in person, those attending the end user identify themselves to the system. For remote processing, it is the end user the one who identifyies itself to the system.

The processing includes a request (and data entry) phase and a response (and data delivery) phase. Users make their request and await a notification to collect the reply. The notification is t sent by mail: by registered letter in the case of personal processing, and by electronic mail in the case of remote processing.

Starting a service involves opening a file, which is stored on the local network in the office. It also involves retrieving data from the central information archive, which are copied locally. When the service is closed, the data and a report of the actions carried out are sent to the central archive for safe keeping, eliminating the information from the local equipment.

The unit's personnel are identified by a user account, while remote users are identified by their identity card number. In both cases the system requires a password for authenticatication.

Finally, the role played by electronic mail throughout processing must be stressed, both as an internal communications medium between personnel and for notifying external users. As a rule, mail must not be used to transport documents; they must always be supplied by Web accesses.

Central archive service

A centralised archive and document recovery service is provided by an intranet. Users access it through a local Web interface that connects via a private virtual network with a remote server, with users identified by their identity card number. This service is only available to personnel in the unit and to the virtual employee who provides the remote formality service.

Computer equipment

The unit has various PCs in its premises. This equipment contains a Web navigator, an e-mail client without local storage of messages and a standard office package (word processor and spreadsheet).

Altough there is local information storage capacity on the PCs' disks, its use is discouraged and security copies are not made. In fact there is a procedure for installations/updates that deletes the local disk and re-installs the entire system.

The equipment have no removable media of any type: diskette, CD, DVD, USB, etc.

A medium-sized, general-purpose server is available as:

- File server.
- Electronic mail server, with local storage and access by Web.

- Database server: current files and user identification.
- Web server for remote processing and for the local intranet.

Communications

A local area network is available that covers the work premises and the equipment room. The installation of remote access modems and wireless networks is explicitly forbidden and there is a routine inspection procedure.

There is an ADSL Internet connection contracted with a commercial carrier. Several services are provided on this connection:

- Remote processing service (own).
- E-mail service (as part of the remote processing service).
- Information access service (own).
- Private virtual network with the central archive.

The Internet connection is exclusively via a firewall that limits the communications to the network, allowing only:

- The exchange of e-mail with the mail server.
- Web access with the Web server.

The private virtual network with the central archive uses a software application. The network is set up at the start of the working day and is automatically shit down at the end of the day. During setting up, terminal equipments recognise each other and set a session key for the day. There is no involvement of any local operator.

There is a feeling that many services depend on the Internet connection. Additionally, in the past, there have been incidents such as cuts in service due to municipal works and a deficient provision of service by the provider. As a result:

1. A service contract has been signed which sets a certain quality level, above which the operator must pay indemnities agreed beforehand in proportion to the period of interruption or to the slowness (insufficient volume of data transmitted in specific periods) of the connection.
2. A digital connection (ISDN) has been contracted with another supplier as a back up. This connection is not usually set up but is activated automatically when the ADSL connection is interrupted for more than 10 minutes.

Physical security

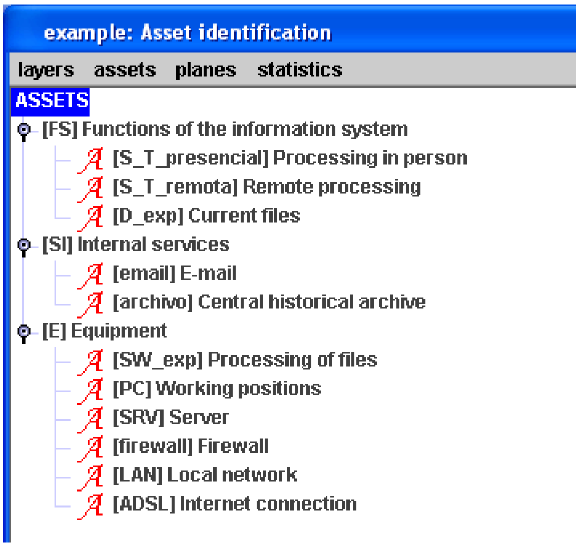
The personnel work in the unit’s premises, mainly inside, except a series of terminals in the public areas. Access to the interior areas is limited to office hours, after which it is closed with a key. During office hours there is an entrance control that identifies the employees and records their entry and exit times.

The equipment room is simply a room that is locked with a key kept by the systems administrator. The room has a fire detection and extinction system, which is checked annually. This room is 50 metres from the nearest water supply.

The unit’s premises occupy the entire fourth floor of a 12-storey office building. The access controls are the unit’s own, not those of the building, the use of which is shared with other activities. There is no control over what is on the floor above or on the floor below.

7.2.1. Task T2.1.1. Identification of assets

As a result of the above interviews, it was decided to work with the following group of assets [57]:



example: Asset identification

ASSETS

- [FS] Functions of the information system
  - [S_T_presencial] Processing in person
  - [S_T_remota] Remote processing
  - [D_exp] Current files
- [SI] Internal services
  - [email] E-mail
  - [archivo] Central historical archive
- [E] Equipment
  - [SW_exp] Processing of files
  - [PC] Working positions
  - [SRV] Server
  - [firewall] Firewall
  - [LAN] Local network
  - [ADSL] Internet connection

The types of assets in chapter 2 of the “Elements catalogue” have been used.

The actual system is more complex than the one modelled hereon. The simplification aims to focus on the usual problems that araise in these cases, rather than to model every detail.

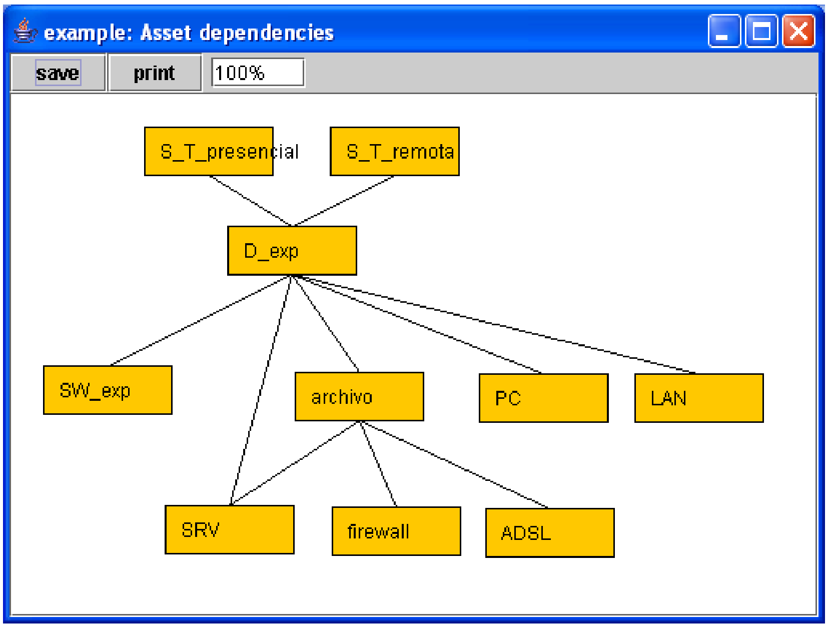
7.2.2. Task T2.1.2: Dependencies

The following matrix of the dependencies between assets has been determined using the operational (availability) and data storage (integrity and confidentiality) dependencies.

	[S_T_in person]	[S_T_remote]	[D_exp]	[email]	[archive]	[SW_exp]	[PC]	[SRV]	[firewall]	[LAN]	[ADSL]
[S_T_in person]			√	√	√	√	√	√		√	
[S_T_remote]			√	√	√	√		√	√	√	√
[D_exp]					√	√	√	√		√	
[email]								√	√	√	√
[archive]								√	√		√
[SW_exp]											
[PC]											
[SRV]											
[firewall]											
[LAN]											
[ADSL]											

[57] The list of assets groups these in three layers (in bold). The layer structure is simply a means of arranging the information. Each layer shows which assets there are of each type. The list in the “Elements catalogue”, Chapter “2, Types of assets”, has been used.

In real systems, this kind of table presentation is unfeasible, due to the large number of asssts. Sometimes, a graph is a better presentation means. The following picture shows the dependencies, above and below the data files:



7.2.3. Task T2.1.3: Valuation

Management is worried by the potential abuse of processing, some of which may include the payment of large amounts of money, either to the organisation or to the users. The existence of a financial motive may encourage abuse both by internal personnel and remote users, with special unease caused by the impunity of attackers who could attack from any remote part of the planet.

There is also special sensitivity regarding the availability of the services. There is especially concern that a request made in person cannot be attended to.

