MAGERIT – version 3.0
Methodology for Information Systems Risk Analysis and Management

Book I - The Method

GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
SECRETARÍA DE ESTADO DE ADMINISTRACIONES PÚBLICAS
DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA, PROCEDIMIENTOS E IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

TITLE: MAGERIT – version 3.0. Methodology for Information Systems Risk Analysis and Management.
Book I - The Method

Promoted by: Directorate General for Administrative Modernisation, Procedures and Promotion of e-Government

Project team:
Direction:
Miguel A. Amutio, Ministerio de Hacienda y Administraciones Públicas
Javier Candau, Centro Criptológico Nacional, Ministerio de la Presidencia.
Consultant:
José Antonio Mañas, Professor, Universidad Politécnica de Madrid

Digital edition with Adobe Acrobat 5.0
Madrid, July, 2014
Available this publication at: Portal de Administración Electrónica (PAe):
http://administracionelectronica.gob.es/

Published by:
© Ministry of Finance and Public Administration
Technical Secretariat
Information, Documentation and Publications Unit
Publications Center

Edita:
© Ministerio de Hacienda y Administraciones Públicas
Secretaría General Técnica
Subdirección General de Información,
Documentación y Publicaciones
Centro de Publicaciones

Colección: administración electrónica

NIPO: 630-14-162-0

Contents

1. Introduction

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 use of information and communication technologies (ICT) clearly benefits the citizens; but it also entails certain risks that must be sensibly managed with security measures that sustain the trust of service users.

1.1. Good governance

Risk management is a cornerstone in good governance handbooks [ISO 38500], public or private, where it is essential for governance decisions to be based on the knowledge of the risks involved:

> **1.6.12 Proposal**
>
> Compilation of benefits, costs, risks, opportunities, and other factors applicable to decisions to be made. Includes business cases.

Covering risks in general and ICT risks in particular:

> This standard establishes principles for the effective, efficient and acceptable use of IT. Ensuring that their organisations follow these principles will assist directors in balancing risks and encouraging opportunities arising from the use of IT

The need of a balance between risks and opportunities in order to take the best decisions is recurrently stressed.

In short, risk management is critical to good governance of organisations. In particular, the risks derived from the use of information technologies shall be communicated to governing bodies and contextualized in the mission of the organisation.

Being aware of the risks will ensure that systems will work as the Management expects, providing a balanced framework for Governance, Risk Management and Compliance (GRC), three areas that must be integrated and lined up to prevent conflicts, duplication of activities and no-man's lands.

Governing bodies do not only have to manage ICT risks. Moreover, they must not manage ICT risks separately from other risks. While Magerit is specialized in ICT risks, we must be fully aware that it is essential to advise governing bodies of the opportunities and risks derived from information technologies, for them to be included in a comprehensive framework, and to take the best decisions for the organisation.

1.2. Trust

Trust is the strong hope that something will work as expected. Trust is a critical value in any organisation providing services. Public administrations are especially sensitive to trust perceived by society.

On the one hand, we strongly depend on information systems to achieve our objectives; but, on the other hand, their security is a recurring concern. People involved, who often are not technicians, wonder if these systems can be trusted. Trust is undermined with every failure, especially when investments do not translate into absence of incidents. Ideal systems do not fail. But the truth is that we accept to live with failing systems. The issue is not so much the lack of incidents in those systems, but the confidence that they are under control: to know what it might happen and what to do when it happens. The fear of the unknown is the main cause of distrust and, consequently, knowledge brings confidence: to know the risks in order to face and control them.

1 CSAE: Higher Council for Electronic Government (Consejo Superior de Administración Electrónica).
2 MAGERIT: Risk Analysis and Management Methodology for Information Systems.

1.3. Management

Knowing the risks to which work elements are subject, is simply essential to manage them.

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.*

Within the National Security Framework [RD 3/2010], Chapter II, Basic Principles, reads:

> *Article 6. Security management based on risks*
>
> *1. The analysis and management of risks will form an essential part of the security process and must be kept permanently updated.*
>
> *2. Risk management will allow the maintenance of a controlled environment, reducing risks to acceptable levels. Reducing these levels will be achieved by deploying security measures to establish a balance between the nature of the information and the processes, the risks to which the information is exposed and security measures.*

1.4. Magerit

According to ISO 31000 terminology, Magerit responds to what is called "Risk Management Process", section 4.4 ("Implementing Risk Management") within the "Framework for Risk Management". In other words, MAGERIT implements the Risk Management Process within a working framework for governing bodies to make decisions taking into account the risks derived from the use of information technologies.

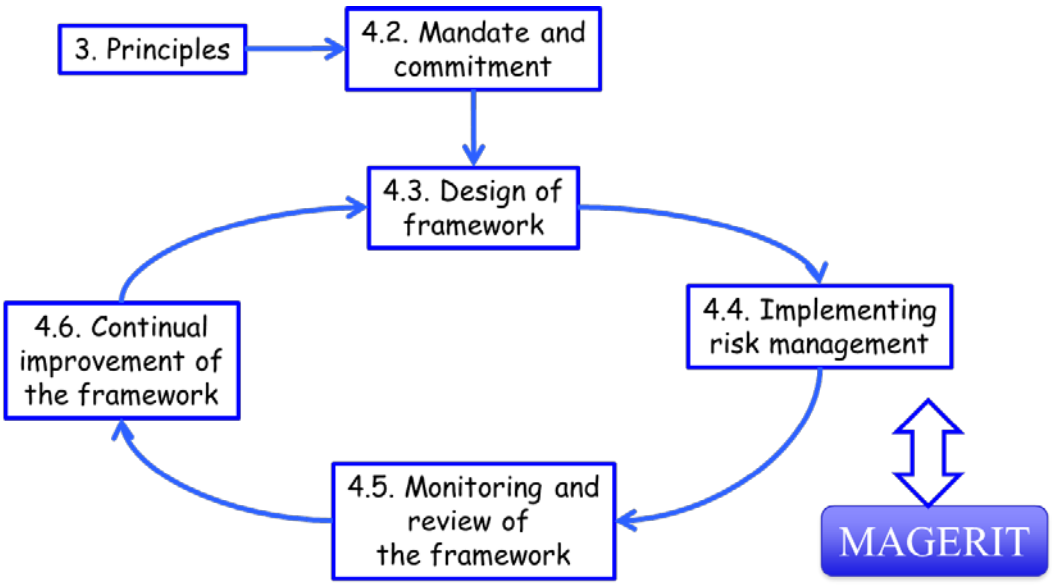

Figure1. ISO 31000 – Framework for risk management

There are several approaches to the problem of analyzing the risks supported by ICT systems: informal handbooks, methodical approaches or supporting tools. All of them aim at objectifying risk analysis to know how secure (or unsecure) systems are. The great challenge of these approaches is the complexity of the problem they have to face; complexity in the sense that there are many elements to be considered and, if it is not done rigorously, the conclusions will be unreliable. Thus, the ultimate aim of using Magerit is to make a methodical approach that leaves no room for improvisation, and not to depend on the analyst's whim.

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

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.

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

Summary of the threats to which the assets are exposed.

Statement of applicability

For a set of safeguards indicate which ones are applicable in the information system under study, and which ones are meaningless.

Safeguard evaluation

Evaluation of the effectiveness of the existing safeguards in relation to the risks systems face.

Risk status

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

Deficiencies report (Vulnerabilities report)

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

Compliance

Meeting some requirements. Formal statement that it is in line and in accordance with the corresponding regulations.

Security plan

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

1.5. 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 mission, taking different security dimensions into account:

Availability

Readiness of the services to be used when necessary. Lack of availability causes an interruption of services. Availability directly affects organisation's productivity.

Integrity

> Maintenance of completeness and correctness of 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. Loss of confidentiality undermines the confidence of others in the organisation, and may involve the breach of laws and contractual commitments related to the custody of the information.

These canonical dimensions of security may be extended with other ones that bring us closer to the users' perception of the security of their information systems:

Authenticity (of who uses the data or services)

> An entity is who it claims to be or guarantee the source from which the data originated. Against the authenticity of the information we can have manipulation of origin or of data. Against the authenticity of users accessing services, we can have spoofing.

Accountability:

> Guarantee that it will be always possible to determine who did what and when. Accountability is essential to analyse incidents, prosecute attackers and learn from experience. Accountability maps into integrity of activity logs.

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

Risk

> Estimate of the degree of exposure to a threat that may occur on one or more assets causing damage to the Organization.

Risk is an indicator of what could happen to assets if not properly protected. It is important to know what features are of interest in each asset and to what extent these features are in danger, that is, analyze the system:

Risk analysis

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

Knowing what may happen, decisions are made:

Risk treatment

> Process devoted to modify identified risks.

There are multiple ways of dealing with risks: preventing or reducing their likelihood, minimizing their consequences, sharing them with other organisation (typically hiring a service or a cover insurance), or, ultimately, accepting them and foreseeing resources to act when needed.

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.

In fact, sometimes we accept operational risks of activities that may yield benefits surpassing the risks involved, or risks that we must face up to. That is the reason why broader definitions of risk are sometimes used:

> effect of uncertainty on objectives.
> [ISO Guide 73]

Because all this is very delicate, it is not merely technical, and it 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 to make informed decisions, and be ready to explain rationally the decisions taken.

1.6. Risk analysis and management in context

Risk analysis and treatment activities 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 co-ordination with the organisation's objectives, strategy and policies, risk treatment activities allow a security plan to be prepared which, when implemented and operated, meets the proposed objectives with the level of risk accepted by the Management. These activities as a whole are called Risk Management Process.

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 recurrent since information systems are rarely immutable; normally they are subject to continuous development both own (new assets) and the environment (new threats), requiring periodic reviews to learn from experience and to adapt to the new context.

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. The treatment phase structure actions that are undertaken on security to meet the needs identified by the analysis.

Information security management systems (ISMS) [ISO 27001] identify four main processes:

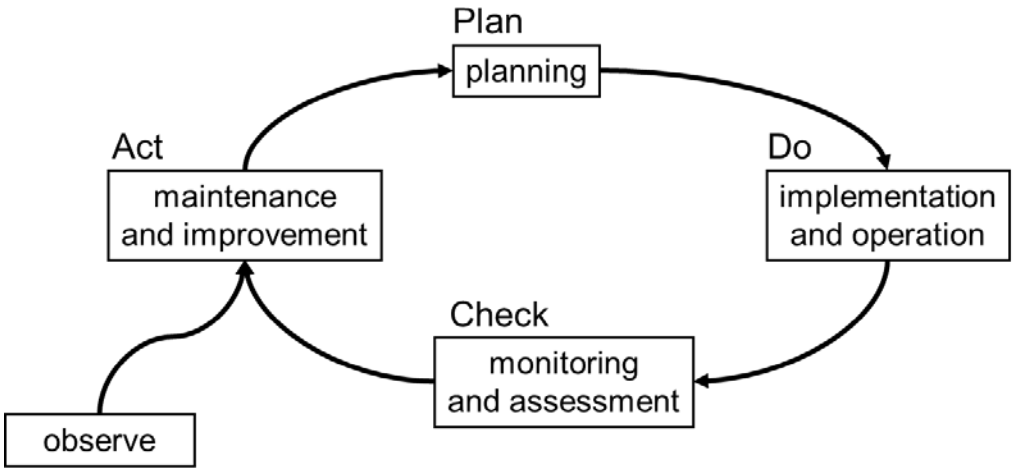

Figure 2. PDCA cycle

Risk analysis is part of planning, where treatment decisions are taken. These decisions materialize in the implementation phase, when it is recommended to deploy some elements that allow controlling the measures implemented in order to assess their effectiveness and to act accordingly, within a framework of excellence or constant improvement.

1.6.1. Awareness and training

The best security plan would be seriously undermined 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 three 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.
- Security policies that, in specific areas of activity, clarify the stance of the Organisation; i.e., defining the correct use and what non-compliance means.
- Continuous training at all levels, with reminders of routine precautions and specialised activities, depending on the responsibility assigned to each job.

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

- 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 leading by example in a daily activity, and reacting swiftly to changes and incidents.

1.6.2. Incidents and recovery

People involved in the use and operation of the system 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, re communicated to the decision points. Thus, the security system will respond to the situation.

When an incident occurs, time starts to run 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 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.

1.7. Organisation of guides

This version 3 of Magerit has been structured into two books and a technical guide:

- Book I – The method
- Book II – Catalogue of elements
- Guide of Techniques – Compilation of different kinds of techniques that could be useful to apply the method.

This book is structured as follows:

- Chapter 2 presents informal concepts. Particularly, analysis and treatment activities are framed within an integral risk management process.
- Chapter 3 defines exactly the steps and formalizes risk analysis activities.
- Chapter 4 describes risk treatment options and criteria and formalizes risk treatment activities.
- Chapter 5 is focused on risk analysis projects, on which we will be immersed in order to carry out the first risk analysis of a system and, on a temporary basis, when substantial changes have been made and the model has to be widely redone.
- Chapter 6 formalizes the activities of security plans, sometimes called master plans or strategic plans.
- Chapter 7 is focused on the development of information systems and on how risk analysis serves to manage the final product security from its initial conception to its production, as well as the protection of the development process.

- Chapter 8 anticipates some problems recurrently coming up when analysing risks.

Annexes contain reference material:

1. A glossary.
2. Bibliographical references used in developing this methodology.
3. Legal references covering the tasks of risk analysis and management in Spanish Public Administration.
4. Standards for evaluation and certification.
5. The features required from present or future tools for supporting the risk analysis and management process.
6. A comparison of how Magerit version 1 has developed into version 2, and then into version 3.

1.7.1. Method of use

The activities to be carried out are always explained informally and, in some cases, they are presented as tasks that can be planned and monitored:

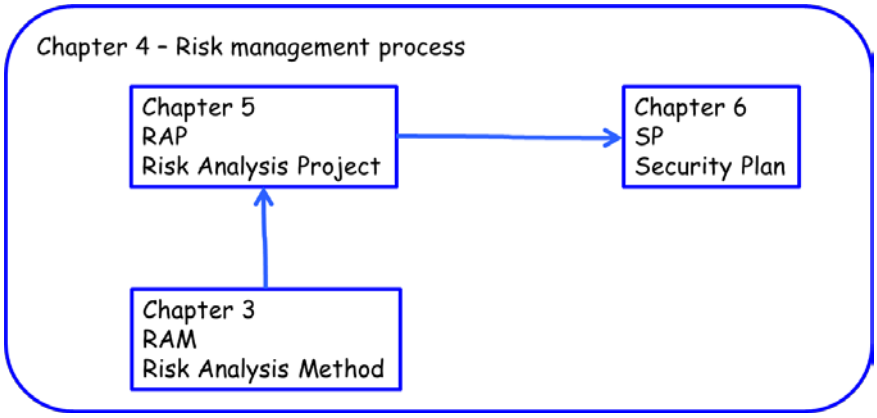

Figure 3. Formal activities

In small systems, these activities can be conducted with almost no conventionalism; but when the system grows bigger and engages different people and working teams for several weeks, months or years, a formal planning helps to keep the process under control.

This method has been designed following a “greatest extent” criteria, reflecting all kinds of situations. In practice, the user can find situations where scope is more restricted. In that case, it is advisable to be practical and try not to apply all the tasks depicted in Magerit from the beginning. The most sensible thing to do is to make a iterative approach, firstly applying the method in general terms, and then revising the model to dig into more detail. The risk management process must identify, and urgently handle critical risks, and progressively handle less critical ones. As the saying goes “the perfect is the enemy of the good.” The sensible thing to do is to harmonize efforts with the value of information and the services provided.

Thus, Magerit should be understood as a guide that may and must be tailored on a case-by-case basis and according to the different circumstances.

1.7.2. 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.

1.7.3. The Guide of 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:
  - Graphical techniques.
  - 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.

1.8. 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:

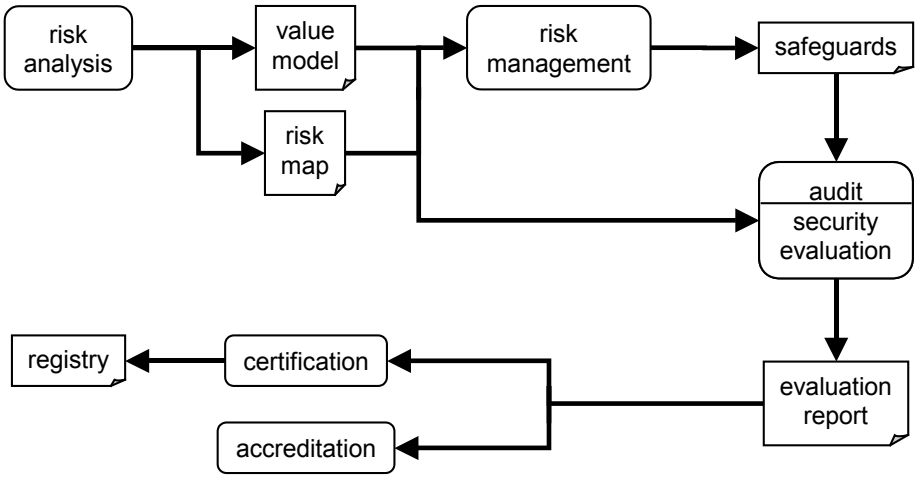

Figure 4. Certification and accreditation of information systems

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.[4]

Certification means that a known party assumes in writing a responsibility on the correctness of the certified items. The subject of the certification - product or system - is submitted to a series of evaluations aimed at an objective: What is it wanted for?[5] 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.

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.

4 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. We have a great variety of situations of lesser confidence: greater risk.

5 And thus we have systems suitable for "human consumption" or for "use in conditions of extreme heat."

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 1720/2007, article 96.2].*

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

- Spanish Royal Decree 1720/2007 of 21 December, 2007
- Spanish National Security Framework - Royal Decree 3/2010, of January 8th, which regulates the National Security Framework within the e-government scope

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.

1.9. When should risks be analysed and managed?

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.

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.

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).

The risk analysis is also a requirement for systems accrediting processes[6]. These processes are necessary for handling classified national, EU, NATO or other information from other international

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

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.

By law

Risk analysis may also be required by legal precept. Such is the case of the Royal Decree 3/2010, dated January 8, that regulates the National Security Framework within the sphere of the Electronic Administration. Chapter II, Basic Principles, states:

Article 6. Security management based on risks.

1. The analysis and management of risks will form an essential part of the security process and must be kept permanently updated.
2. Risk management will allow the maintenance of a controlled environment, reducing risks to acceptable levels. Reducing these levels will be achieved by deploying security measures to establish a balance between the nature of the information and the processes, the risks to which the information is exposed and security measures.

This same Royal Decree 3/2010, in its Chapter III, Minimum Requirements, states:

Article 13. Risk analysis and management

1. Each organisation developing and establishing systems for processing information and communications will carry out its own risk management.
2. This management will be done by analysing and processing the risks to which the system is exposed. Without prejudice to the terms of appendix II, an internationally-recognised method will be used.
3. The measures adopted to mitigate or eliminate the risks will be justified and there will always exist proportionality between them and the risks.

Act 11/2007, dated June 22, regulating electronic citizen Access to Public Services, in its Article 1, Purpose of this Act, states:

2. Public Administration Entities must use information technology according to what is stated in this Act, ensuring availability, access, integrity, authenticity, confidentiality and preservation of data, information and services they manage in the exercise of their powers.

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.

Finally, continuous risk management is one of the basic principles of the aforementioned National Security Framework.

To conclude

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

2. Overview

Two main tasks need to be carried out:

I. risk analysis,

Establishes what the organisation has at its disposal and calculates possible events.

II. risk treatment,

Allows a thorough and sensible defence schema, preventing anything bad from happening and at the same time being prepared to tackle emergencies, survive incidents and continue operating under the best possible conditions; as nothing is perfect, we say that risk is reduced to a residual level that is accepted by the Management.

Both activities, analysis and treatment, are combined into the process named **Risk Management**.

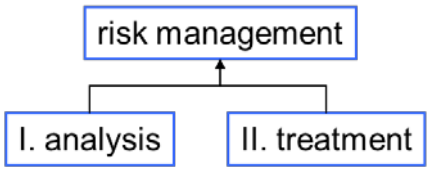

Figure 5. Risk management

Elements:

1. Assets, which are the elements in the information system (or closely related to it) that are direct or indirectly valuable to the organisation.
2. Threats, which are incidents that may impact 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 estimation of:

4. The impact: what may happen.
5. The risk: what is likely to happen.

Risk analysis allows these elements to be analysed methodically to reach conclusions with a basis and decide on treatment.

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.

Formally, risk management is structured methodically in the ISO standards (see Appendix 4.1). ISO uses he following diagram:

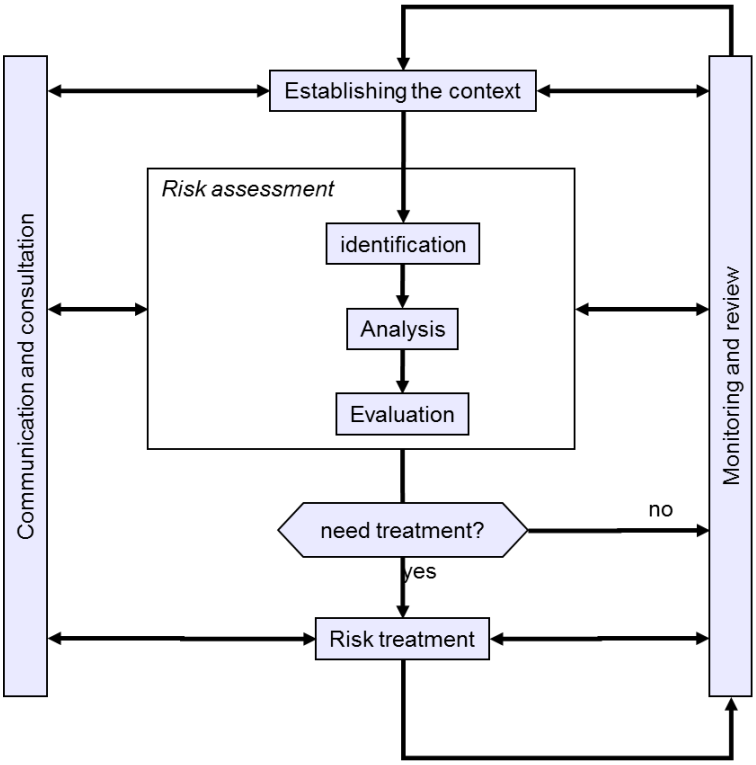

Figure 6. Risk management process (source: ISO 31000)

Establishing the context requires the definition of parameters as well as external and internal parameters that allow a framing of the policy to be followed to manage the risks. One element to be highlighted is the scope of the analysis, including its own obligations and those incurred in, as well as relations with other organisations, either for exchange of information and services or providers of subcontracted services. See [ISO 31000] for a further development of factors which establish the context.

Risk identification prepares a list of potentially dangerous spots. All that is identified will be analysed in the following stage. Whatever is not identified will remain as a hidden or ignored risk.

Risk evaluation evaluates identified risks, either quantifying their consequences (quantitative analysis) or sorting out their relative importance (qualitative analysis). Either way we will obtain, as a result, a structured vision that allows focusing on the essential.

Risk assessment goes one step further from the technical analysis and maps consequences into business terms. Here, perception, strategy and policy factors come into consideration allowing decision-making concerning which risks are acceptable or not, as well as in what set of circumstances we can accept a given risk or work on its treatment.

Risk treatment gathers activities aimed at changing the risk situation. It is an activity with numerous options as we will see later on.

Communication and consultation. It is important not to forget that information systems must support Organisation's mission. It seems absurd to have an extremely secure system that keeps the organisation from reaching its goals. A balance between security and productivity needs to be kept, and within that balance, it is necessary to count on the cooperation of several interlocutors:

- Users whose needs are to be kept into account and who are to be informed to actively cooperate in the system's operation within the security parameters established by the Management.
- External suppliers, who must be given clear instructions in order to be able to demand both required levels of service as well as the management of security incidents that may occur
- Stakeholders, to establish communication channels that consolidate the belief that the information system will respond without any surprises to attend to the organisation's mission and that any incidents will be contained according to plan.

Monitoring and inspection. It is important not to forget that risk analysis is an activity that is conducted in an office. It is thus of paramount importance to check what is happening in practice and to act accordingly, reacting diligently to incidents and continuously improving our knowledge of the system and its environment to improve the analysis and adjust it to the experience.

3. Risk analysis method

3.1. Concepts

Risk analysis is a methodical approach to estimate 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 impact weighted by the rate of occurrence (or the expectation of occurrence) of the threat.
6. In order to organize the presentation, the concepts of “impact and potential risk” are introduced between steps 2 and 3. These assessments are “theoretical”: in case no safeguard were deployed. Once this theoretical scenario is obtained, the safeguards of step 3 are included, thus deriving realistic impact and risk estimates.

The following figure shows this first round. The steps are described in the following sections:

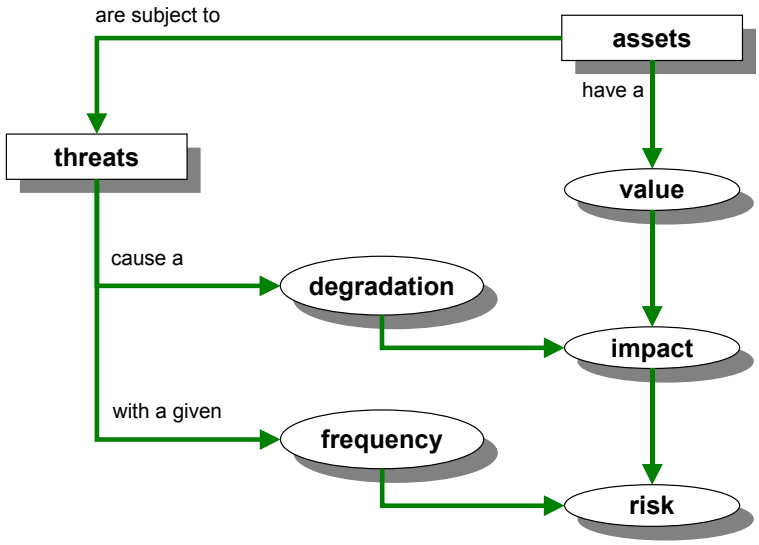

Figure 7. Elements for potential risk analysis

3.1.1. Step 1: Assets

An asset is a component or function of an information system that may be subject to deliberate or accidental attacks that may have consequences for the organisation. Assets include: information, data, services, applications (software), equipment (hardware), communications, media, facilities, and personnel.

There are two essential types of assets in an information system:

- the **information** it handles and
- the **services** it provides.

These essential assets mark the security requisites for all other assets.

Other relevant assets, subordinated to that essence can be identified:

- Data that materialize the information.
- Auxiliary services needed to organize the system.
- Computer applications (software) that process data.
- Computer equipment (hardware) that hosts data, applications and services.
- Information media, which store data.
- Auxiliary equipment that complements computer equipment.
- Communications networks that exchange of data.
- Facilities that house computer communications equipment.
- The persons who use or operate all the above elements.

Not all the assets are of the same type. The threats and safeguards are different according to the type of assets[7]. Chapter 2 of the “Elements catalogue” gives a list of types of assets.

Dependencies

The essence is the managed information and services provided. But these depend on other, more prosaic, assets such as equipment, communications or the often-forgotten persons who work with them.

Therefore, assets are organised into trees or graphs showing dependencies, where the security of the assets higher up in the tree depends on assets in the lower positions. When we move top-down, we talk about dependencies: upper assets depend on lower assets to protect their security requirements. And the other way round, when we move bottom-up, incidents on lower assets have an impact on the upper ones.

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[8].

A “higher asset” is said to depend on the “lower asset” when the security needs of the higher one are translated into the security needs of the lower one. In other words, when the occurrence of a threat in the lower asset has a detrimental effect on the high asset. Informally, this could be interpreted as the lower assets being the pillars supporting the security of the higher assets.

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

- essential assets
    - information that is handled
    - services provided
- internal services
    - that structure the information system in an orderly manner
- computer equipment
    - applications (software)
    - computer equipment (hardware)
    - communications

7 A remote access service is not attacked or defended in the same way as a work place.

8 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 is lost.

    - media: disks, tapes, etc.
- the environment:
    - equipment and supplies: energy, air conditioning, etc.
    - furniture
- all services subcontracted to third parties
- physical facilities
- staff
    - users
    - operators and managers
    - developers

Valuation

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

We are not talking of what things cost, but their value. If something is of no value, discard it. If an asset cannot be easily discarded, this is because it is of value. This is what needs to be discovered since this is what has to be protected.

Valuation can be observed from the perspective of the '**need to protect'.** The more valuable an asset, the higher the protection level it will require in the appropriate security dimension (or dimensions).

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 in the information that is handled by the system and the services provided (named essential assets). All other assets are subordinated to exploitation needs and protection of the essential.

Dimensions

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

- Its **confidentiality**: What damage would be caused by unauthorised access?
  This valuation is typical of information.
- Its **integrity**: What damage would be caused if it were damaged or corrupt?
  This evaluation is typical of information.
- Its **availability**: What damage would be caused if it were not available or could not be used?
  This valuation is typical of services.[9]

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. Therefore, it is interesting to calibrate for the essential assets:

- Its **authenticity**: To what extent is harmful the lack of knowledge about who has done what?

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

9 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.

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

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, notwithstanding that these may add 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 loss of value caused by an incident. There are many factors to be considered:

- Replacement cost: acquisition and installation.
- Labour cost invested in recovering (the value of) the asset.
- Loss of income.
- Loss of capacity to operate: lack of confidence of users and suppliers resulting in a loss of activity, or in worse 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.
- 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 “repair” 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 reputation) the exact financial valuation can be slippery and the cause of heated 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.

The “Guide of 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 cause for 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 is the investment recovered?
- What is the reasonable cost of an insurance policy?

The “Guide of 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 assessed by a single measure, qualitative or quantitative, but there is one exception: the 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:

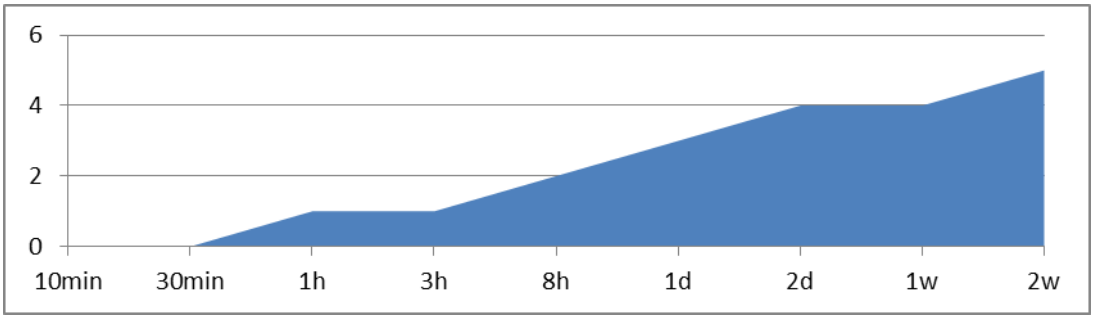

Figure 8. Cost of the (interruption of the) availability

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.