Web services for external users are considered “symbolic” and need special care to give an image of modernity, effectiveness and a vocation for service. Anything that could give a bad image, either because the service is not available or it is provided erroneously or because incidents are not attended to quickly, etc, are all situations that are to be avoided as far as possible.

Local databases contain information on persons regarded as of medium level within the classification of personal data.

Because of all this, the following valuation[58] of the system’s assets has been obtained. Only the higher assets in the dependencies tree have been explicitly valued, as follows:

	Security dimensions						
Asset	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_T_in person] Processing in person	[5][(1)]			[7][(2)]		[6][(3)]	
[S_T_remote] Remote processing	[3][(4)]			[7][(5)]		[6][(6)]	
[D_exp] Current files		[5][(7)]	[6][(8)]		[5][(9)]		[5][(10)]

[58] The valuation of each asset is given in each security dimension.
Chapter “4, Valuation criteria” in the “Catalogue of Elements” has been used as the evaluation criterion.
The list in Chapter “3, Valuation dimensions” in the “Catalogue of Elements” has been used for the security dimensions.

Using:

- the security dimensions described in chapter 3 of the “Elements catalogue”.
- The levels and valuation criteria described in chapter 4 of the “Elements catalogue”.

Especially, the levels have been assigned for the following reasons (footnotes in the above table):

(1) [5.1] Probably causes the interruption of the organisation’s activities.

(2) [7.3] Probably has a great impact in other organisations.
[5.3] Legal obligations: probably the cause of non-compliance with a law or regulation.

(3) [6.3] Probably seriously breaks the law or regulations protecting personal information.

(4) [3.2] Probably causes the interruption of the organisation’s activities.

(5) [7.3] Probably has a great impact in other organisations.
[6.2] Probably seriously affects a group of individuals.
[5.3] Legal obligations: probably the cause of non-compliance with a law or regulation.

(6) [6.3] Probably seriously breaks the law or regulations protecting personal information.

(7) [5.2] Probably causes a certain impact in other organisations.

(8) [6.3] Probably seriously breaks the law or regulations protecting personal information.

(9) [5.3] Legal obligations: probably the cause of non-compliance with a law or regulation.

(10) [5.3] Legal obligations: probably the cause of non-compliance with a law or regulation.

When this valuation is propagated through the dependencies tree[59], the following table of accumulated value is provided for each of the assets in the system (the value itself shown on a white background and the accumulated value on a coloured background):

	Security dimensions						
Asset	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
[S_T_in person] Processing in person	[5]			[7]		[6]	
[S_T_remote] Remote processing	[3]			[7]		[6]	
[D_exp] Current files	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[email] E-mail	[5]			[7]		[6]	
[archive] Central historical archive	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[SW_exp] Processing files	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[PC] Working positions	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[SRV] Server	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[firewall] Firewall	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[LAN] Local network	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[ADSL] Internet connection	[5]	[5]	[6]	[7]	[5]	[6]	[5]

This is when the organisation’s “Value model” [60] is obtained.

[59] See “Guide to techniques” section “2.2.1. Qualitative model”.

[60] See “Appendix 4.1. Value model” in the “Catalogue of Elements”.

7.2.4. Activity A2.2: Characterisation of threats

It is difficult, even impossible, to be precise about what would occur if no safeguard were in place. Therefore, it is used a standard, typical, qualification of the potential threats, taking into consideration the type of the asset and the value it accumulates.

All considerations made, the following table[61] shows the potential threats on the data files.

		dimensions of security						
asset / threat	frequency	D	I	C	A_S	A_D	T_S	T_D
[D_exp] Current files		50%	50%	100%	100%	100%	100%	100%
[E.1] Users' errors	10	10%	10%					
[E.2] Administrator errors	1	20%	20%	10%	10%	10%	20%	20%
[E.3] Monitoring errors	1						50%	50%
[E.4] Configuration errors	0,5	50%	10%	10%	50%	50%	50%	50%
[E.14] Information leakage	1			1%				
[E.15] Information alteration	10		1%					
[E.16] Insertion of faulty information	100		1%					
[E.17] Information degradation	10		1%					
[E.18] Destruction of information	10	1%						
[E.19] Disclosure of information	1			10%				
[A.4] Manipulation of the configuration	0,1	50%	10%	50%	100%	100%	100%	100%
[A.11] Unauthorised access	100		10%	50%	50%			
[A.14] Evesdropping	10			50%				
[A.15] Alteration of information	10		50%					
[A.16] Entry of false information	20		50%					
[A.17] Corruption of information	10		50%					
[A.18] Destruction of information	10	50%						
[A.19] Disclosure of information	10			100%				

Notice that there is a difference between the user's perception (described in the above paragraphs) and the potential threats in the system. This difference is due to the existence of safeguards, which will be taken into account below.

The organisation's "Risk map" [62] is obtained at this point.

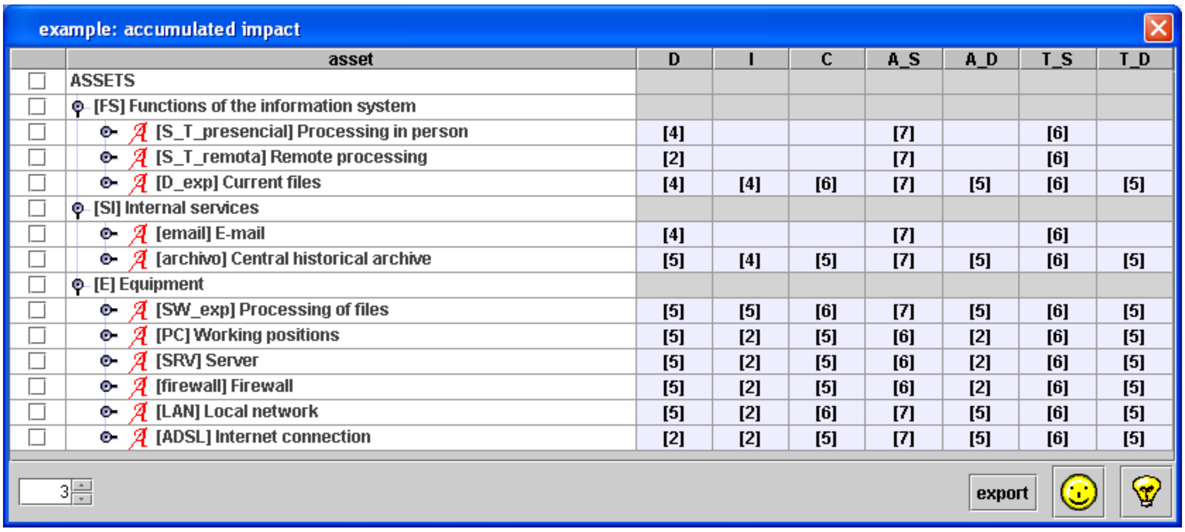
7.2.5. Activity A2.4: Estimate of impact and risk

While still not considering the safeguards, the following table estimates the accumulated impact and risk to the assets.

[61] The first column shows the potential threats on the asset. The second contains the frequency of occurrence expressed as an annual rate (incidents per year). The other columns contain the degradation of the asset expressed as a percentage of its value. There is one column per security dimension (see "Catalogue of Elements", chapter "3, Valuation dimensions").

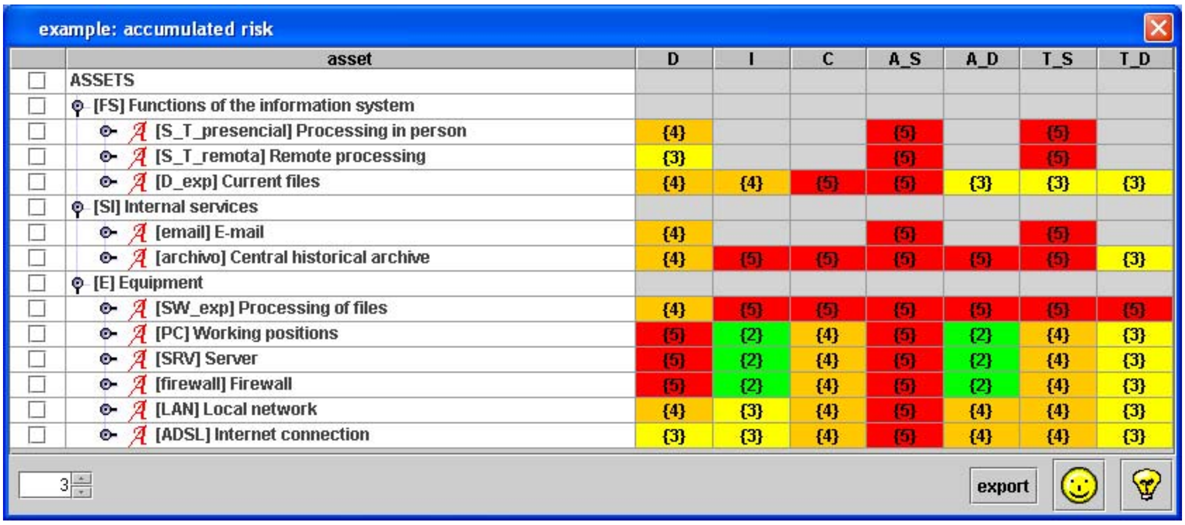
[62] See Appendix 4.2. "Risk map" in the "Catalogue of Elements".