3.1.2. Step 2: Threats

The next step is to determine the threats that may affect each asset. Threats are things that could happen to our assets and impair its value.

Threat

> Events that can cause an incident in the organization, causing damage to property or intangible losses on its assets.

Threat identification

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

Of natural origin

> The information system is a passive victim of natural disasters (earthquakes, floods …); we have to assess what the consequences are.

Environmental (of industrial origin)

> The information system is a passive victim of some industrial disasters (pollution, contamination, electric failures ...); we have to assess what the consequences are.

Application failures

There are problems caused by design and/or implementation failures that have negative consequences for the system. They are commonly called technical vulnerabilities or just "vulnerabilities"[10].

Accidental threats caused by people

People with access to the information system can cause unintentional problems, especially due to error or default.

Caused by people deliberately

People with access to the information system can cause intentioned problems: deliberate attacks either to get unfair advantage or with the intention of causing damages to the rightful owners.

Not all threats affect all assets[11] 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 exposure of the asset[12] must be estimated considering two aspects:

Degradation: The amount of damage done to the [value of the] asset.

Likelihood: How often the threat occurs.

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

Degradation is often described as a fraction 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 fraction of the asset in order to calculate the proportional loss of value. But when the threat is intentional, one cannot think in such a simple-minded manner since the attacker may cause a great deal of damage indirectly.

Likelihood of occurrence is more complex to determine and explain. Sometimes it is qualitatively modeled through a nominal scale:

VH	very high	almost certain	easy
H	high	very high	medium
M	medium	possible	difficult
L	low	unlikely	very difficult
VL	very low	very rare	extremely difficult

Table1. Value degradation

10 These defects are usually known as CVE (Common Vulnerability Enumeration), an international de facto standard. Most of these defects often affect software applications.

11 Installations may catch fire but not applications. Persons may be subjected to a bacteriological attack but not services. Computer viruses affect applications but not persons.

12 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 likelihood of occurrence.

Sometimes, the likelihood is numerically modeled as a rate of occurrence. It is common to use one year as a reference, so that it uses the annual rate of occurrence as a measure of the likelihood of something happening. Typical values are:

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

Table 2. Likelihood

3.1.3. Determination of the potential impact

Impact is the measurement of the damage to an asset arising from the occurrence 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.

It should not be forgotten the dependencies between assets. Frequently, the value of the information system is on the services it provides and the data it handles while the threats usually appear in the supporting assets.

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.

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 on 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.

3.1.4. Determination of the potential risk

Risk is the measurement of the likely 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 likelihood of occurrence.

Higher impact and higher likelihood increase risk. We should consider several zones when managing risks.

- zone 1 – very likely and high impact risks
- zone 2 – covers a wide range from unlikely and medium impact situations to very likely and very low impact ones
- zone 3 – unlikely and low impact risks
- zone 4 – unlikely and very high impact risks

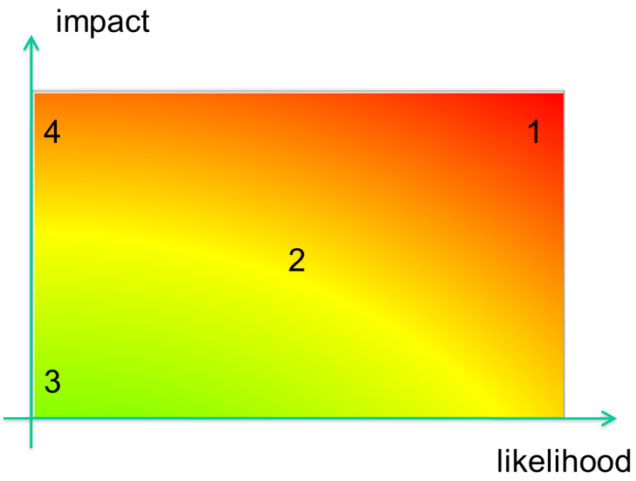

Figure 9. Risk as a function of impact and likelihood

Accumulated risk

This is calculated for an asset taking into account:

- The accumulated impact on an asset arising from a threat.
- The likelihood 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 likelihood of occurrence.

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 working 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 likelihood 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 likelihood of occurrence.

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 deriving from different threats on the same asset may be aggregated, but it should be considered to what extent different threats are independent and can be concurrent,.
- The risk of a threat in different dimensions may be aggregated.

3.1.5. Step 3: Safeguards

So far, safeguards have not been taken into consideration. Thus, we are evaluating the impacts and risks to which the assets would be exposed if they were not protected in any way.

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.

Selection of safeguards

Given the wide variety of safeguards, it is necessary to go through all of them and retain only those which are relevant for protecting the asset. When making the selection, we should consider the following aspects:

1. Kind of assets to be safeguarded; each asset must be safeguarded in a specific way
2. Security aspect/aspects that require to be safeguarded
3. Threats we need to be safeguarded against
4. Potential alternative safeguards

Furthermore, it is advisable to establish a principle of proportionality and take into account the following:

1. The value to protect in the asset, either intrinsic or accumulated, focusing on the most valuable assets and ignoring the irrelevant
2. The likelihood of occurrence of a threat, focusing on the most important risks (see risk zones)

3. Risk coverage provided by alternative safeguards

Therefore, there are two kinds of statements to reject a given safeguard:

- it does not apply – when a safeguard does not apply because it is not technically suitable for the assets to be protected, does not provide the necessary protection or does not protect the asset against the threat in question.
- it is not justified – when the safeguard applies but it is disproportionate to the risk.

As a result, we will have a “statement of applicability” or group of safeguards that must be analysed as part of our protection system.

The effect of safeguards

Safeguards are taken into account in the calculation of risk in two ways:

Reducing the likelihood of occurrence of threats

> These ones 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 escalation of the incident. There are even some safeguards that are focus on quick recovery of the system after the threat destroys it. In all of these versions, the threat occurs but the consequences are limited.

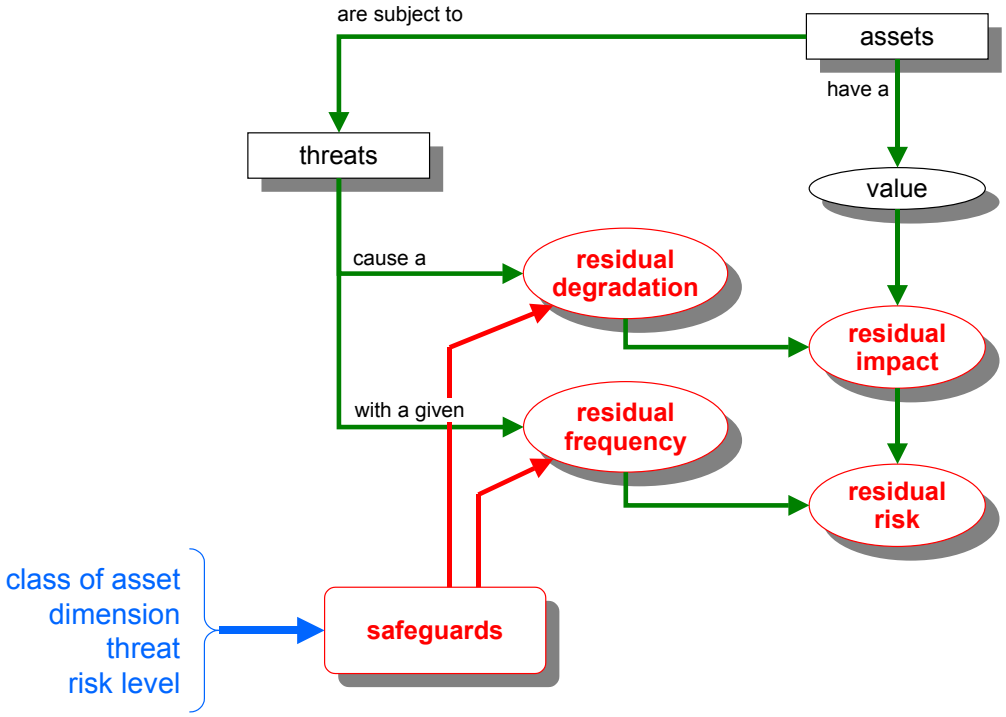

Figure 10. Elements to estimate residual risk

Type of protection

It is customary to speak of different types of protection provided by the safeguards:

[PR] prevention

> A safeguard is preventive when it reduces the chances of the incident to happen. If the safeguard fails, and the incident occurs, the impact is not changed.

Examples: user authorisation, privilege management, …, capacity planning, …, software development standards, …, testing before deploying, …, separation of duties, …

[DR] deterrence

A safeguard deters attackers when these ones do not dare to attack. If the safeguard is not effective enough, the attack will occur, the impact is not changed.

Examples: high walls, armed guards, prosecution warnings, …

[EL] elimination

A safeguard eliminates an incident when it prevents the incident from occurring. These safeguards work before the incident happens. They do not limit damages if the safeguard is not perfect, and the incident occurs.

Examples: removing standard user accounts, accounts without a strong password, unnecessary services, in general any activity that bastions an asset,…, channel encryption, …, fire-proof cabinets, …

[IM] impact minimization

A safeguard minimizes impact when it does not prevent the incident to occur, but limits the consequences.

Examples: network isolation upon intrusion detection, services halt when attacked, insurance, law compliance, …

[CR] correction

A safeguard is corrective when it actuates after the incident or attack has occurred, repairing the damages.

See recovery below.

Examples: incident management, alternative communication lines, alternative power supplies, …

[RC] recovery

Safeguards that, after the incident has occurred, are able to recover the previous situation after a while. The incident is not less likely, but the consequences are limited.

Examples: back-up copies, …

[MN] monitoring

Monitoring safeguards discover incidents by inspecting activity logs. If the safeguard is fast enough, it may enable reaction or recovery safeguards. If the safeguard is not fast enough to act on real time, the discoveries are still useful to learn from the experience, and improve the security.

Examples: activity logs, web download log, …

[DC] detection

Safeguards that detect incidents and enables or fires immediate reaction.

Examples: anti-virus, IDS, smoke detectors, …

[AW] awareness

Awareness safeguards are those ones devoted to improve the capabilities of the people that may interact with the system. Awareness reduces unintentional errors. Training of operators improves the reaction time to incidents, and the performance of recovery safeguards.

Examples: personnel training, …

[AD] administration

Administrative safeguards are those ones devoted to check every element of the system, preventing anything to work unnoticed. A good administrative safeguard impedes open doors that might be exploited.

Examples: inventory of assets, …, risk analysis, …, continuity plan, …

The following table links each kind of protection with the former model (decreasing degradation and likelihood):

effect	type of protection
preventive: reduce likelihood	[PR] prevention [DR] deterrence [EL] elimination
reduce degradation	[IM] impact minimization [CR] corrective [RC] recovery
strengthen the effect of the other	[MN] monitoring [DC] de detection [AW] awareness [AD] administrative

Table2. Safeguard types

Effectiveness of safeguards

Safeguards are characterized by their effectiveness against the risk they intend to counter. The ideal safeguard is 100% effective; this effectiveness includes two factors:

From the technical point of view:

- It is technically suitable to confront the risk
- It is always on

From the point of view of the safeguard operation

- It is perfectly deployed, configured and maintained
- There are clear procedures for normal operation, and for reaction to incidents
- Users are trained and aware
- There are controls in place to warn about possible failures

A real effectiveness level shall be estimated on a case by case basis, ranging from 0% (inexistent safeguards) to 100% (suitable and well-established). To measure the organisational aspects, a maturity scale to measure the confidence deserved by the safeguard management process (as a correction factor):

factor	level	meaning
0%	L0	inexistent
	L1	initial / ad hoc
	L2	repeatable, but intuitive
	L3	defined process
	L4	managed and measurable
100%	L5	optimised

Table3. Effectiveness and maturity of safeguards

Vulnerabilities

Vulnerability is any weakness that can be exploited by a threat or, more specifically, any weakness of an asset or its safeguards that facilitate the success of a potential threat.

Using the terms in the above paragraphs, we define vulnerability as the absence or ineffectiveness of the safeguards required to protect the own or accumulated value of an asset. Sometimes we use the term “insufficient” to stress the fact that the effectiveness of the safeguard is inadequate to protect the value of an asset exposed to a threat.

3.1.6. Step 4: residual impact

When a series of safeguards are in place and the management process is mature to a certain extent, the system can suffer an impact named “residual”. The impact changes from potential to residual.

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

The residual degradation is estimated taking into account the deployment of safeguards.

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

3.1.7. Step 5: residual risk

When a series of safeguards are in place and the management process is mature to a certain extent, the system is exposed to a risk called “residual”. The risk changes from potential to residual.

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

The degradation was taken into consideration when calculating the residual impact.

The residual likelihood is estimated taking into account the deployment of safeguards.

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

3.2. Formalization of the activities

These activities have the following goals:

- To establish a system value model, identifying and assessing relevant assets.
- To prepare a system risk map, identifying and assessing the threats against the assets.
- To know the current situation of safeguards
- To assess the potential impact on the system under study, both the potential impact (without safeguards) and the residual impact (including the effect of the safeguards deployed to protect the system)

- To assess the risk against the system under study, both the potential risk (without safeguards) and the residual risk (including the effect of the safeguards deployed to protect the system).
- To report on the system areas with higher impact/risk so as to make the appropriate decisions on the proper grounds.

Risk analysis is carried out through the following tasks:

RAM – Risk Analysis Method
RAM.1 – Characterization of assets
RAM.11 – Identification of assets
RAM.12 – Dependencies between assets
RAM.13 – Valuation of assets
RAM.2 – Characterization of threats
RAM.21 – Identification of threats
RAM.22 – Valuation of threats
RAM.3 – Characterization of safeguards
RAM.31 – Identification of relevant safeguards
RAM.32 – Evaluation of safeguards
RAM.4 – Risk status estimate
RAM.41 – Impact estimate
RAM.42 – Risk estimate

RAM.1: Characterization of assets

This activity identifies the relevant assets within the system to be analysed and characterizes them according to the type of assets, identifying relations between different assets, determining which security dimensions are important, and valuates this importance.

The outcome of this activity is a report named “value model”

Sub-tasks:

RAM.11: Identification of assets

RAM.12: Dependencies between assets

RAM.13: Valuation of assets

RAM.2: Characterization of threats

This activity identifies the relevant threats on the system to be analysed and characterizes them according to the estimates of occurrence (likelihood) and the damage done (degradation).

The outcome of this activity is a report named “risk map”

Sub-tasks:

RAM.21: Identification of threats

RAM.22: Valuation of threats

RAM.3: Characterization of safeguards

This activity identifies the safeguards deployed in the system to be analysed and characterizes them according to their effectiveness against the threats they intend to mitigate.