Accumulated impact[63]



☐	asset	D	I	C	A_S	A_D	T_S	T_D
☐	ASSETS							
☐	[FS] Functions of the information system							
☐	[S_T_presencial] Processing in person	[4]			[7]		[6]	
☐	[S_T_remota] Remote processing	[2]			[7]		[6]	
☐	[D_exp] Current files	[4]	[4]	[6]	[7]	[5]	[6]	[5]
☐	[SI] Internal services							
☐	[email] E-mail	[4]			[7]		[6]	
☐	[archivo] Central historical archive	[5]	[4]	[5]	[7]	[5]	[6]	[5]
☐	[E] Equipment							
☐	[SW_exp] Processing of files	[5]	[5]	[6]	[7]	[5]	[6]	[5]
☐	[PC] Working positions	[5]	[2]	[5]	[6]	[2]	[6]	[5]
☐	[SRV] Server	[5]	[2]	[5]	[6]	[2]	[6]	[5]
☐	[firewall] Firewall	[5]	[2]	[5]	[6]	[2]	[6]	[5]
☐	[LAN] Local network	[5]	[2]	[6]	[7]	[5]	[6]	[5]
☐	[ADSL] Internet connection	[2]	[2]	[5]	[7]	[5]	[6]	[5]

Accumulated risk[64]

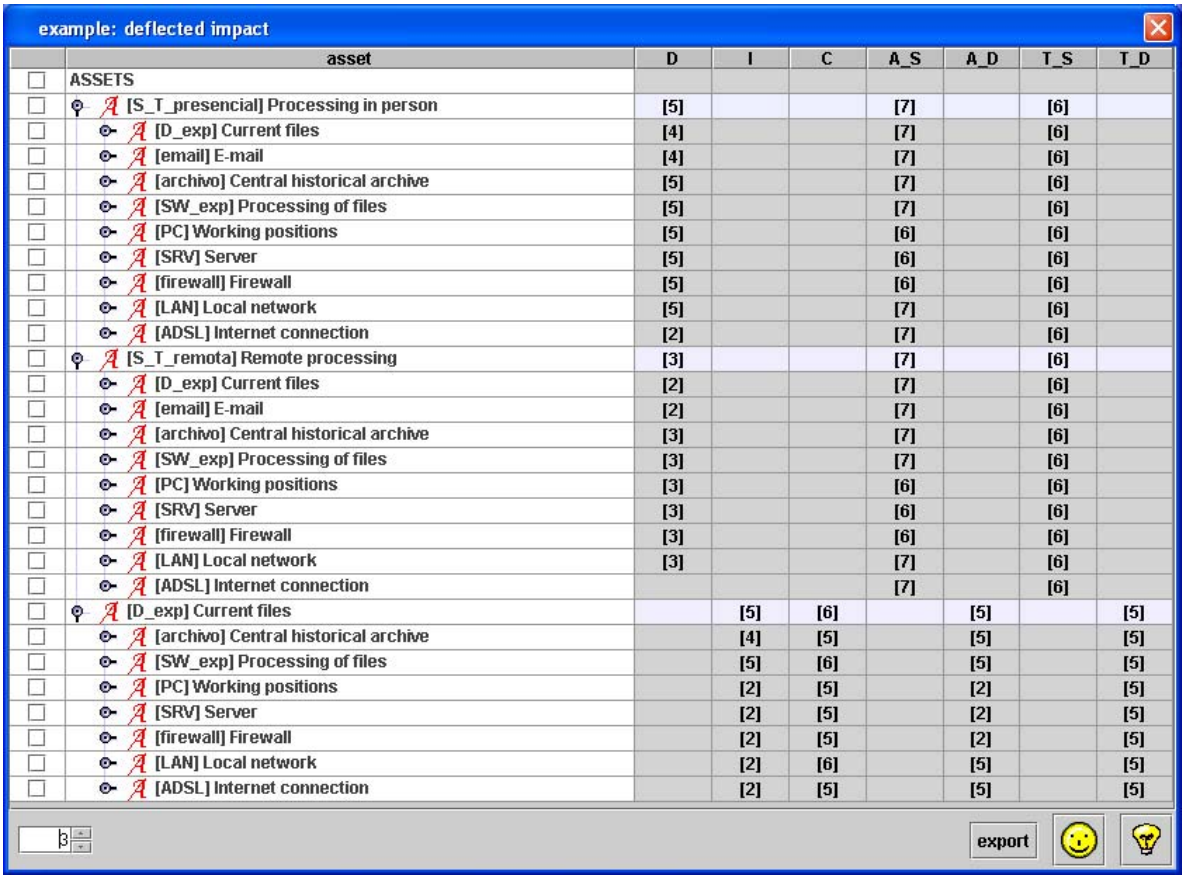


☐	asset	D	I	C	A_S	A_D	T_S	T_D
☐	ASSETS							
☐	[FS] Functions of the information system							
☐	[S_T_presencial] Processing in person	{4}			{5}		{5}	
☐	[S_T_remota] Remote processing	{3}			{5}		{5}	
☐	[D_exp] Current files	{4}	{4}	{5}	{5}	{3}	{3}	{3}
☐	[SI] Internal services							
☐	[email] E-mail	{4}			{5}		{5}	
☐	[archivo] Central historical archive	{4}	{5}	{5}	{5}	{5}	{5}	{3}
☐	[E] Equipment							
☐	[SW_exp] Processing of files	{4}	{5}	{5}	{5}	{5}	{5}	{5}
☐	[PC] Working positions	{5}	{2}	{4}	{5}	{2}	{4}	{3}
☐	[SRV] Server	{5}	{2}	{4}	{5}	{2}	{4}	{3}
☐	[firewall] Firewall	{5}	{2}	{4}	{5}	{2}	{4}	{3}
☐	[LAN] Local network	{4}	{3}	{4}	{5}	{4}	{4}	{3}
☐	[ADSL] Internet connection	{3}	{3}	{4}	{5}	{4}	{4}	{3}

[63] To estimate the accumulated impact, see section "2.1.3. Step 4: Determination of the impact". It takes into account the accumulated value on the asset (on each security dimension) and the degradation caused by the threat. See also section "2.2.1. Qualitative model" of the "Techniques Guide".

[64] To estimate the accumulated risk, see section "2.1.4. Step 5: Determination of the risk". It takes into account the accumulated impact, and the estimated frequency of occurrence of the threat. See also section "2.1. Tabular analysis" of the "Techniques Guide", where risk is classified in a range from {0} (neglible) to {5} (very high).

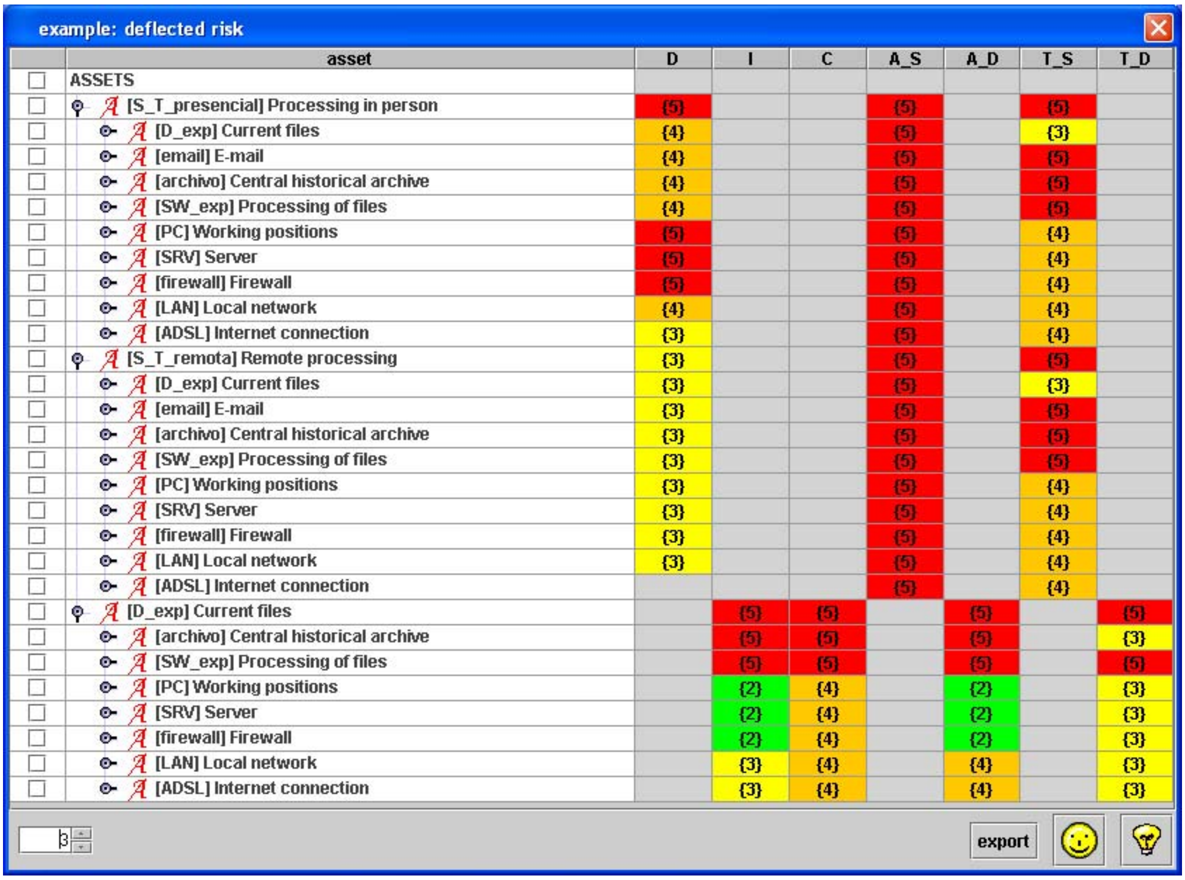
Deflected impact[65]



	asset	D	I	C	A_S	A_D	T_S	T_D
☐	ASSETS							
☐	[S_T_presencial] Processing in person	[5]			[7]		[6]	
☐	[D_exp] Current files	[4]			[7]		[6]	
☐	[email] E-mail	[4]			[7]		[6]	
☐	[archivo] Central historical archive	[5]			[7]		[6]	
☐	[SW_exp] Processing of files	[5]			[7]		[6]	
☐	[PC] Working positions	[5]			[6]		[6]	
☐	[SRV] Server	[5]			[6]		[6]	
☐	[firewall] Firewall	[5]			[6]		[6]	
☐	[LAN] Local network	[5]			[7]		[6]	
☐	[ADSL] Internet connection	[2]			[7]		[6]	
☐	[S_T_remota] Remote processing	[3]			[7]		[6]	
☐	[D_exp] Current files	[2]			[7]		[6]	
☐	[email] E-mail	[2]			[7]		[6]	
☐	[archivo] Central historical archive	[3]			[7]		[6]	
☐	[SW_exp] Processing of files	[3]			[7]		[6]	
☐	[PC] Working positions	[3]			[6]		[6]	
☐	[SRV] Server	[3]			[6]		[6]	
☐	[firewall] Firewall	[3]			[6]		[6]	
☐	[LAN] Local network	[3]			[7]		[6]	
☐	[ADSL] Internet connection				[7]		[6]	
☐	[D_exp] Current files		[5]	[6]		[5]		[5]
☐	[archivo] Central historical archive		[4]	[5]		[5]		[5]
☐	[SW_exp] Processing of files		[5]	[6]		[5]		[5]
☐	[PC] Working positions		[2]	[5]		[2]		[5]
☐	[SRV] Server		[2]	[5]		[2]		[5]
☐	[firewall] Firewall		[2]	[5]		[2]		[5]
☐	[LAN] Local network		[2]	[6]		[5]		[5]
☐	[ADSL] Internet connection		[2]	[5]		[5]		[5]

[65] To estimate the deflected impact, see section “2.1.4. Estimation of the impact”. It takes into account the own value of the upper asset, and the degradation caused by the threat on the lower asset.

Deflected risk[66]



example: deflected risk

	asset	D	I	C	A_S	A_D	T_S	T_D
□	ASSETS							
□	[S_T_presencial] Processing in person	{5}			{5}		{5}	
□	[D_exp] Current files	{4}			{5}		{3}	
□	[email] E-mail	{4}			{5}		{5}	
□	[archivo] Central historical archive	{4}			{5}		{5}	
□	[SW_exp] Processing of files	{4}			{5}		{5}	
□	[PC] Working positions	{5}			{5}		{4}	
□	[SRV] Server	{5}			{5}		{4}	
□	[firewall] Firewall	{5}			{5}		{4}	
□	[LAN] Local network	{4}			{5}		{4}	
□	[ADSL] Internet connection	{3}			{5}		{4}	
□	[S_T_remota] Remote processing	{3}			{5}		{5}	
□	[D_exp] Current files	{3}			{5}		{3}	
□	[email] E-mail	{3}			{5}		{5}	
□	[archivo] Central historical archive	{3}			{5}		{5}	
□	[SW_exp] Processing of files	{3}			{5}		{5}	
□	[PC] Working positions	{3}			{5}		{4}	
□	[SRV] Server	{3}			{5}		{4}	
□	[firewall] Firewall	{3}			{5}		{4}	
□	[LAN] Local network	{3}			{5}		{4}	
□	[ADSL] Internet connection				{5}		{4}	
□	[D_exp] Current files		{5}	{5}		{5}		{5}
□	[archivo] Central historical archive		{5}	{5}		{5}		{3}
□	[SW_exp] Processing of files		{5}	{5}		{5}		{5}
□	[PC] Working positions		{2}	{4}		{2}		{3}
□	[SRV] Server		{2}	{4}		{2}		{3}
□	[firewall] Firewall		{2}	{4}		{2}		{3}
□	[LAN] Local network		{3}	{4}		{4}		{3}
□	[ADSL] Internet connection		{3}	{4}		{4}		{3}

7.2.6. Activity A2.3: Characterisation of safeguards

When evaluating the state of security of the unit being studied, it is necessary to investigate a series of general aspects and a series of specific aspects for each asset. This investigation involves taking into account the nature of the assets and their value and the threats to which they are exposed.

Generally speaking, it is necessary to find out:

- How the security is organised: person responsible, decision-making, external contacts, etc.
- If the roles of the personnel, associated with access privileges, are identified.
- If there is an effective segregation of tasks.
- If there is a documented security policy that is periodically revised.
- How incidents are managed.
- How the activity logs are managed.
- If there is a contingency plan: management of emergencies, continuity and recovery.

With regard to the services provided by the organisation, it is necessary to find out:

- If there are standards and procedures for use that are known and used.
- If there is capacity planning.
- If there are mechanisms to prevent repudiation.

[66] To estimate the deflected risk, see section “2.1.4. Estimation of the risk”. It takes into account the deflected impact, and the estimated frequency of occurrence of the threat on the lower asset.

- If there are mechanisms to prevent service denial attacks.
- How the users are managed.
- What trace is left of what is done.

With regard to the data handled by the organisation, it is necessary to find out:

- If there is an inventory of files with the identification of the person responsible.
- If there are standards and procedures for use that are known and used.
- If back-up copies are made and with what quality.
- If there are mechanisms that guarantee secrecy.
- If mechanisms are planned to guarantee integrity.
- If access control mechanisms are planned.

With regard to the applications in use, it is necessary to find out:

- How their maintenance is managed.
- How their configuration is controlled, especially of users and access rights.
- If the code is inspected, especially for rear access doors.

With regard to the e-mail service, it is necessary to find out:

- If there are standards and procedures for use that are known and used.
- How the users are managed.
- How the contents of the messages and attached files are controlled.
  - From the point of view of information leaks.
  - From the point of view of the injection of harmful programs (for example, viruses).
  - From the point of view of the authenticity of their origin.
- How the availability of the service is assured.

With regard to the archive service, it is necessary to find out:

- If there are standards and procedures for use that are known and used.
- How those who access its use are controlled.
- How the secrecy of the data it carries is assured.
- How its availability is assured.

With regard to the computer equipment, it is necessary to find out:

- If there are standards and procedures for use that are known and used.
- How its maintenance is managed.
- How its configuration is controlled, especially of users and access rights.
- How its availability is assured.

With regard to the communications, it is necessary to find out:

- If there are standards and procedures for use that are known and used.
- How those who access its use are controlled.
- How the secrecy of the data it carries is assured.
- How its availability is assured.