The outcome of this activity is a collection of reports:

— Statement of applicability

— Evaluation of safeguards

— Deficiencies (or vulnerabilities of the protection system)

Sub-tasks:

RAM.31: Identification of relevant safeguards

RAM.32: Evaluation of safeguards

RAM.4: Estimate of the risk status

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

• elaborate a risk status report : impact and risk estimate

• elaborate a deficiencies (vulnerabilities) report: flaws or weaknesses of the safeguards system

Sub-tasks:

RAM.41: Estimate of impact

RAM.42: Estimate of risk

Tasks related to assets (RAM.1) are often carried out at the same time that tasks related to threats against those assets (RAM.2) and the identification of the current safeguards (RAM.3), just because people are usually the same and the interlocutor tends naturally to deal with every asset “vertically”, by analysing everything that affects it before moving on to the following asset.

3.2.1. RAM.1: Characterization of assets

This activity has three sub-tasks:

RAM.11: Identification of assets

RAM.12: Dependencies between assets

RAM.13: Valuation of assets

The objective of these tasks is to know the assets making up the system, to define the dependencies between them, and to determine which part of the system is supported by each asset. It can be summarized in the expression “Know yourself!”

RAM: Risk analysis *RAM.1: Characterization of assets* *RAM.11: Identification of assets*
Objectives • To identify the assets composing the system and determine their characteristics, attributes and classification in the specific types.
Input products • Inventory of the information handled by the system • Inventory of the services provided by the system • Business processes • Use case diagrams • Data flow charts • Inventory of software • Inventory of hardware

RAM: Risk analysis *RAM.1: Characterization of assets* *RAM.11: Identification of assets*
• Premises and offices of the Organisation • Functional characterization of jobs
Output products • List of assets to consider • Characterization of assets: own and accumulated values • Relationship between assets
Techniques, practices and guidelines • See “Book II – Catalogue”. • Data flow charts • Process charts • Interviews (see "Guides to techniques") • Meetings

This task is crucial. A good identification is important from several points of view:

- settles down the scope of the project
- allows interlocution with the group of users: all speak the same language
- allows to determine the specific dependency between assets
- allows to value the assets accurately
- allows to identify and value the threats accurately
- allows to determine which safeguards will be required to protect the system

Characterization of assets

For each asset, a series of characteristics defining it has to be defined:

- code, usually coming from the inventory
- name (short)
- description (long)
- type (or types) that characterizes the asset
- the responsible unit. Sometimes, there is more than one unit. For example, in the case of applications the unit maintaining it may be different from the unit exploiting it
- the responsible person. Particularly relevant in the case of data. Sometimes, there is more than one person responsible. For example, in the case of personal data, there may be a difference between the person responsible for the data and the operator(s) that handles them
- technical (in intangible assets) or geographical (in material assets) location
- amount, where appropriate; for example, in the case of the personal computing (for example, 350 desktop equipment)
- other specific characteristics of the type of asset

RAM: Risk analysis *RAM.1: Characterization of the assets* *RAM.12: Dependencies between assets*
Objectives • Identify and assess the dependencies between assets, that is to say, the degree to which a higher asset is affected by a threat against a lower asset •
Input products • Results of the task RAM.11, Identification • Business processes • Data flow charts • Use case diagrams
Output products • Dependencies between assets chart
Techniques, practices and guidelines • Data flow charts • Process charts • Interviews (see "Guide of Techniques") • Meetings • Delphi evaluation (see "Guide of Techniques")

For each dependency, the following information has to be registered:

- estimate of the degree of dependency: up to 100%
- explanation of the dependency valuation
- interviews from which the above-mentioned estimates have been deduced

RAM: Risk analysis *RAM.1: Characterization of assets* *RAM.13: Valuation of assets*
Objectives • Identify to which level the asset is valuable • Valuate the cost that the destruction of the asset will cause to the Organisation
Input products • Results of RAM.11, Identification of the assets • Results of RAM.12, Dependencies between assets
Output products • Value model: report on the value of the assets

RAM: Risk analysis *RAM.1: Characterization of assets* *RAM.13: Valuation of assets*
Techniques, practices and guidelines • See “Book II – Catalogue”. • Interviews (see "Guide of Techniques ") • Meetings • Delphi evaluation (see "Guide of Techniques ")

Several groups within the Organisation have to be interviewed to obtain this knowledge:

- leaders or managers, who know the effect on the mission of the Organisation
- people responsible for the data, who know the impact of their security failures
- people responsible for the services, who know the impact caused when no service or a degraded service is provided
- people responsible for the information systems and the operations, who know the impact of an incident

The following information should be registered for each evaluation:

- dimensions into which an asset is relevant
- estimate of the valuation of each dimension
- explanation of the valuation
- interviews from which the above-mentioned estimates have been deduced

3.2.2. RAM.2: Characterization of the threats

This activity has two sub-tasks:

RAM.21: Identification of threats

RAM.22: Valuation of threats

The objective of these tasks is to characterize the environment the system must face, what can happen, what consequences it could have, and how likely it is that it occurs. We could summarize it in the expression “know your enemy”.

RAM: Risk analysis *RAM.2: Characterization of threats* *RAM.21: Identification of threats*
Objectives • Identify the relevant threats against each asset
Input products • Results of RAM.1, Characterization of assets • Reports on flaws in the product, that is to say, vulnerabilities reports
Output products • List of possible threats

RAM: Risk analysis
RAM.2: Characterization of threats
RAM.21: Identification of threats

Techniques, practices and guidelines

- Catalogue of threats (see "Elements catalogue")
- Attack trees (see "Guide of Techniques")
- Interviews (see "Guide of Techniques ")
- Meetings
- Delphi evaluation (see "Guide of Techniques ")

This task identifies the important threats against identified assets by taking into consideration:

- the type of the asset
- the dimension in which an asset is valuable
- the experience of the Organisation
- the defects reported by manufacturers and organisations that respond to security incidents (CERTS)

The following information has to be registered for each threat against each asset:

- explanation of the impact of the threat
- interviews from where the above-mentioned estimate has been deduced
- relevant background, if any, in either the own Organisation or other organisations

RAM: Risk Analysis
RAM.2: Characterization of threats
RAM.22: Valuation of threats

Objectives

- Estimate the likelihood of occurrence of each threat against each asset
- Estimate the degradation that the threat may cause in each dimension of the asset if it occurred

Input products

- Results of RAM.21, Identification of threats
- Historical series of incidents
- Reports of defects in the products
- Background: incidents in the Organisation

Output products

- Risk map: report on the possible threats characterized by their rate of occurrence and the possible degradation they could cause on the assets

Techniques, practices and guidelines

- Attack trees (see "Guide of Techniques")
- Interviews (see "Guide of Techniques")
- Meetings
- Delphi evaluation (see "Guide of Techniques ")

This task assesses the threats identified in the previous task by taking into consideration:

- the universal experience (history)
- the experience (history) of the activity sector
- the experience (history) of the environment where systems are located
- the experience (history) of the Organisation itself
- the reports attached to the reports of defects provided by manufacturers and organisations that respond to security incidents (CERTS)

There is a series of possible aggravating factors, described in section 8.6, which has to be taken into account

The following information should be registered for each threat:

- estimate of the likelihood of the threat
- estimate of the damage (degradation) that it could cause if it occurred
- explanation of the estimates of likelihood and degradation
- interviews from which the above-mentioned estimates have been deduced

3.2.3. RAM.3: Characterization of safeguards

This activity is made up of two sub-tasks:

RAM.31: Identification of the relevant safeguards

RAM.32: Evaluation of safeguards

These tasks have two objectives: to know what it is necessary to protect the systems and whether the protection is suitable for the needs.

RAM: Risk analysis *RAM.3: Characterization of safeguards* *RAM.31: Identification of relevant safeguards*
Objectives • Identify the safeguards suitable for protecting the system
Input products • model of assets in the system • model of threats against the system • residual impact and risk indicators • reports on products and services on the market
Output products • Statement of applicability: justified list of the safeguards required • List of the safeguards deployed
Techniques, practices and guidelines • Catalogue of safeguards (see "Elements Catalogue ") • Attack trees (see "Guide of Techniques ") • Interviews (see "Guide of Techniques ") • Meetings

The following information should be registered for each safeguard:

- description of the safeguard and its implementation status
- description of the threats it intends to face
- interviews from where the above-mentioned information has been deduced

Catalogues of safeguards or the advice of experts is often used to determine the relevant safeguards. Eventually, there will be a set of possible safeguards. Thus, the complex problem of finding what we need will come down to the easier problem of discarding what we do not need.

There are several reasons to discard a proposed safeguard:

- it is not suitable for the asset to be protected
- it is not suitable for the security dimension to be protected
- it is not effective when opposing the threat to be countered
- it is excessive (disproportionate) to the value to be protected
- there are alternative measures available

RAM: Risk analysis *RAM.3: Characterization of safeguards* *RAM.32: Valuation of safeguards*
Objectives • Determine the effectiveness of the relevant safeguards
Input products • Inventory of the safeguards from RAM.31
Output products • Safeguard evaluation : report on the safeguards deployed, characterized by their degree of effectiveness • Deficiencies (or vulnerabilities) report: list of safeguards that should be deployed but they are not , or are poorly deployed
Techniques, practices and guidelines • Interviews (see "Guide of Techniques ") • Meetings • Delphi evaluation (see "Guide of Techniques ")

This task assesses the effectiveness of the safeguards identified in the previous task by taking into account:

- the suitability of the safeguard to the objective pursued
- the quality of the implementation
- the training of the people responsible for their configuration and operation
- the training of the users, if they play an active role
- the existence of controls to measure their effectiveness

- the existence of regular revision procedures

The following information should be registered for each safeguard:

- Assessed efficiency to face those threats
- Explanation of the estimated efficiency
- Conducted interviews from which the above information has been collected

3.2.4. RAM.4: Estimated risk status

This task combines the findings of the previous tasks (RAM.1, RAM.2 and RAM.3) to derive estimated risk status of the Organisation.

This activity is made up of three tasks:

RAM.41: Estimated impact

RAM.42: Estimated risk

These tasks derive estimations based on what may happen (impact) and on its likeliness to happen (risk).

RAM: Risk Analysis *RAM.4: Estimated risk status* *RAM.41: Estimated impact*
Objectives • To determine the potential impact on the system • To determine the residual impact on the system
Incoming Products • Results of activity RAM.1, Characterization of the assets • Results of activity RAM.2. Characterization of the threats • Results of activity RAM.3, Characterization of the safeguards
Output Products • (Potential) Impact Report per asset • Report of residual impact per asset
Techniques, practices and patterns • Analysis using tables (see "Guide of Techniques") • Algorithmic Analysis (see "Guide of Techniques")

This task estimates the impact on the system's assets:

- The potential impact on the system, taking into consideration the value of the assets and the assessment of the threats; but not the currently implemented safeguards. ,
- The residual impact on the system, taking into consideration the value of the assets and the assessment of the threats, and the efficiency of the currently implemented safeguards.

RAM: Risk Analysis *RAM.4: Estimated risk status* *RAM.42: Estimated risk*
Objectives • To determine the potential risk on the system • To determine the residual risk on the system
Incoming Products • Results of activity RAM.1, Characterization of assets • Results of activity RAM.2, Characterization of threats • Results of activity RAM.3, Characterization of safeguards • Results of activity RAM.4, Estimated impact
Output Products • (Potential) Risk Report per asset • Report of residual risk per asset
Techniques, practices, and patterns • Analysis using tables (see "Guide of Techniques") • Algorithmic Analysis (see "Guide for Techniques")

This task estimates the risk to which the system assets are exposed:

- The potential risk to which the system is exposed, taking into consideration the value of the assets, and the threat assessment; but not the currently implemented safeguards.
- The residual risk to which the system is exposed, taking into consideration the value of the assets and the threat assessment, and the efficiency of the currently implemented safeguards.

3.3. Documentation

Intermediate Documentation

- Results of the interviews.
- Documentation of other sources: statistics, remarks by experts and remarks by analysts.
- Existing information to be used for the Project (for example, assets inventory)
- Additional documentation: maps, charts, requirements, specifications, functional analyses, accounting books, user's manuals, exploitation manuals, information and process flowcharts, data patterns, etc.
- Reports and assessments of flaws in the products, from manufacturers and centres for response to security incidents (CERTs).

Final Documentation

- Value Model

  Report detailing the assets, inter-dependencies, sizes in which they are valuable and estimated value.

- Risks Map:

  Report detailing major threats on each asset, characterized by their likelihood and degradation caused on the assets.

- Statement of Applicability:

  Report collecting the counter-measures regarded as appropriate to protect the information system under examination.

- Assessment of safeguards:

  Report detailing the existing safeguards, classifying them according to their efficiency to reduce the risk they face.

- Report on shortcomings or vulnerabilities:

  Report detailing the safeguards that are necessary, but absent, or insufficiently effective.

- Risk Status:

  Report detailing for each asset the impact and the potential and residual risks regarding every threat.

This documentation is a true reflection of the risk status and the reasons for which the risk is not acceptable. It is essential to understand the reasons that lead to a determined risk assessment so as the risk management process will be well founded. The risk management process will stem from these assessments to eliminate the risk or reduce it to an acceptable level.

3.4. Checklist

√	Activity	task
	Key assets have been identified: information to be dealt with and services provided	RAM.11
	Needs or levels of security have been assessed that are required for each key asset in each security dimension	RAM.13
	Other system assets have been identified	RAM.11
	It has been established the value (or the required security level) of the other assets depending on their relation with other essential assets (for example, through the identification of the premises)	RAM.12
	Possible threats on the assets have been identified	RAM.21
	The consequences have been estimated, if those threats actually occurred	RAM.22
	The likelihood that those threats actually occurred has been estimated	RAM.23
	Potential impacts and risks- inherent to the system - have been estimated	RAM.4
	The applicable safeguards have been identified to tackle potential impacts and risks	RAM.31
	The implementation of the identified safeguards has been assessed	RAM.32
	The values of residual impact and risks have been estimated, which correspond to the level of impact and risk that the system, after the implementation of the safeguards, continues to support.	RAM.4

4. Risk management process

Given the impacts and risks to which the system is exposed, a number of decisions determined by several factors have to be taken:

- Seriousness of the impact and/or risk
- The obligations to which the Organisation is subject under the law
- The obligations to which the Organisation may be subject under sectorial regulations
- The obligations to which the Organisation may be subject under the contract

With the room of manoeuvre provided for by this framework, there could be additional considerations on the capacity of the Organisation to accept certain impacts of intangible nature[13] such as:

- Public image (reputation aspects)
- Internal policy: relationship with those employees, such as the capacity to hire the suitable personnel, capability to keep the best employees, capability to support shifts of employees, capability to offer an attractive professional career, etc.
- Relationship with the providers, such as capability to reach advantageous agreements in the short, medium and long term, capability to have a privileged treatment, etc.
- Relationship with the clients or users, such as capability to keep clients, capability to increase the offer, capability to make a difference before the competitors, ...
- Relationship with other organisations, such as capability to reach strategic agreements, alliances, etc.
- New business opportunities, such as forms to recover the investment in security
- Access to seals or known security classifications

All the previous considerations lead to classifying each major risk, specifying whether...

1. It is **critical** in the sense of demanding urgent attention
2. It is **serious** in the sense that it demands attention
3. It is **substantial** in the sense that it deserves further examination
4. It can be **taken** in the sense that no actions are going to be taken to counter the risk

Option 4, taking the risk, is always risky, and it has to be taken with caution and justification. The reasons that could lead to such an acceptance are:

- If residual impact can be assumed
- If residual risk can be assumed
- If the cost of timely safeguards is disproportionate when compared to residual impact and risk.

The classification of the risks will have consequences in the subsequent tasks, establishing the relative priority of different actions.

13 Risk analysis and management methodology focuses on harm. Therefore, there is a difficulty to address benefits from lack of harm. However, trust on the system enables a better performance of the organisation in its environment.

4.1. Concepts

Risk analysis determines the impact and risk. Impact includes absolute damages, regardless of whether that a given circumstance is more or less likely. Risk, however, ponders likelihood of occurrence. The impact reflects the possible damage (i.e. the worst to occur), while the risk reflects the expectable damage (i.e. what is likely occur).

The analysis result is just an analysis. Based on it, we have information to take decisions once we know what we want to protect (assessed assets) what we want to protect it against (assessed threats) , and what we have done to protect it (assessed safeguards). All of this is synthesized in impact and risk values.

From that moment on, decisions will come from the management bodies of the Organisation that will take two (2) steps:

- step 1: Evaluation
- step 2: Treatment

The following chart is a summary of the possible decisions that can be taken after examining the risks. The box 'risk assessment' combines analysis and evaluation.

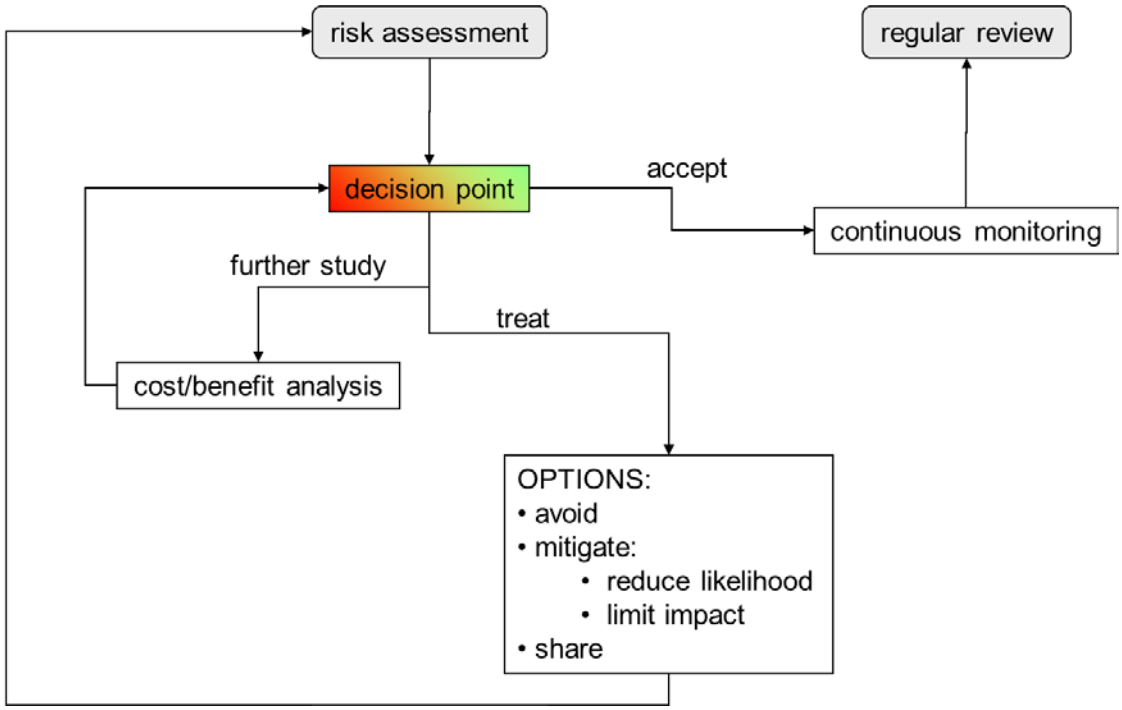

Figure 11. Risk treatment decision making

All these aspects are further discussed below.

4.1.1. Evaluation: interpretation of the residual impact and risk values

Residual impact and risk are a measure of the current status between potential insecurity (without any safeguard), and the adequate measures that will reduce the impact and risk to acceptable values.

The following paragraphs refer to both impacts and risks.

If the residual value is equal to the potential value, the existing safeguards are useless, either because there is nothing done, or because there are essential elements that have not been taken into consideration.

It is important to understand that a residual value is just a number. For its correct interpretation it must be accompanied by the account of what should be done and has not been done; that is to say, system vulnerabilities. Those responsible for taking decisions must pay careful attention to the account of pending tasks, which is named **Report on shortcomings or vulnerabilities**.

4.1.2. Risk acceptance

Management of the Organisation subject to risk analysis must determine the acceptable impact and risk levels. More precisely, it must accept the responsibility of residual values. This is not a technical decision. It may be a political or managerial decision, or it could be determined by law or by the contractual obligations with providers and users. These acceptance levels may be established by an asset or by adding up assets (in a determined department, in a determined service, in a determined dimension ...)

Any impact and/or risk level is acceptable if the Managing Board is aware of and accepts it[14].

4.1.3. Treatment

Management may decide to apply some particular treatment to the deployed security system to protect the information system. There are two broad options:

- Reducing the residual risk (accepting a lower risk)
- Extending the residual risk (accepting a higher risk)

To take either decision we have to make a picture of the risks that the information system bears within a wider context that covers a wide spectrum of considerations out of which we could pinpoint some without intending to be comprehensive:

- Complying with obligations; whether legal, public regulation or regulation for the sector, internal commitments, mission of the Organisation, corporative responsibility, etc.
- Possible benefits stemming from an activity that does entail risks.
- Technical, economic, cultural, political or any other conditioning factor.
- Balance with regard to other types of risks: commercial, financial, regulatory, environmental, labour and other risks …

Under **extreme residual risk** conditions, virtually the only option is to reduce the risk.

Under **acceptable residual risk** conditions, we may choose between accepting current risk, or accepting higher risks. In any case we have to maintain a continuous monitoring of the circumstances to check whether expected risk matches real experience, and react to any major deviation.

14 It may be most adequate to write “stakeholders” to refer to those affected by the strategic decisions in an Organization: owners, managers, users, employees and even society in general. Because ultimately if high risks are recklessly accepted, the affected party cannot be just the organization leaders, but all those who have put their trust in the organization and whose shameful performance darken their legitimate expectations. Ultimately, it may be affected confidence in a sector or a technology by the reckless staging of some actors.

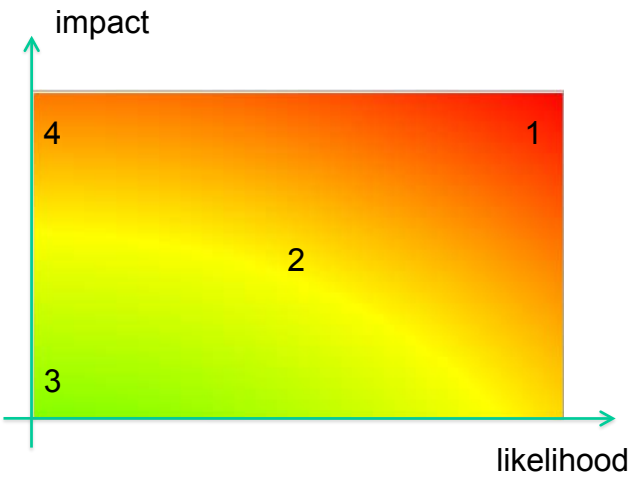

Figure 12. Risk areas

Under **medium residual risk** conditions, we may observe other features such as benefits and losses that may be affected by the present scenario, or even we may analyse the status of the sector where we operate to compare ourselves to the “standard”.

In terms of risk areas that were presented above,

- zone 1 – very likely or very high impact and risk; we try to leave this zone
- zone 2 – relatively likely and medium impact and risk; several options
- zone 3 – unlikely and low impact and risk; we may retain the risks as they are, or we may take higher risk if there were some advantage or benefit for other reasons.
- zone 4 – unlikely but very high impact; it is a challenge because it does not justify preventive measures to be taken, but its high impact demands to have something ready to react; that is to say, we have to highlight reaction measures to limit damages, and measures to recover from disasters.

We also have to take into account the uncertainty of the analysis. Sometimes when we suspect the consequences, but there is a wide range of opinions on the magnitude (uncertainty of the impact). Sometimes uncertainty affects likelihood. These scenarios usually affect zones 4 and 3, because when likelihood is high, we gain experience very quickly –either our own, or others’ experience-, and we get out of uncertainty. In any case, any uncertainty must be considered as bad, and we must do something:

- to look for ways to improve foresight, typically investigating into fora, centres for response to incidents, or experts on the matter;
- to prevent the risk changing some aspect, component, or architecture of the system; or
- to have implemented early warning systems and flexible procedures for contention, limitation, and recovery of the possible incident.

Sometimes these scenarios occur on a field where there are regulations to comply with, and regulations themselves eliminate, or notably reduce available options; that is to say, the system protects itself out of regulations rather than out of certainty of the risk.

Treatment decisions will be taken having in mind these considerations:

4.1.4. Quantitative study of costs/benefits

It is common sense that we cannot invest in safeguards beyond the value that we want to protect.

In practice there are a number of charts as the one in Figure 13 setting insecurity costs (what would cost having no protection) and safeguard costs against one another.

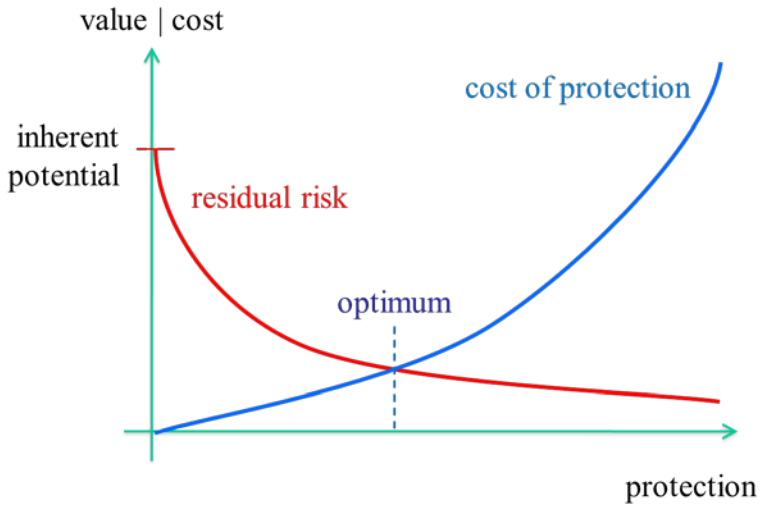

Figure 13. Relationship between spending on security and the residual risk

These charts are intended to reflect how moving from a security level 0 to a security level 100%, the insecurity cost (the risk) diminishes, while cost increases. Its intended that risk falls sharply with small investments[15], and that the cost of investments rockets to achieve security levels near 100%[16]. Somehow, there is a balance point between what is risked and what is invested in defence, a point to try to achieve when the only consideration is economic.

But applying common sense to practice is not evident, based neither on the risk estimate, or safeguards cost estimate. In other words, the above curve is conceptual and cannot be drawn in a real case.

In practice, when we have to protect from a risk that is considered major, there are several hypothetical scenarios:

E0: if nothing is done

E1: if a certain set of safeguards is implemented

E2: if another set of safeguards is implemented

And so on, up to N scenarios with different combinations of safeguards.

The economic analysis will decide between these options, being E0 (to continue as we are) a possible option, which could be justified in economic terms.

In each scenario we have to estimate the cost that will mean overtime. To be able to add up costs, losses of money will be accounted for as negative values, and money incomes will be accounted for as positive values. Let's consider the following components:

- (recurrent) residual risks[17]
- (once) cost of safeguards[18]
- (recurrent) cost of safeguards' maintenance per year

15 Basic security measures represent a significant reduction in risk. So they are inexcusable.
16 Showing once again that absolute security (zero risk) does not exist.
17 If the rate of occurrence of threats has been estimated as an annual rate, data will be automatically annualized residual risk. If you had used a different scale, we should convert to annual terms.
18 If the safeguard already exists, its improvement is resource consuming. It is does not exist, its acquisition and deployment requires resources. In either circumstance, you have to add training costs.

- (recurrent) productivity improvements[19]
- (recurrent) improvement in the Organisation's capability to provide new services, obtain better conditions from suppliers, associate with other organisations, etc.

Scenario E0 is very simple: every year we pay the expenses derived from risks, and the total cost accumulates year after year.

In the rest of the scenarios, there are things that add and things that subtract, and different situations[20] could occur, like those included in the graphic below. Values represented are those accumulated along a five-year period. The gradient corresponds to the recurrent costs. The value of the first year corresponds to implementation costs.

	risk (annual)	cost (initial)	cost (annual)	improvements (annual)	other (annual)	year 1	2	3	4	5
E0	10	0	0	0	0	-10	-20	-30	-40	-50
E1	5	20	5	0	0	-30	-40	-50	-60	-70
E2	2	50	10	20	0	-42	-34	-26	-18	-10
E3	1	70	15	35	0	-51	-32	-13	6	25

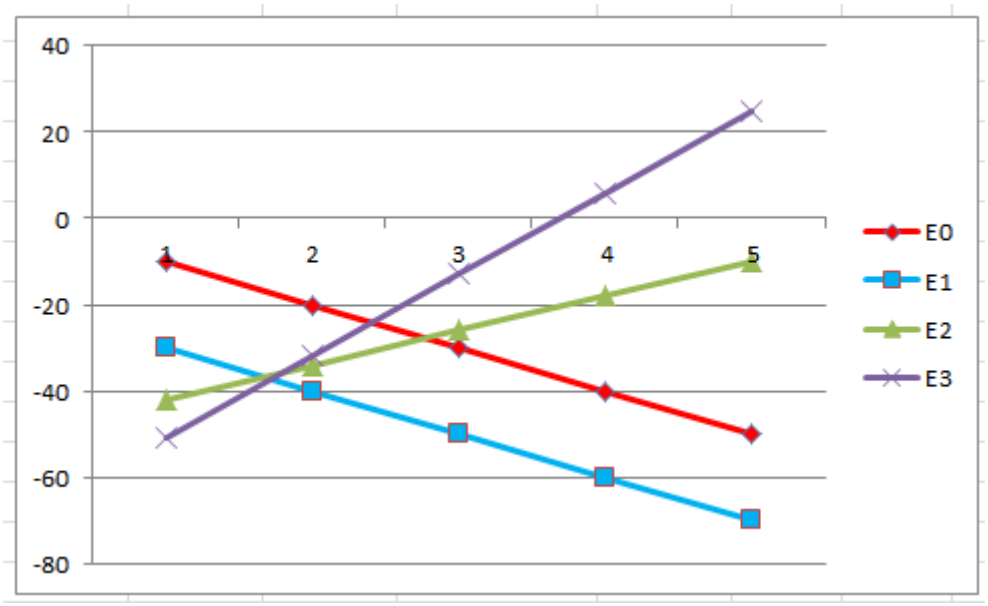

Figure 14. Examples of risk management decisions

- In scenario EO, the (estimated) loss per year is known.
- Scenario E1 looks like a bad idea since it adds expenses to the first year, but this expenditure is not recovered in future years.
- Scenario E2 is different; a higher initial payment is made, but it is profitable from the fourth year onwards.
- Even more appealing is scenario E3, where an even higher initial payment leads to savings from the third year onwards and operational profits starting the fifth year. Scenario E3 can be considered a good investment.