The reader must remember that this is only an example that does not try to be exhaustive. The most important aspects have been referenced, not all of them. The absence of an analysis of the physical installations and personnel is especially noteworthy; these have been left out to keep the example small.

Investigation shows that:

- There is a security policy, inherited from the unit's head office. Because it is a small unit, there is a single person responsible for security who reports directly to management and is the contact for other organisations. There is also a local incident escalation procedure that can cause escalation beyond the unit itself.
- The central server hosts a table to control the access privileges of each user, especially differentiating the administrative capability to handle files during their processing. All activity is recorded in a file to which only the operator has access and which is sent daily to the central archive.
- Procedures for working with the systems are not in writing. The Web applications themselves are left to adapt the activities that can be carried out at any time depending on the status of the formality under way and the user's privileges. All the actions of the personnel on the Web services are logged. For manual processing, there is a series of forms with instructions on when they should be used, what data must be provided and how to handle them.
- One person in the unit acts as the operator, taking care of all the installation, configuration and incident solving tasks. This person has written procedures for the routine activities but must improvise in atypical situations, for which he has the help of the technical support in the head office.
- There is no contingency plan.
- There are maintenance contracts with the suppliers of the equipment and of the basic programs: operating system, office computing, e-mail and Web servers.
- Internal users are administrated by the operator who requires written requests for entering new users, deleting users and making changes. This request must be signed by the manager.
- External users are entered personally by giving their identity card number. They must attend in person to obtain their password the first time. Once they are registered, there is no tracking of the accounts, which last indefinitely.
- Both internal and external users are identified by a user name and a password. They all receive brief instructions on how to choose passwords but there is no check to see that these are complied with or that the passwords are changed regularly.
- An audit was recently carried out of the personal data and this was easily passed in all its aspects.
- The data from the central archive are considered to be correct. The data entered by the public must be validated by the unit's personnel. The data entered by the internal users must be validated by a second user. Normally they are entered by one person and validated by the person signing the progress of the file.
- The formality files application is supplied by the head office and is considered to be of "sufficient quality".
- An anti-virus system has been installed and a 24x7 maintenance service contracted through the head office with a response time of less than one day.
- The mail service is centralised in the server with access by internal users through a Web interface. Systematically, all attachments in outgoing e-mails are removed and incoming attachments are analysed with the anti-virus system.
- The central archive service is provided externally and is considered to be of "sufficient quality". A more detailed analysis must investigate the provision of this service.
- Internet communications take place via a standard ADSL contract, without a study of requirements having been made and without any contractual clauses regarding quality of service or increase of capacity.
- The connection to the central archive takes place over the Internet, using a private virtual end-to-end network. This network is configured and maintained from the central archive with

no local configuration capacity. It is considered to be of “sufficient quality”.

The organisation’s “Safeguards evaluation” [67] is obtained at this point.

Deficiencies found

The following deficiencies were found after the investigations:

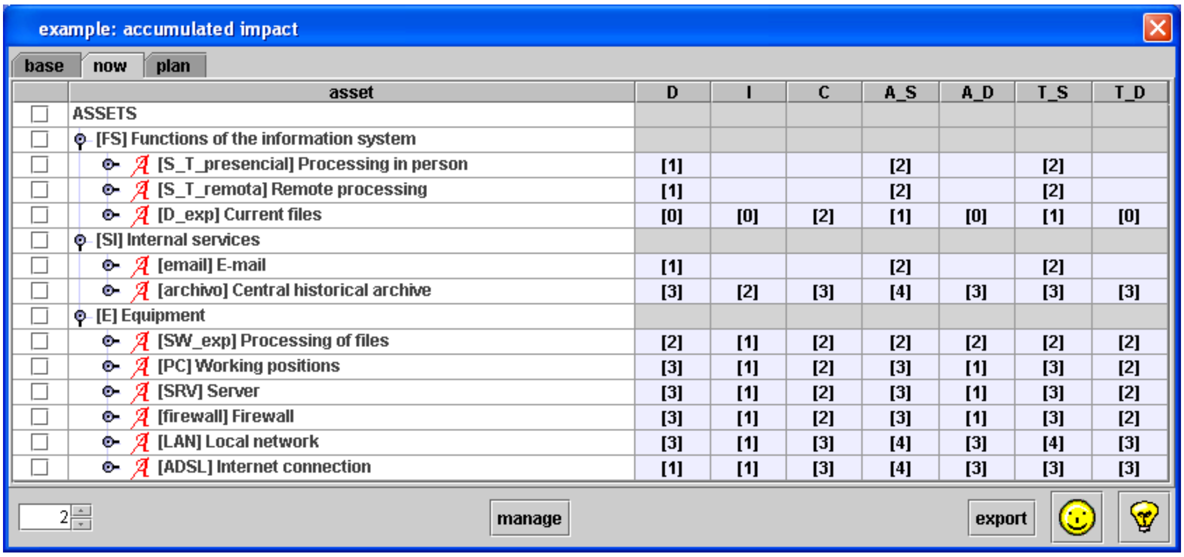
- The segregation of tasks is suitable except in the case of the systems administrator who has a wide access capability to all the systems, installations and configurations.
- There must be a contingency plan: emergencies management, continuity plan and recovery plan.
- There must be written procedures for all the ordinary tasks and for foreseeable incidents, including all those that have happened in the past.
- A study must be carried out on the use of the ADSL connection and its development in order to be able to plan an increase of capacity. It is also necessary to establish a service quality agreement with the supplier that includes an alternative communications channel in the case of a drop-out.
- Mechanisms must be established to detect and react to a service denial attack.
- The accounts of the external users must be monitored, at least to detect long periods without activity, penetration attempts and anomalous behaviour in general.
- The use of passwords as an authentication mechanism is considered “weak”; the use of encrypted identification cards is recommended.

The organisation’s “Deficiencies report” [68] is obtained at this point.

7.2.7. Activity A2.4: Estimate of the risk status

Once the “Value model”, the “Risk map” and the “Safeguards evaluation” are known, the impact and risk indicators can be calculated, both accumulated (on the lower assets) and deflected (on the higher assets).

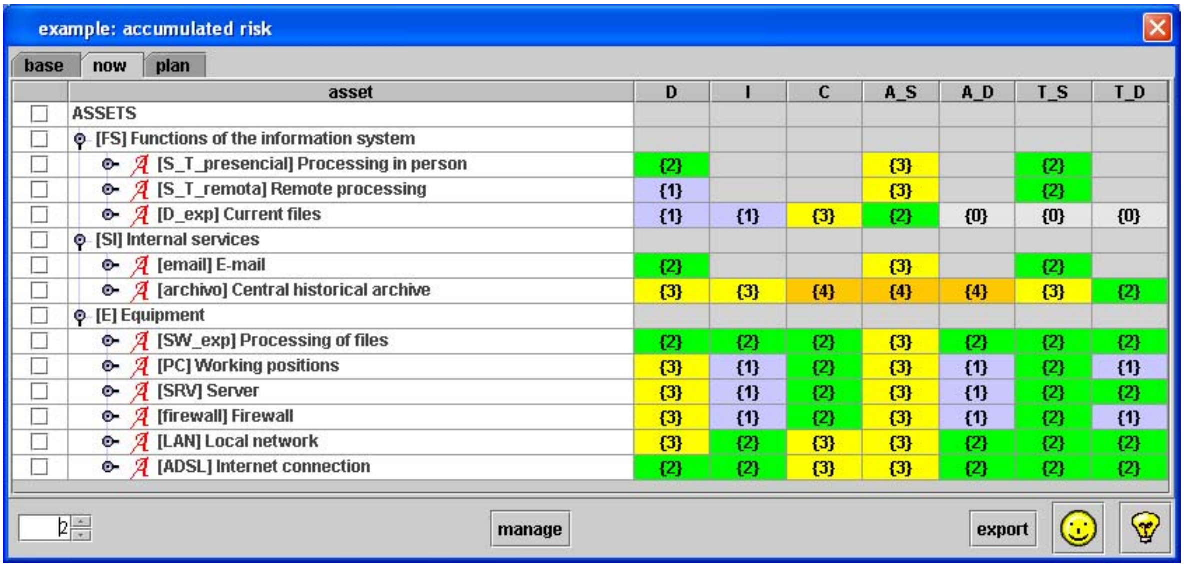
Accumulated residual impact



	asset	D	I	C	A_S	A_D	T_S	T_D
□	ASSETS							
□	[FS] Functions of the information system							
□	[S_T_presencial] Processing in person	[1]			[2]		[2]	
□	[S_T_remota] Remote processing	[1]			[2]		[2]	
□	[D_exp] Current files	[0]	[0]	[2]	[1]	[0]	[1]	[0]
□	[SI] Internal services							
□	[email] E-mail	[1]			[2]		[2]	
□	[archivo] Central historical archive	[3]	[2]	[3]	[4]	[3]	[3]	[3]
□	[E] Equipment							
□	[SW_exp] Processing of files	[2]	[1]	[2]	[2]	[2]	[2]	[2]
□	[PC] Working positions	[3]	[1]	[2]	[3]	[1]	[3]	[2]
□	[SRV] Server	[3]	[1]	[2]	[3]	[1]	[3]	[2]
□	[firewall] Firewall	[3]	[1]	[2]	[3]	[1]	[3]	[2]
□	[LAN] Local network	[3]	[1]	[3]	[4]	[3]	[4]	[3]
□	[ADSL] Internet connection	[1]	[1]	[3]	[4]	[3]	[3]	[3]

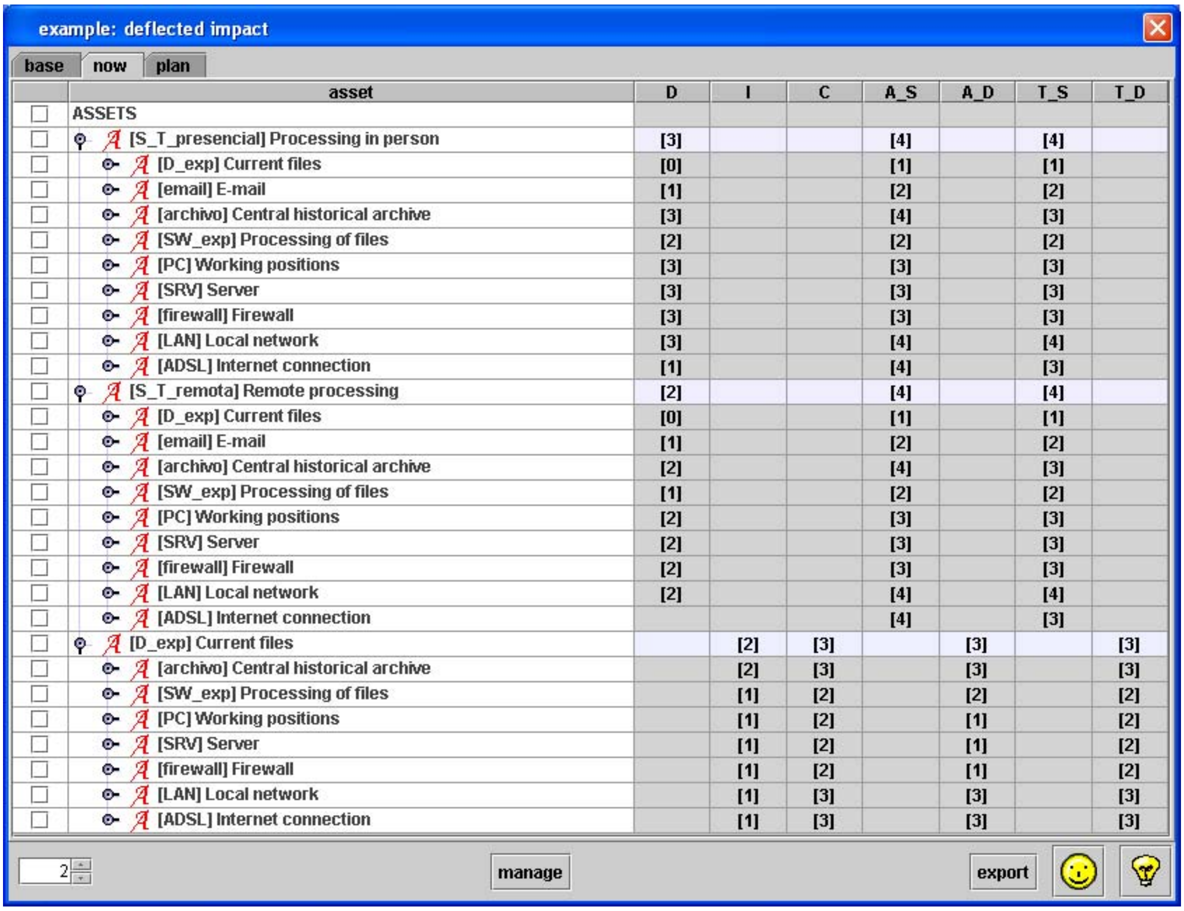
[67] See “Appendix 4.3, Evaluation of safeguards” in the “Catalogue of Elements”.
[68] See “Appendix 4.5, Deficiencies report” in the “Catalogue of Elements”.

Residual risk



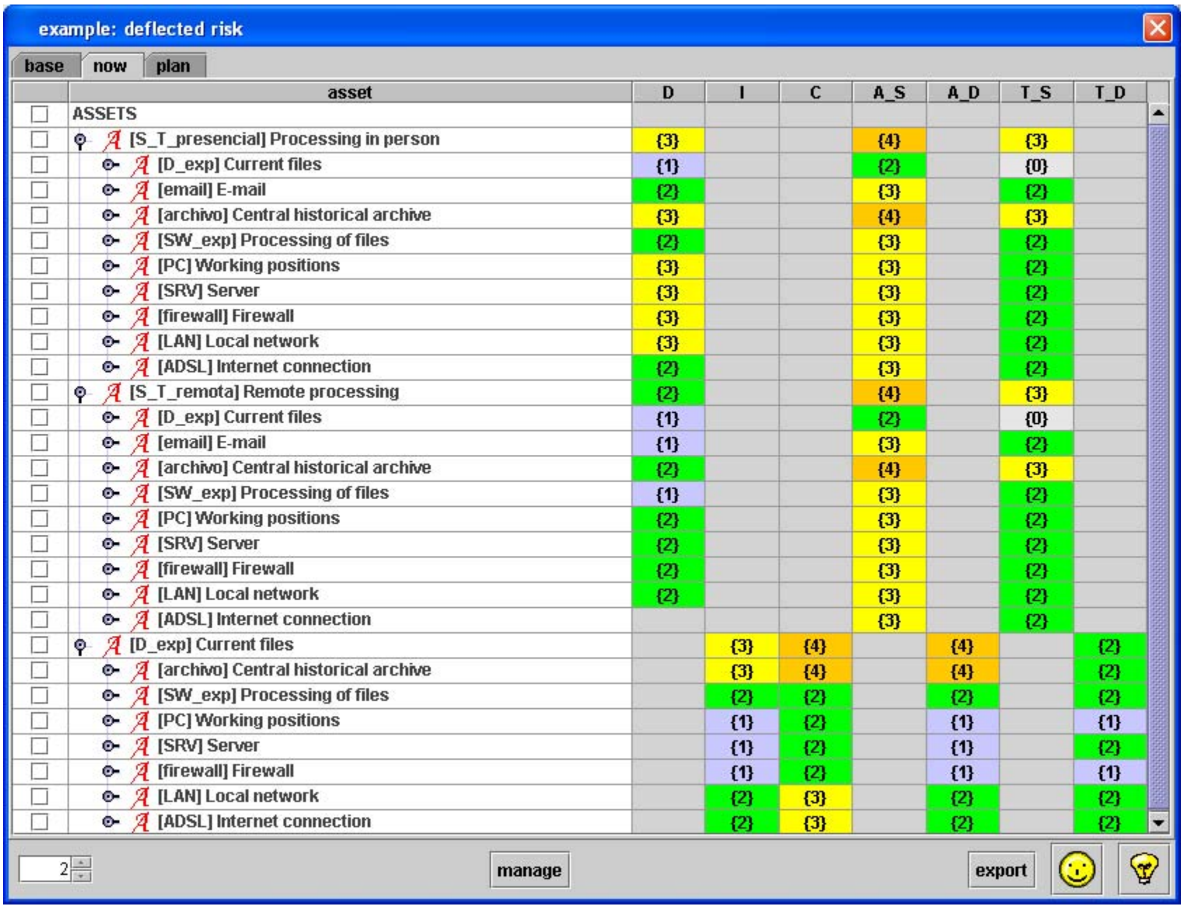
	asset	D	I	C	A_S	A_D	T_S	T_D
□	ASSETS							
□	[FS] Functions of the information system							
□	[S_T_presencial] Processing in person	{2}			{3}		{2}	
□	[S_T_remota] Remote processing	{1}			{3}		{2}	
□	[D_exp] Current files	{1}	{1}	{3}	{2}	{0}	{0}	{0}
□	[SI] Internal services							
□	[email] E-mail	{2}			{3}		{2}	
□	[archivo] Central historical archive	{3}	{3}	{4}	{4}	{4}	{3}	{2}
□	[E] Equipment							
□	[SW_exp] Processing of files	{2}	{2}	{2}	{3}	{2}	{2}	{2}
□	[PC] Working positions	{3}	{1}	{2}	{3}	{1}	{2}	{1}
□	[SRV] Server	{3}	{1}	{2}	{3}	{1}	{2}	{2}
□	[firewall] Firewall	{3}	{1}	{2}	{3}	{1}	{2}	{1}
□	[LAN] Local network	{3}	{2}	{3}	{3}	{2}	{2}	{2}
□	[ADSL] Internet connection	{2}	{2}	{3}	{3}	{2}	{2}	{2}