19 This entry may be positive or negative. Positive if the organisation improves its efficiency. Negative if it decreases. As a classical example of safeguards that improve productivity, consider replacing passwords with authentication tokens. As an example of safeguards that reduce productivity, consider an information classification scheme with strong access control.

20 Axis X shows years. Axis Y shows cost in unspecified units.

4.1.5. Qualitative study of costs and benefits

When a qualitative analysis is made, the costs/benefits balance shows intangible aspects that hinder calculating a break-even point.

These intangible aspects include:

- aspects related to image/reputation
- aspects related to the competence: comparison to other organisations in the same field
- compliance with regulations, either on a voluntary or compulsory basis
- capability to operate
- productivity

These considerations lead us to consider different scenarios in order to determine the net balance. For instance, if measures are not adopted, we could be exposed to a certain risk, and this could lead us to give a bad image, but if the preventive solution also gives a bad image or leads to a relevant loss of opportunity or productivity, a balance has to be found through a combination of measures.

4.1.6. Mixed study of costs / benefits

When only qualitative risks are analysed, the decision is made taking into account the balance between costs and intangible benefits, although a calculation of the solution costs must be made and checking whether those costs can be afforded. Otherwise, the proposed solution would not be a solution. Thus, an economic filter should be applied before choosing the best option.

4.1.7. Risk treatment options: elimination

Eliminating the source of risk is an option when we are facing a non-acceptable risk.

Several things could be eliminated from a system, provided that it does not affect the essence of the Organisation. Eliminating essential information or services is almost impossible, since they are the core mission of the Organisation. Changing these assets would entail reorienting the mission of the Organisation.

It is more feasible dealing without non-essential components, which are in place only to implement the task but are not an essential part of it. This option could adopt different ways:

- Elimination of certain kind of assets, replacing them with others. For instance, changing the operational system, the equipment's manufacturer, …
- Restructuration of the system's architecture (that is, dependencies) in order to alter the added value of certain assets exposed to big threats. For instance: segregating networks, splitting teams to answer to particular needs, keeping the most valuable items as far as possible from threats …

The decision of eliminating sources of risk implies reassessing the risk of the new system.

4.1.8. Risk treatment options: mitigation

Risk mitigation refers to one of these two options:

- Reducing the degradation caused by a threat (sometimes the expression 'to delimit the impact' is used)
- Reducing the likelihood of that threat

In both cases, it is necessary to enhance or improve the safeguards, namely to upgrade them.

Some safeguards, particularly the technical ones, entail the deployment of more equipment[21] that becomes a system's asset. These new assets will also increase the system's value and be subject to threats that could damage essential assets.

21 An example of this could be a firewall, a system of management of private online networks, smart cards to identify users, a public key PKI, etc.

Therefore, the risk analysis should be repeated, including now the new deployment and checking that the risk of the new system is lower than the original one, that is to say, that safeguards do reduce risks within the Organisation.

4.1.9. Risk treatment options: sharing

The traditional term used was “to transfer risks”. Since transfers can be partial or total, we should talk of “sharing risks”.

There are two basic ways of sharing risks:

- Qualitative risks: They are shared by outsourcing system components, so as to share responsibilities: the technical ones for those who operate the technical components and the legal responsibilities, as envisaged in the agreement to provide the service.
- Quantitative risks: they are shared through insurances, so that by means of a fee, the policyholder reduces the impact of potential threats and the insurer accepts the consequences. There are multiple kinds of insurances and clauses that specify the degree of responsibility of each part.

When risks are shared, all the components of the system and their assessment change and a new analysis of the resulting system is necessary.

4.1.10. Risk treatment options: funding

When a risk is accepted, the Organisation should reserve funds in case the risk should materialize to face its consequences. Sometimes they are called “contingency funds”; in other cases, they will be part of insurance contracts.

This option does not usually entail any change in the system and the available risk analysis is enough.

4.2. Formal activities

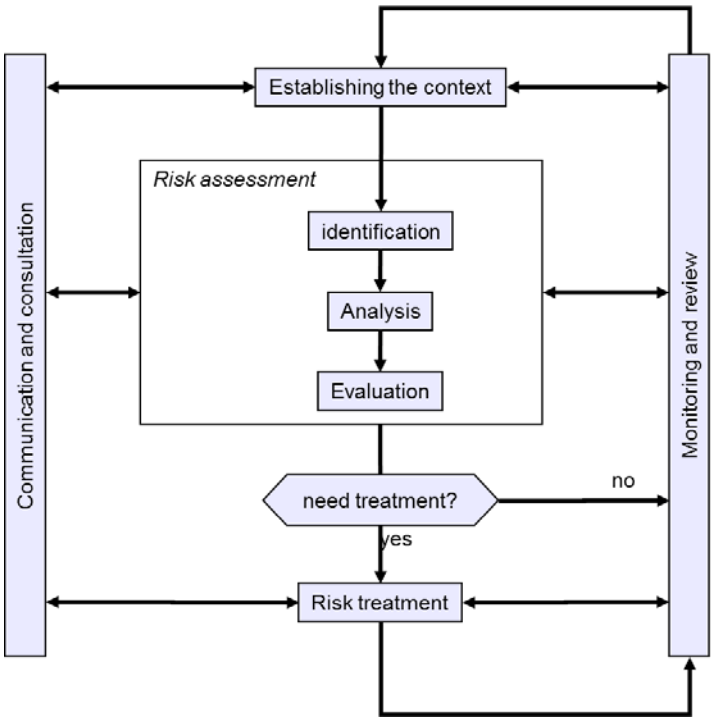

Figure 15. Risk management process

4.2.1. Roles and functions

Several actors take part in the process of risk management. We will try to identify them and briefly explain their functions and responsibilities.

Governing bodies

This level includes those corporate or individual bodies deciding the mission and objectives of the Organization.

This category usually includes the senior positions of these bodies.

You will often see at this level a Committee of Information Security.

These bodies are the ultimate authority to accept risks. They are considered the “risk owners”.

Executive Board

This level includes those corporate or individual bodies taking decisions which specify how to achieve the business goals set by government bodies.

This category usually includes those responsible for business units, responsible for service quality, etc.

Operational Directorate

Corporate or individual bodies that make decisions to implement the indications suggested by the Executive Board.

This category includes those responsible for operations, production, exploitation, etc.

National Security Framework

The Spanish National Security Framework identifies some roles that may be involved in the process of risk management:

Responsibility for the information

Governing level. This role is accountable for the security requirements of each piece of information managed by the system.

Personal information and information marking are usually part of this role.

Quite often, this role is exercised by the Information Security Committee.

Responsibility for the service

It may be governing level or managing level. This role is accountable for the required levels of service.

Quite often, this role is exercised by the Information Security Committee.

Responsibility for the security (CISO – Chief Information Security Officer)

Usually at executive level, working as a mechanism between the guidelines laid down by those responsible for information and services and the responsible for the system. At the same time serves as supervisor of the system operation and reports to the Information Security Committee.

Integral to the risk management process, it is the person that

- translates the value of essential assets into operation elements,
- approves the statement of applicability of safeguards,
- validates operational procedures,
- translates residual risks to risk owners, and
- validates security plans.

According to this informant role, this is the person in charge of developing metrics and indicators to measure system security.

Responsibility for system operation or production

At operational level. Decisions related to: system architecture, procurement, facilities and daily performance.

As far as risk management is concerned, this is the person who suggests the security's architecture, applicability of safeguards, operational procedures and security plans. This is also the person accountable for the implementation and adequate operation of safeguards.

Administrators and operators

They are the people responsible for implementing the daily actions of system operation according to the instructions received from his superiors.

RACI matrix

The matrix below is approximate and should be adapted to each particular organisation.

The responsibility allocation Matrix (which acronym is RACI) is usually used in project management methodologies to match activities and resources (individuals or working teams). This way, each activity is assigned to an individual or collective.

	role	description
R	Responsible	Those who do the work to achieve the task. There is at least one role with a participation type of *responsible*, although others can be delegated to assist in the work required (see also *RASCI* below for separately identifying those who participate in a supporting role).
A	Accountable	The one ultimately responsible for the correct and thorough completion of the deliverable or task, and the one who delegates the work to those *responsible*. In other words, an *accountable* must sign off (approve) on work that the *responsible* provides. There **must** be only one *accountable* specified for each task or deliverable.
C	Consulted	Those ones whose opinions are sought, typically subject matter experts; and with whom there is two-way communication.
I	Informed	Those who are kept up-to-date on progress, often only on completion of the task or deliverable; and with whom there is just one-way communication.

Table 5. Roles

Task	Direction	RINFO	RSERV	RSEG	RSIS	ASS
Security levels required by information		A	I	R	C	
Security levels required by the Service		I	A	R	C	
Risk analysis		I	I	A/R	C	
Statement of applicability		I	I	A/R	C	
Acceptance of residual risk	I	A	A	R	I	
Implementation of security measures		I	I	C	A	R
Status of security measures				A	C	R
Supervision of security measures	I	I	I	A	I	R
Status of the system's security				A	C	
Plans to enhance security				A	C	
Awareness and training plans				C	A	
Continuity plans				C	A	

Table4. RACI matrix –Tasks releted to risk management

Being

Direction – Top Management, governing bodies

RINFO – Responsibility for the information

RSERV – Responsibility for the services

RSEG – Responsibility for the security

RSIS – Responsibility for system operation

ASS – Security administrators

4.2.2. Context

The context where the organisation operates must be taken into account: cultural, social and political background. It includes both national and international aspects, depending on where the activity of the Organisation takes place.

Legal, regulation and contractual obligations should be identified. For instance, obligations related to

- Personal data processing,
- Handling classified information,
- Handling information and products with copyright
- Provision of public services
- Critical infrastructures
- etc.

You have to identify the environment in terms of competition and competitive positioning with respect to competitors.

The internal situation of the organisation should be identified: the internal policy, the commitment with stakeholders and with workers or their representatives.

The context where risk management takes place must be constantly reviewed in order to adapt to changing circumstances.

4.2.3. Criteria

Many aspects related to risks are subject to estimations. Estimations should be as objective as possible or, at least, they should be repeatable, explainable and comparable.

It is advisable to establish assessment scales in order to:

- Assess information security requirements
- Assess the requirements on service availability
- Estimate the likelihood of a threat
- Estimate the impact of a security incident
- Estimate the risk level basing on impact and likelihood estimations
- … (see “Book II – Catalogue of Elements”)

Some rules and/or criteria should be considered when taking decisions:

- Impact thresholds
- Likelihood thresholds
- Impact and likelihood combined thresholds
- Risk level thresholds

- Impact on the reputation of the Organisation or its managers
- Impact on the competitive position
- Impact compared to other risk areas: financial, regulatory, environmental, industrial security, etc.
- combinations of risks that could have a joint effect
- Particularly sensitive threats (either due to technical reasons, because of their uncertainty or because its occurrence would cause a large social alarm with a serious impact on the reputation or the continuation of the Organisation's operations, even if the technical or material consequences are scarce)
- …

4.2.4. Risk assessment

The guidelines described in the previous chapter are applied.

It would be very useful to carry out a specific risk analysis the first time this activity is carried out. See the following chapter.

4.2.5. Decisions on treatment

As mentioned above, there are different options to deal with risk:

- Eliminating risk by eliminating its causes: handled information, provided services, system's architecture,
- reducing or limiting the impact
- reducing the likelihood of threats
- in the case of threats stemming from defective products (technical vulnerabilities): repairing the product (for instance, applying manufacturer's patches)
- introducing new safeguards or upgrading the existing ones
- outsourcing certain parts of the system
- taking insurances

Sometimes, the decision entails accepting a risk increase:

- accepting working with new information or providing further services
- altering the system's architecture
- reducing safeguards
- reducing safeguards' quality (allocating less resources)

Ultimately, some residual risk shall be accepted; therefore, some funds should be kept aside to deal with any contingency.

4.2.6. Communication y consultation

Before taking any decision on how to manage a risk, it should be understood what the system is used for and how it is used.

This entails maintaining a fluent contact with several actors

- Governing and decision bodies, since every decision should be in line with the Organisation's mission
- Systems' users and technicians, since every decision must take into account its impact on the system's productivity and use
- Providers, since their cooperation is essential for any decision.

We must bear in mind that any security measure entailing a loss of productivity, a hindrance to the system's operational capability or requiring thoroughly trained users is doomed to failure.

Every measure must be

- Backed by the Management
- Covered by the Organisation's security policy
- Backed by clear and highly disseminated regulation
- Briefly and clearly explained in security operational procedures

Finally, the presence of indicators showing approval rate among users is desirable to identify both the level of compliance and the problems derived from its observance.

4.2.7. Monitoring and review

Risk analysis is a formal exercise based on numerous estimates and assessments that might not match reality. It is absolutely necessary for the system to be under continuous monitoring. The indicators of potential risk and impact are useful to decide which items should be monitored.

An early detection system should be prepared for potential incidents (on the basis of predictive indicators) as well as a reaction system to security incidents.

A set of Key Risk Indicators (KRI) should be obtained. These indicators:

- are proposed by the Security Officer;
- its definition is agreed upon by the Security Officer and the owner of the risk; the definition will indicate exactly:
  - what measures are they based on,
  - what is the calculation algorithm,
  - periodicity of assessment and
  - threshold of warning and alert (urgent attention)
- are presented to the appropriate officer
  - routinely, with the periodicity agreed,
  - occasionally, at request of the owner of the risk measured,
  - and extraordinarily when a threshold of risk is exceeded
- these indicators will be at the auditors' disposal

The owner is responsible for monitoring risk; the function can be delegated on the daily work, but control of the situation shall be regained when measures have to be taken in order to contain a risk that exceeds tolerance.

Whenever reality differs from our estimates, we should revise the analysis and the decisions of treatment.

Outsourced services

When we depend on third parties, it is particularly important to know the performance of our providers, both with a good system of reporting, escalation and resolution of security incidents, and the establishment of predictive indicators. From the analysis of dependences made during the risk analysis, we receive information about to which extent and security range we depend on each external provider. From this information, we find out which elements should be monitored so that we make sure they meet our security requirements.

4.3. Documentation of the process

Internal documents

- Definition of roles, functions and reporting schemes
- Criteria to assess information
- Criteria to assess services
- Criteria to assess risk and impact scenarios

Documents for others

- Security Plan

4.4. Control indicators in the risk management process

√	**Activity**	**task**
	Roles and responsibilities concerning risk management have been defined	4.2.1
	The context of risk management has been established	4.2.2
	The criteria of risk assessment and treatment decision-making process have been established	4.2.3
	Residual risks have been interpreted in terms of impact on the business or mission of the Organisation	4.2.4
	Options of treatment of residual risks have been identified and assessed (proposal for security programs)	4.2.5
	Government bodies have adopted a risk treatment proposal — avoid the risk — prevent: mitigate the likelihood that it will happen — mitigate the impact in case it occurs — share the risk with a third party — assume the risk	4.2.5
	Resources to undertake the security plan have been planned	4.2.5
	Resources to meet contingencies have been planned	4.2.5
	Decisions have been communicated to the involved parties	4.2.6
	There is a continuous monitoring system to detect deviations in the risk analysis assumptions	4.2.7
	Procedures and rules have been established to deal with deviations from the risk analysis assumptions	4.2.7

5. Risk analysis projects

Risk analysis activities are recurrent since analysis has to be under continuous review and update. Let us call 'marginal risk analysis' to the outputs of these activities that, usually, require little workload in each iteration.

But, before moving into marginal iterations, a whole analysis is essential to serve as a working platform. This occurs the first time a risk analysis is made and whenever the policy of the organisation establishes that a new platform should be created, either due to formal reasons, or because the accumulated changes justify a complete revision.

When a risk analysis is started from scratch, a series of substantial resources are used and these activities should be scheduled within a project, either internal or outsourced to an external consultancy.

Considerations to be taken into account to make this project success are presented in this section.

RAP.1 – Preliminary activities

RAP.2 – Development of the risk analysis

RAP.3 – Communication of results

5.1. Roles and functions

During the execution of the project some specific roles are frequently established to carry out the project successfully.

Follow-up Committee

It is made up of the heads of the units involved in the project; as well as those responsible for computers and management within these units. The participation of common services of the Organisation (planning, budget, human resources, administration, etc.) will also be useful. Anyhow, the composition of the committee depends on the characteristics of the units involved.

The duties of this committee are the following:

- dealing with incidents during the development of the project
- ensuring the availability of manpower with appropriate profiles and their participation in the activities where their cooperation is needed
- approving intermediate or final reports of each milestone
- developing final reports for the executive committee

This committee is usually appointed by the Information Security Committee, and it reports on the progress of the project. Sometimes the Follow-up Committee is a sub-committee of the Information Security Committee.

Project team

Made up of experienced staff on information systems and technologies and qualified technical personnel of the field involved. Knowledge of security management in general and the application of the methodology of analysis and risk management in particular are needed. If the project requires technical assistance from external contracting, the personnel expert on information systems security will be integrated this project team.

The responsibilities of this team are the following:

- performing the project tasks
- gathering, processing and consolidating data

- developing the reports

The Project Team reports to the Follow-up Committee through the Project Manager.

Contact persons

It consists of representative users within the units affected by the project:

- People responsible for service, aware of the Organisation's mission and its strategies in the middle and long term
- People responsible for internal services
- Personnel in charge of exploiting and operating computing services, aware of the deployed means (production and safeguards) and incidents that are usual

Besides these corporate bodies, it is necessary to identify some singular roles:

Promoter

It is a singular figure that leads the first tasks of the project, outlining the opportunity and scope to launch the risk analysis project itself.

It should be a person with a global view of the information systems and their role in the Organisation's activities, without necessarily knowing the details, but being aware of the incidents.

Project Director

It should be a senior manager, with responsibility for security within the Organisation, information systems, or failing that, with responsibilities concerning planning, coordination or similar areas, services or matters.

It is the visible head of the project team and interlocutor to the Organisation's Security Officer.

Operational Liaison

It will be a person within the Organisation with a good knowledge of the individuals and units involved in the project, with the capacity to link the project team with the users.

It is the visible interlocutor of the follow-up committee with user groups.

It is worth recalling that a risk analysis project is always mixed due to its own nature; that is, it requires permanent cooperation of experts and users both in the preparatory stages and in its development. The figure of the operational liaison acquires a permanent importance that is not usual in other type of more technical projects.

The risk analysis project is carried out through the following tasks:

RAP – Risk Analysis Project
RAP.1 – Preliminary activities
RAP.11 – Study of timeliness
RAP.12 – Definition of the scope of the project
RAP.13 – Project planning
RAP.14 – Project launch
RAP.2 – Development of the risk analysis
RAP.3 – Communication of results

5.2. RAP.1 – Preliminary activities

RAP.11: Study of timeliness

Timeliness to perform the risk analysis project, just now, is justified, framing it within the development of the other activities of the Organisation.

The result of this activity is the report called “preliminary”.

RAP.12: Definition of the scope of the project

The project’s final objectives, reach and limits are defined.

The result of this activity is a profile of the risk analysis project.

RAP.13: Project planning

Estimated workloads. Project progress is usually marked by a series of interviews with the contact persons who know the information on an asset or group of assets of the system under analysis. The interviews to be carried out to collect information are scheduled: who will be interviewed. The work schedule is drafted to perform the project.

In this activity, participants are decided and the different groups and committees are structured to perform the project.

The result of this activity is formed by:

- A work schedule for the project
- Working procedures

RAP.14: Project launch

Questionnaires to collect information are adapted to the current project. The criteria established within the Risk Management Process are the starting point.

An information campaign is also carried out to sensitize those affected about the objectives and requirements of their participation.

The result of this activity is formed by:

- The questionnaires for the interviews
- The catalogue of types of assets
- The list of security dimensions and
- The valuation criteria

5.2.1. RAP.11: Study of timeliness

RAP: Risk Analysis Project ***RAP.1: Preliminary activities*** ***RAP.11: Study of timeliness***
Objectives • Identify or attract interest of the Organisation’s Management in carrying out a risk analysis project
Inputs

RAP: Risk Analysis Project ***RAP.1: Preliminary activities*** ***RAP.11: Study of timeliness***
Outputs • **Preliminary report** advising to perform the project • Awareness and support of the Management to address the project • Establishment of the follow-up committee
Techniques, practices and guidelines
Participants • The promoter

The Management is usually aware of the advantages provided by the electronic, computer and telematics techniques to its performance; but it is no so usually aware of the security problems these techniques involve, or the legal obligations or regulations they are affected by.

In any public or private Organisation, it is important to transform into action the increasing concern for the lack of security of the information systems. Since its effects not only affect those systems, but the actual functioning of the Organisation and, in critical situations, to his own mission and survivability.

Development

The initiative to perform a risk analysis project starts from a promoter, from inside or outside the Organisation, aware of the problems related to the information systems' security, like:

- Continuous incidents related to security.
- Lack of foresight in issues related to the assessment of needs and means to reach an acceptable security level of information systems compatible with the right fulfilment of the mission and tasks of the Organisation.
- Restructuring in the products or services provided.
- Changes in the technology used.
- Development of new information systems.

The promoter may draft a framework-questionnaire (document difficult to systematize, to be created in each case) to provoke reflection on aspects of security of information systems by:

The heads of the operational units (responsible for services).

The questionnaire allows to make an informal study of the situation concerning the security of their information systems; they should be able to express their opinion about the security projects already carried out (with their level of satisfaction or their limitations), as well as their expectations from a risk analysis project[22]. This high-level approach provides a first view of the specific objectives and the options that should underlie the performance of the project.

Operations managers

The questionnaire provides a technical overview to draft the project and allows tackling the study of timeliness to perform it, after integrating the previous options.

22 Most likely, its meaning will be unknown and the framework-questionnaire should include a short explanation of what it is and the objectives pursued by the risk analysis in general and the project in particular.

From the answers to the framework-questionnaire and the interviews held with the above-mentioned heads and collectives, the promoter obtains a first approach to the tasks, services and products involved in issues related to the information system security, their geographical location, the technical means, human means, etc.

Based on all these elements, the promoter drafts the **preliminary report** recommending the preparation of the risk analysis project and including the following elements:

- Presentation of basic arguments.
- List of precedents concerning the information system security (Strategic Plan, Action Plan, etc.).
- First approach to the reach of the project according to:
  - the objectives of the units or departments
  - the managerial or technical orientations
  - the structure of the Organisation
  - the technical environment.
- First approach to the means, both human and material, to carry out the project.

The promoter presents this preliminary report to the Management, which can decide:

- to approve the project as is, or
- to modify its reach and/or its objectives, or
- to postpone the project.

5.2.2. RAP.12: Definition of the scope of the project

Once the timeliness to carry out the project has been checked and the Management's support has been confirmed, this activity assesses the project planning elements, that is, the participants and their workloads.

In the assessment one should consider the possible existence of other plans (for example, a general Strategic Plan of Information Systems or Security Plan in the units that can be involved or in the Organisation) and the period of time considered for the implementation of the project. Particularly, the existence of a Strategic Plan of Information Systems for the units that can be affected within the Organisation could determine to a large extent the scope and extension of the activities carried out in this activity.

RAP: Risk Analysis Project ***RAP.1: Preliminary activities*** ***RAP.12: Definition of the scope of the project***
Objectives • Determining the objectives of the project, with short- and middle-term deadlines • Determining the general limitations imposed on the project • Determining the domain, scope or perimeter of the project • Determining the domain, scope or limits of the project
Inputs • Compilation of the Organisation's appropriate documents

RAP: Risk Analysis Project
RAP.1: Preliminary activities
RAP.12: Definition of the scope of the project

Outputs

- Detailed specification of the project's objectives
- List of general limitations
- List of the Organisation units that will be affected as part of the project
- List of relevant roles in the units involved within the scope of the project
- The essential assets
- The interconnection points with other systems
- The external suppliers

Techniques, practices and guidelines

- Interviews (see "Guide of Techniques")
- Meetings
- *31010:B.1: Brainstorming*
- *31010:B.2: Structured or semi-structured interviews*
- *31010:B.3: Delphi technique*

Participants

- The follow-up committee

A risk analysis project can pursue very short-term objectives like guaranteeing a certain system or certain business process, or it can pursue much wider objectives like the global analysis of the Organisation's security. Anyhow, it has to be specified.

Particularly when taking correcting actions, one should bear in mind that "not everything is allowed"; the project will face a number of restrictions, not necessarily technical, that establish a framework to abide by. To include the restrictions in the risk analysis and management, these are grouped by different concepts, typically:

Managerial or political restrictions

Typically of government bodies or organisations closely linked with government bodies, either as providers or services' suppliers.

Strategic restrictions

Derived from the scheduled evolution of the Organisation's structure or objectives.

Geographical restrictions

Derived from the physical location of the Organisation or its dependence from communications physical means. Islands, locations abroad, etc.

Time restrictions

That take into consideration temporary situations: labour conflicts, international crisis, change of ownership, process re-engineering, etc.

Structural Restrictions

Taking into account the internal structure: decision making processes, international head offices they are attached to, etc.

Functional Restrictions

Considering the objectives of the Organisation.

Legal Restrictions

Laws, specific rules and regulations, external and internal contracts, etc.

Restrictions related to the staff

Working profiles, contractual obligations, union commitments, professional careers, etc.

Methodological Restrictions

They depend on the nature of the Organisation, its habits or working procedures, which may impose a specific way to do things.

Cultural Restrictions

The “culture” or internal working procedures should coexist with other theoretically ideal safeguards.

Budgetary Restrictions

Total money needs, as well as budget execution plan.

Scope

This task identifies the units included in the project, specifying the general data of those units regarding their managers, services provided and geographical location. It also identifies key relations of the project units with other entities, namely the exchange of information using different media, access to common computing media, etc.,

This task rests on a basic principle: risk analysis and management should focus on a limited scope, which may include either several units or just one (depending on the complexity and type of problem to tackle); a too extensive/undefined project may be impossible to deal with, because either it is too general or lasts for too long, thus being detrimental for the estimated analysis items.

The following items should be specified to state the scope of the project:

- **Essential assets**: information handled and services provided
- **Interconnections** to interrelate with other systems, making it clear what information is exchanged and what services are provided on a mutual basis.
- **External suppliers** used by our information system.

5.2.3. RAP.13: Project planning

RAP: Risk analysis project
RAP.1: Preliminary activities
RAP.13: Project planning

Objectives

- Defining the points of contact in each unit
- Planning interviews to collect information
- Identifying the resources required by the project: human, time and financial resources.
- Drafting a definite timetable for the completion of the different stages, activities and tasks of the project.
- Setting a monitoring schedule defining approximate dates for the meetings of the steering committee, a delivery plan for the products of the project, possible changes in the objectives, etc.

RAP: Risk analysis project *RAP.1: Preliminary activities* *RAP.13: Project planning*
Inputs • Results of the activity RAP.12; defining the scope of the project
Outputs • List of points of contact • Agenda of interviews • Report on resources required • Report on workloads
Techniques, practices and guidelines • Project planning
Participants • The project director • the follow-up committee

The agenda of interviews should specify the person to be interviewed, when and what for. This plan determines the load that the project will mean for the affected units, either internal or external.

The agenda of interviews is especially relevant when the persons to interview are located in different places and making the interview involves travelling for one or both parties.

It is also advisable to arrange the interviews in such a way that technical opinions are collected first and later on managerial ones, so that the interviewer may change the questions depending on developments (historical record) rather than on assessments and prospects of services.

5.2.4. RAP.14: Project launch

This activity completes preparatory tasks. First, it selects and adapts the questionnaires used to collect data and carries out an awareness campaign among those involved.

RAP: Risk analysis project *RAP.1: Preliminary activities* *RAP.14: Project launch*
Objectives • Having the necessary working elements to undertake the project
Inputs • Working framework established in the Risk Management Framework: criteria and relations with the parties involved
Outputs • Adapted questionnaires

RAP: Risk analysis project ***RAP.1: Preliminary activities*** ***RAP.14: Project launch***
• Determining the catalogue of assets • Determining asset assessment dimensions • Determining asset assessment levels, including a common guide of criteria applied to assign a level to a specific asset • Determining threat assessment levels: likelihood and degradation. • Allocating the relevant resources (human, organisational, technical, etc.) to materialize the project • Reporting the units involved • Creating an atmosphere of general awareness of the objectives, responsibilities and deadlines.
Techniques, practices and guidelines • Questionnaires (See "Catalogue of Elements")
Participants • Project manager • Project team

Questionnaires used to collect information are adapted to the objectives of the project, its scope and the subjects that should be discussed in detail with users.

Questionnaires are adapted so as to rightly identify working elements: assets, threats, vulnerabilities, impacts, existing safeguards, general restrictions, etc. taking into account the requirements of activities RAM.1 (asset description), RAM.2 (threat description) and RAM.3 (safeguard description).

There is always the need for adaptation (given the enormous variety of security problems that Magerit can and should address). However, the extent of adaptation also depends on the conditions of questionnaire exploitation. Interviews made by security experts will not undergo the same level of adaption as questionnaires made by the manager of the system or by the information systems users.

5.3. RAP.2 – Development of the risk analysis

The stages described in chapter 3 above are followed.

Most of the tasks will require two/three interviews with the relevant interlocutors:

- A first interview to explain the needs and collect data
- A second interview to verify that there are no missing data and that they were correctly understood.
- Depending on the circumstances, an additional interview may be necessary if verification shows many doubts or inaccuracies.

When doing all these tasks, the documents handled should be in written and follow a formal management procedure; namely, they should be approved and include continuous revision procedures. Oral and informal information should just be used to facilitate understanding, and should not transmit relevant data that are not included anywhere else.

5.4. RAP.3 – Communication of results

The conclusion of the analysis stage entails the beginning of the treatment stage. In order to make decisions regarding treatment, it is necessary to know both potential and residual indicators of impact and risk. For each risk scenario it is necessary to have information enough to understand the nature of risk, its dynamics and the arguments or basis of the estimations used to derive results. Knowing the final value of the indicator does not suffice; rather, the reason for that value should be analysed.

Moreover, decisions regarding treatment may require a modification of the risk analysis. It is often necessary to analyse different hypothetical scenarios (what if …?) to choose one decision or another. Therefore, it is critical to have tools to automate the calculus.

For the final executive report, graphically emphasize enough scenarios greatest impact, high level of risk and dangerous combinations of both indicators(see quadrants or areas above).