Deflected residual impact



	asset	D	I	C	A_S	A_D	T_S	T_D
□	ASSETS							
□	[S_T_presencial] Processing in person	[3]			[4]		[4]	
□	[D_exp] Current files	[0]			[1]		[1]	
□	[email] E-mail	[1]			[2]		[2]	
□	[archivo] Central historical archive	[3]			[4]		[3]	
□	[SW_exp] Processing of files	[2]			[2]		[2]	
□	[PC] Working positions	[3]			[3]		[3]	
□	[SRV] Server	[3]			[3]		[3]	
□	[firewall] Firewall	[3]			[3]		[3]	
□	[LAN] Local network	[3]			[4]		[4]	
□	[ADSL] Internet connection	[1]			[4]		[3]	
□	[S_T_remota] Remote processing	[2]			[4]		[4]	
□	[D_exp] Current files	[0]			[1]		[1]	
□	[email] E-mail	[1]			[2]		[2]	
□	[archivo] Central historical archive	[2]			[4]		[3]	
□	[SW_exp] Processing of files	[1]			[2]		[2]	
□	[PC] Working positions	[2]			[3]		[3]	
□	[SRV] Server	[2]			[3]		[3]	
□	[firewall] Firewall	[2]			[3]		[3]	
□	[LAN] Local network	[2]			[4]		[4]	
□	[ADSL] Internet connection				[4]		[3]	
□	[D_exp] Current files		[2]	[3]		[3]		[3]
□	[archivo] Central historical archive		[2]	[3]		[3]		[3]
□	[SW_exp] Processing of files		[1]	[2]		[2]		[2]
□	[PC] Working positions		[1]	[2]		[1]		[2]
□	[SRV] Server		[1]	[2]		[1]		[2]
□	[firewall] Firewall		[1]	[2]		[1]		[2]
□	[LAN] Local network		[1]	[3]		[3]		[3]
□	[ADSL] Internet connection		[1]	[3]		[3]		[3]

Residual deflected risk



	asset	D	I	C	A_S	A_D	T_S	T_D
□	ASSETS							
□	[S_T_presencial] Processing in person	{3}			{4}		{3}	
□	[D_exp] Current files	{1}			{2}		{0}	
□	[email] E-mail	{2}			{3}		{2}	
□	[archivo] Central historical archive	{3}			{4}		{3}	
□	[SW_exp] Processing of files	{2}			{3}		{2}	
□	[PC] Working positions	{3}			{3}		{2}	
□	[SRV] Server	{3}			{3}		{2}	
□	[firewall] Firewall	{3}			{3}		{2}	
□	[LAN] Local network	{3}			{3}		{2}	
□	[ADSL] Internet connection	{2}			{3}		{2}	
□	[S_T_remota] Remote processing	{2}			{4}		{3}	
□	[D_exp] Current files	{1}			{2}		{0}	
□	[email] E-mail	{1}			{3}		{2}	
□	[archivo] Central historical archive	{2}			{4}		{3}	
□	[SW_exp] Processing of files	{1}			{3}		{2}	
□	[PC] Working positions	{2}			{3}		{2}	
□	[SRV] Server	{2}			{3}		{2}	
□	[firewall] Firewall	{2}			{3}		{2}	
□	[LAN] Local network	{2}			{3}		{2}	
□	[ADSL] Internet connection				{3}		{2}	
□	[D_exp] Current files		{3}	{4}		{4}		{2}
□	[archivo] Central historical archive		{3}	{4}		{4}		{2}
□	[SW_exp] Processing of files		{2}	{2}		{2}		{2}
□	[PC] Working positions		{1}	{2}		{1}		{1}
□	[SRV] Server		{1}	{2}		{1}		{2}
□	[firewall] Firewall		{1}	{2}		{1}		{1}
□	[LAN] Local network		{2}	{3}		{2}		{2}
□	[ADSL] Internet connection		{2}	{3}		{2}		{2}

The organisation's "Risk status" [69] is obtained at this point. This "Risk status" is documented in the "Safeguards evaluation" report that contains the current security deployment and in the "Deficiencies report" [70] which contains the weaknesses discovered.

7.3. Process P3: Risk Management

7.3.1. Activity A3.1: Decision making

Given the residual risk indicators and the deficiencies in the unit, management decides to classify the security programs to be carried out into the following levels:

Urgent
P1: Develop a contingency plan. P2: Monitor and manage the accounts of external users.
Important considerations
P3.1: Document all the working procedures, revising the current ones and adding those that are lacking. P3.2: Segregate the functions of the systems administrator.
Matters for future consideration
• Use of identity cards. • Relationship with the communications provider to guarantee quality of service. • Contracting of an alternative communications service. • Measures against denial of service attacks.

[69] See "Appendix 4.4., Risk status" in the "Catalogue of Elements".

[70] See "Appendix 4.5., Deficiencies report" in the "Catalogue of Elements".

7.3.2. Activity A3.2: Security plan

All the above considerations must be contained in a “Security plan” [71] that organises the activities in a planned and managed way.

The development of the contingency plan (programme P1) becomes a specific project for which:

1. This year the project’s costs will be estimated and a call for tenders requested, to be completed with the awarding to an external contractor.
2. Depending on the winning tender, funds will be set aside next year to prepare a plan. This preparation will include all the administrative tasks (dimensioning, selection of solutions, procedures, etc) except for possible building work or contracting of external continuity services, which will be the subject of future tenders.

For the accounts monitoring (programme P2), a project is launched to develop an accounts management system that includes the detection of intrusions and the sounding of alarms. It is estimated that this project can be launched immediately and that it will last for one year.

To document all the procedures (programme P3.1), the head office’s current consulting contract will be enlarged. In this enlargement, external consultants will gather the relevant information and complete the current manuals. This task will not be carried out until next year. In preparing procedures, the specific tasks of an operator (local) will be defined together with those of an administrator (remote) in order to attain the objective of programme P3.2. Negotiations will be held with the central archive on the availability of a centralised administration service, leaving just the operating functions at the local level.

Finally, the head office will be consulted about the use of corporate identity cards and even electronic identity cards as means that could be used in the future to improve user authentication. A study will be carried out next year on the changes required to incorporate these mechanisms for both internal and external users. Part of the study will be a detailed undertaking plan, although this will not be carried out for two years.

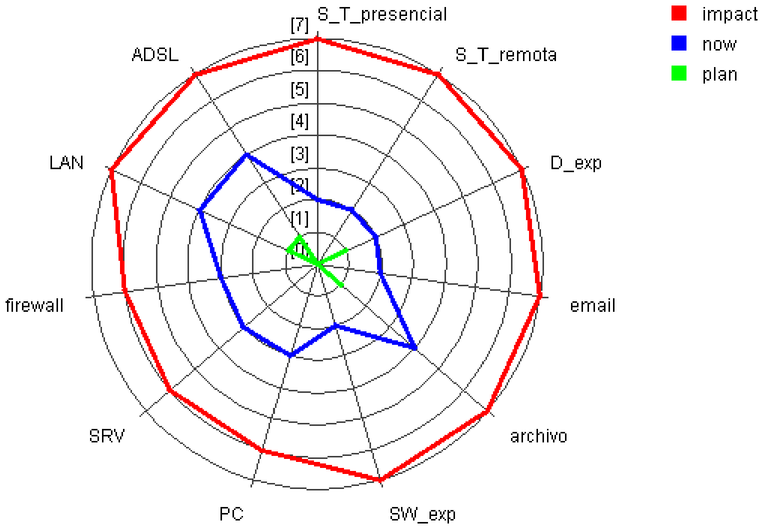
[71] See “Appendix 4.6, Security plan” in the “Catalogue of Elements”.

7.3.3. Evolution of the impact and risk indicators

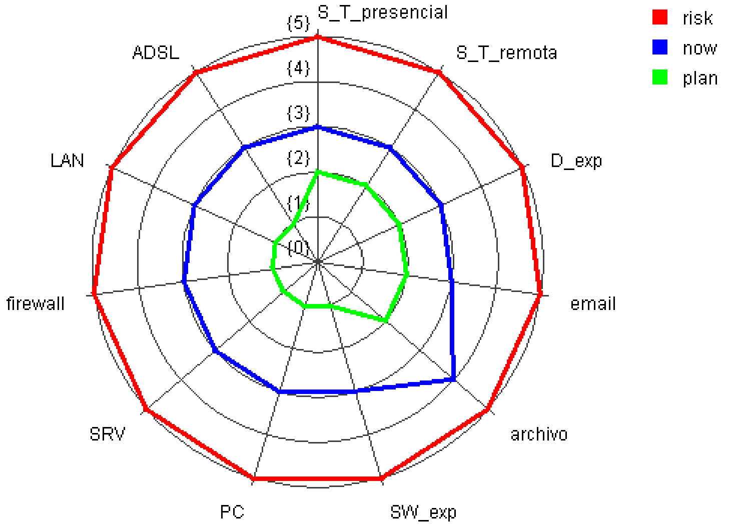
The following figures show the evolution of the impact and risk indicators, both accumulated and deflected, in three moments of the management of the information being studied:

- Without safeguards.
- At the present time.
- After carrying out programmes P1, P2 and P3 of the security plan.

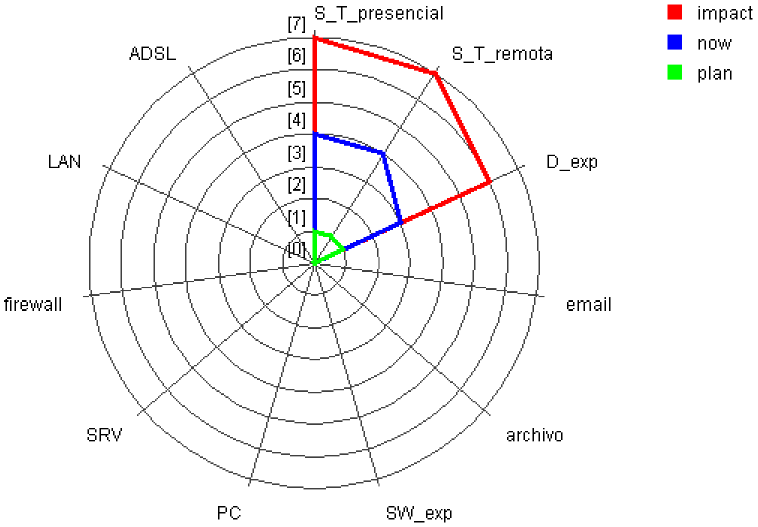
Residual accumulated impact



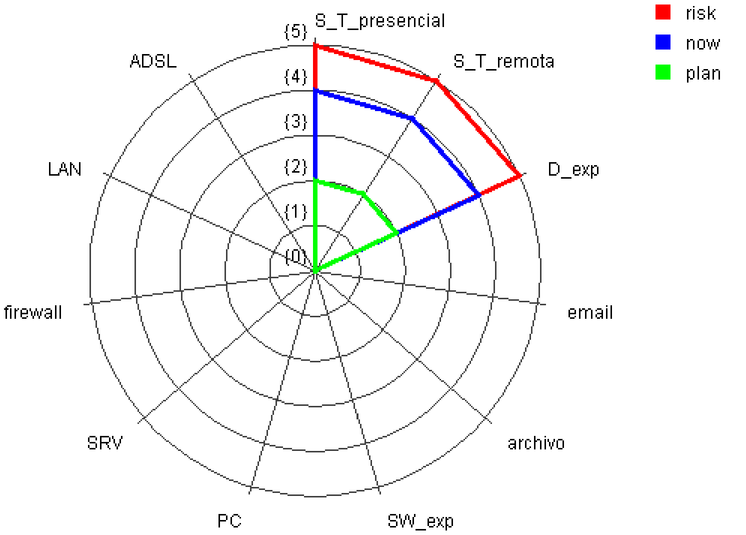
Residual accumulated risk



Residual deflected impact

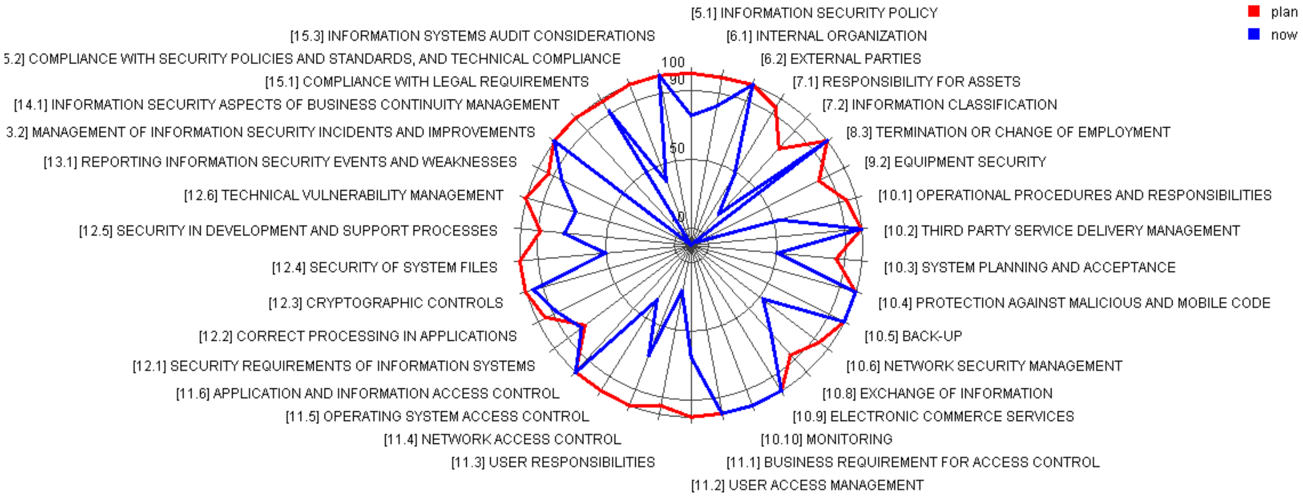


Residual deflected risk



7.3.4. Classification according to ISO/IEC 17799:2005

The international standard 17799 stands for “Code of Practice for Information Security Management”. It defines a number of security controls relevant for the adequate management of security (ISMS – Information Security Management System). The following graph shows the satisfaction of those controls, based on the information collected regarding safeguards:


[5.1] INFORMATION SECURITY POLICY
[6.1] INTERNAL ORGANIZATION
[6.2] EXTERNAL PARTIES
[7.1] RESPONSIBILITY FOR ASSETS
[7.2] INFORMATION CLASSIFICATION
[8.3] TERMINATION OR CHANGE OF EMPLOYMENT
[9.2] EQUIPMENT SECURITY
[10.1] OPERATIONAL PROCEDURES AND RESPONSIBILITIES
[10.2] THIRD PARTY SERVICE DELIVERY MANAGEMENT
[10.3] SYSTEM PLANNING AND ACCEPTANCE
[10.4] PROTECTION AGAINST MALICIOUS AND MOBILE CODE
[10.5] BACK-UP
[10.6] NETWORK SECURITY MANAGEMENT
[10.8] EXCHANGE OF INFORMATION
[10.9] ELECTRONIC COMMERCE SERVICES
[10.10] MONITORING
[11.1] BUSINESS REQUIREMENT FOR ACCESS CONTROL
[11.2] USER ACCESS MANAGEMENT
[11.3] USER RESPONSIBILITIES
[11.4] NETWORK ACCESS CONTROL
[11.5] OPERATING SYSTEM ACCESS CONTROL
[11.6] APPLICATION AND INFORMATION ACCESS CONTROL
[12.1] SECURITY REQUIREMENTS OF INFORMATION SYSTEMS
[12.2] CORRECT PROCESSING IN APPLICATIONS
[12.3] CRYPTOGRAPHIC CONTROLS
[12.4] SECURITY OF SYSTEM FILES
[12.5] SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES
[12.6] TECHNICAL VULNERABILITY MANAGEMENT
[13.1] REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES
3.2] MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS
[14.1] INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT
[15.1] COMPLIANCE WITH LEGAL REQUIREMENTS
5.2] COMPLIANCE WITH SECURITY POLICIES AND STANDARDS, AND TECHNICAL COMPLIANCE
[15.3] INFORMATION SYSTEMS AUDIT CONSIDERATIONS
🟥 plan
🟦 now