5.5. Project control

5.5.1. Milestones

Control Milestone M1.1:

The Management will either authorize or reject the execution of the risk analysis project, on the basis of a timeliness assessment made by the promoter.

Control Milestone M1.2:

The committee that follows up the project will validate the report "Risk Analysis Project Planning" including a summary of the results of activities carried out.

5.5.2. Output documents

Intermediate Documents

- Results of the interviews.
- Documents from other sources: statistics, comments made by experts and comments made by analysts.
- Additional documents: maps, organisation charts, requirements, specifications, functional analysis, burden notebooks, user manuals, exploitation manuals, information flow and process diagrams, data models, etc.
- Analysis of results, detecting critical areas.
- Existing information of possible use for the project (namely, asset inventory)
- Results of possible implementation of risk management and analysis methods previously used (namely cataloguing, grouping and evaluation of assets, threats, vulnerabilities, impacts, risk, safeguards, etc.).

Final Documents

- Value Model: identification of assets and dependencies; own and accumulated value.
- Map of threats, their consequences and likelihood
- Document of safeguard applicability.
- Assessment of the effectiveness of existing safeguards.
- Report on shortages or weaknesses of the safeguard system in place.
- Indicators of impact and risk, both potential and residual.

6. Security plan

This section deals with the implementation of security plans envisaged as projects aimed at implementing the decisions made to manage risks.

These plans are given different names under different backgrounds and circumstances:

- Plan to enhance security
- Security Master Plan
- Security Strategic Plan
- Adaptation Plan (this is the name used within the ENS)

Three tasks are identified:

SP –Security Plan
SP.1 – Identification of security projects SP.2 – Implementation plan SP.3 – Implementation

6.1. SP.1 – Identification of security projects

The decisions made regarding how to treat risks become specific actions.

SP: Security plan ***SP.1 – Identification of security projects***
Objectives • Drafting a harmonized set of security programs
Inputs • Results of risk analysis and treatment activities • Knowledge of security techniques and products • Catalogues of security products and services
Outputs • Results of risk analysis and treatment activities • Knowledge of security techniques and products • Catalogue of security products and services
Techniques, practices and guidelines • Project planning
Participants • The project team • Security experts • Experts in specific security fields

Ultimately it comes to implement or improve the implementation of a series of safeguards to meet residual impact or risk levels determined by the Management. This treatment results in a series of

tasks to be done. A security program is a group of tasks. Groups are created on suitability grounds, either because parts would not be efficient on their own, or they have a common objective, or because they all fall into the same action.

Each security program must detail the following:

- Its general objective.
- Specific safeguards to be implemented or improved, including its objectives regarding quality, efficiency and effectiveness.
- A list of impact and risk scenarios faced: assets involved, types of assets, threats faced, and assessment of assets, threats, and impact and risk levels.
- Which unit will implement the program
- Estimated cost, both economic and regarding the implementation effort, taking into account the following:
  - Costs of procurement (of products); hiring (of services), or development (of immediate solutions), where it may be necessary to explore different alternatives
  - Initial implementation and maintenance costs
  - Cost of training provided to both operators and users, on a case by case basis
  - Cost of exploitation
  - Impact on the performance of the Organisation
- A list of subtasks to address, taking into account the following:
  - Regulatory changes and development of procedures
  - Technical solution: programs, equipment, communications and facilities,
  - Deployment plan
  - Training plan
- Estimated implementation time from the beginning to actual operation.
- Estimated risk status (residual risk and impact on completion).
- A system of efficiency and effectiveness indicators to know at any time the desired quality of performance of the security task and its temporary evolution.

The estimations above may be very precise in simple programs, while they may be just rough in complex programs that entail the development of a specific security program. In this case, each project will develop the final details through a series of specific tasks for that project which, generally speaking, will cover the following items:

- Market analysis: products and services available.
- Cost of a specific development, either done by the organisation or through outsourcing.
- If a specific development is deemed to be appropriate, the following should be determined:
  - Functional and non-functional specifications of the development.
  - The development process that guarantees the security of the new component
  - Measure mechanisms (controls) that should be built-in
  - Acceptance criteria
  - Maintenance plan: incidents and evolution

6.2. SP.2 – Implementation plan

SP: Security plan ***SP.2 – Implementation plan***
Objectives • Time schedule for security programs
Inputs • Outputs from risk analysis and treatment • Output from SP.1 Security programs
Outputs • Plan implementation time schedule • **Security Plan**
Techniques, practices and guidelines • Risk analysis (See “Risk Analysis Method”) • Project planning
Participants • Development department • Procurement department

Security programs shall be ordered on a time basis taking into account the following:

- the relevance, seriousness or convenience of the impacts and risks faced: programs that deal with critical situations are a priority.
- the cost of the program
- the availability of the organisation’s staff to manage the tasks scheduled and implement them, if necessary.
- other factors, such as the annual budget of the organisation, relations with other bodies, legal, regulatory or contractual changes, etc.

A security plan is usually planned at three detail levels:

Master plan (one)

Often called “strategic plan”; it covers a long period of time (usually 3 to 5 years), and identifies the guidelines that should be followed.

Annual plan (a series of annual plans)

It covers a mid-period of time (usually 1 to 2 years) and deals with the planning of the security programs.

Project plan (a set of projects and their planning)

It covers a short period of time (usually less than a year) and specifies a detailed implementation plan for each security program.

A single strategic plan (1) should be developed. It gives an overview and unity of purpose of specific actions. This strategic plan facilitates the development of annual plans that help budget and resources allocations for the execution of the different tasks. Finally, the security programs will materialize into different projects.

6.3. SP.3 – Implementation

SP: Security plan ***SP.3 – Implementation***
Objectives • Achieving the objectives set in the security plan for each planned project.
Inputs • Results of SP.1 (security projects) and SP.2 (planning) • Security project
Outputs • Implemented safeguards • Rules for use and operational procedures • System of indicators of efficiency and effectiveness in the performance of the security objectives. • Updated value model • Updated map of risks • Updated risk status (residual risk and impact).
Techniques, practices and guidelines • Risk analysis (see “Risk Analysis Method”) • Project planning
Participants • Project team: evolution of risk analysis • Experts in the specific safeguards

6.4. Security plan control list

√	**description**	**task**
	The relevant projects have been defined	SP.1
	Interrelation between projects has been identified (a project should progress to allow another project to progress)	SP.1
	Resources have been allocated — available for ongoing projects — estimated for future projects	SP.2
	Roles and responsibilities have been identified	SP.1
	An implementation agenda has been drafted	SP.2
	Progress indicators have been defined	SP.3
	Awareness and training requirements have been identified	SP.1
	Documents required: — Security policies — Security operational procedures	SP.1

7. Development of information systems

Applications *(*software*)* are a frequent type of asset for processing 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 occur. Sometimes, moreover, the applications are part of the answer in the sense that they form a safeguard 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 the development process itself during its development phase, 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.

The National Security Framework envisages risk as a critical factor for the system security in several of its basic principles:

Article 5. Security as an integral process

1. Security must be understood as an integral process, constituted by all the technical, human, material and organisational elements related to the system. The application of the National Security Framework will be governed by this principle, which excludes any case-by-case or short-term ad-hoc treatment
2. Maximum attention will be paid to arousing awareness in the persons intervening in the process and their superiors in rank, so that neither ignorance nor a lack of organisation and coordination or inappropriate instructions are a source of risk for security.

Article 6. Security management based on risks

1. The analysis and management of risks will form an essential part of the security process and must be kept permanently updated.
2. Risk management will allow the maintenance of a controlled environment, reducing risks to acceptable levels. Reducing these levels will be achieved by deploying security measures to establish a balance between the nature of the information and the processes, the risks to which the information is exposed and security measures.

Article 9. Regular re-evaluation

The security measures will be re-evaluated and updated regularly, to adapt their efficacy to the ongoing evolution of the risks and protective systems, to the point of re-considering security, if necessary.

There are two types of activities:

- **ISS**: Information System Security: Activities relating to the own security of the information system.
- **DPS**: Development Process Security: Activities relating to security during the process of developing the information system.

7.1. 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. It may involve the removal of operational applications.
- The initiative may be taken by the development manager, with the security manager supervising it.

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. May involve the removal of operational applications.
- The process must be led by the development manager, with the security manager supervising it.

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 removal of operational applications.
- The process must be led by the security manager, with the systems manager supervising it.

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 removal of operational applications.
- The process must be led by the security manager, with the systems manager supervising it.

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 removal of operational applications.
- The process must be led by the security manager, with the systems manager supervising it

7.2. ISS – Information System Security

The whole lifecycle of an information system can be observed as stages with increasing specification: from an overall perspective during the planning processes down to a detailed view during development and use. However, this life cycle is not linear, rather it will often be necessary to try alternative options and review decisions made.

Risk and impact estimates from a risk analysis must be based on the reality of systems, specified on their assets. Consequently, the value model can be considered to be progressive comprising the detail level available at any time. As a methodology, Magerit provides systematic and homogeneous processing, essential to enable comparison between alternative options and drive system development.

Risk analysis must, as a basic principle, follow faithfully the reality of the information system and its context providing the best risk analysis possible to make the appropriate treatment decisions at any time.

7.2.1. Life cycle of applications

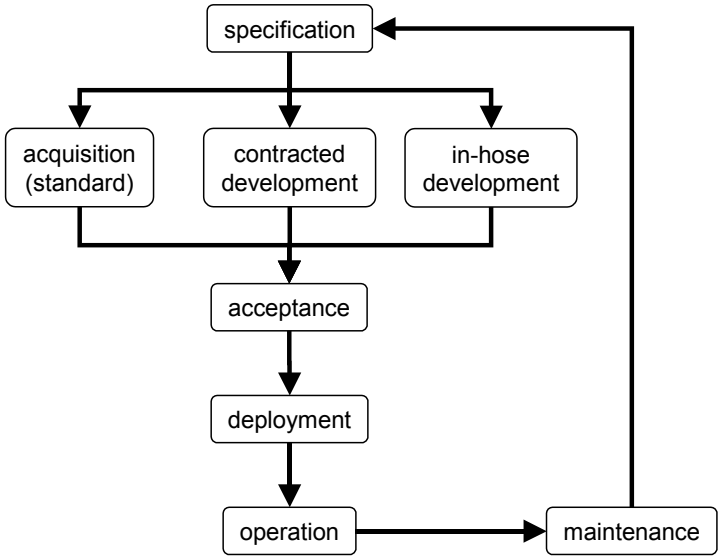

Figure 16. Lifecycle of software applications

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

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 application is used by the users and incidents are attended to by users and/or operators.

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.

MÉTRICA version 3

MÉTRICA version 3 is a methodology that offers organisations a tool to systematise activities providing support to the software life cycle. MÉTRICA identifies the following elements:

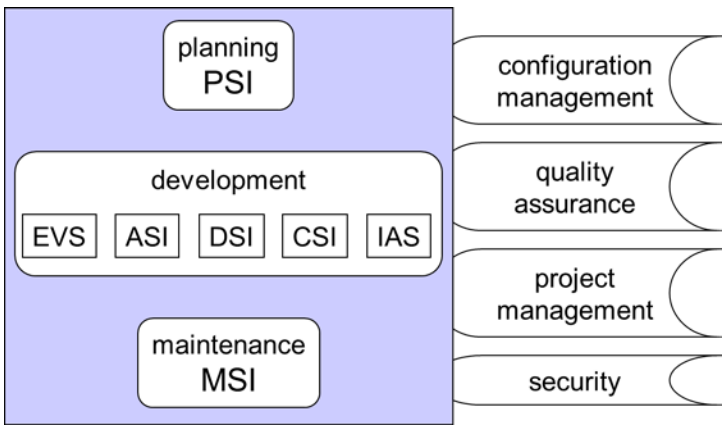

Figure 17. Métrica 3 – Activities

Métrica version 3

specification	PSI – Information System Planning EVS – System Feasibility Study ASI – Information System Analysis
acquisition or development	DSI – Information System Design CSI – Information System Construction
acceptance	IAS – System Introduction and Acceptance
deployment	
operation	
maintenance	MSI – Information System Maintenance

Table 7. Metrica 3: lifecycle and activities

7.2.2. Context

A general context must be identified:

- security policy and security guidelines
- regulatory compliance requirements
- contractual obligations
- roles and tasks
- information and services valuation criteria
- risk assessment criteria
- risk acceptance criteria

Particularly, operational procedures must be set up in order to implement communication between development tasks and risk analysis and treatment tasks.

- The Management establishes required levels of security for information and services
- The development team provides technical elements to materialize the application.
- The risk analysis team provides critical judgement about the system security.
- Management approves the residual risk.

7.2.3. Specification stage: information gathering

Information must be gathered regarding:

- essential information and its security requirements;
- essential services and their security requirements;
- the context the system is to be developed and used.

In particular, a threat profile shall be identified, whether they are natural, environmental or human threats, or accidental, deliberate threats. Characterizing the attackers' capabilities must be part of the design specifications, and modifying this design later on within the system life cycle will lead to another analysis and treatment decision.

7.2.4. Design stage: options analysis

Decision-making concerning risk treatment may lead to recommend safeguards assessing its influence on impact and risk indicators. Decisions made will depend on the criteria laid down in the organisation security policy, and other considerations particular to each different case. Although the security policy lays down a reference framework which must not be breached, it is not unusual for it not to provide for every technical and occasional detail regarding the service to make accurate decisions.

Given the interrelation among elements comprising a system, protecting certain types of assets in order to afford protection to the whole does not suffice. That is why decision-making on treatment occurs on one part of the system but it does not always entail an overall security analysis of the whole.

Risk analysis and treatment

The security that needs to be afforded to the information to be processed and services to be provided was established during the specification stage and cannot be modified now.

The risk development team and the risk analysis team work on a recurring basis until they hit a solution that suits both parties. It is usually the development team that takes the initiative and suggests a technical solution that meets the system functional requirements. The security team will then analyse the proposal informing about any associated risks and, where appropriate, suggesting safeguards for bringing risks down to acceptable levels. Whenever these suggested safeguards affect the design, the team will redo its proposal for a new analysis.

Safeguard specifications should include action mechanisms as well as configuration, monitoring, and efficiency and effectiveness control mechanisms. Some developments specifically focused on configuring the group of safeguards and monitoring its operation often come about.

The development team may submit two or more options. When this is the case, they will all be assessed for required risks and safeguards. A risk report will be yet another element to be taken into account when deciding what option to choose among the different available ones.

When both teams reach a stable situation that has a technical feasible design, acceptable risks and acceptable sources requirements, the proposal is submitted for approval.

The result of this stage will be technical development specifications together with a risk analysis and decisions on how to treat these risks.

7.2.5. Support to development: critical items

Safeguards approved within the design stage must be incorporated during development, as well as those controls for performance monitoring. These monitoring requirements usually involve:

- activity logs;
- mechanisms to process these records and to inform about protection system efficiency;
- triggering alarms when facts show that there is a security issue.

Deployment of these elements is modulated by the potential risk level undertaken by each one of the information system components.

During development, risks are better managed according to the guidelines indicated in “Security of the Development Process” section below.

7.2.6. Acceptance and implementation: critical items

Following approval of the system, and before it is implemented, all activity logs must be checked to ensure that they work properly; processing logs and alarms.

It must also be checked that the system design is as expected, particularly that safeguards have been deployed, deployment is effective, and that there is no possibility to get around them or avoid them; that is, that the system does not allow for backdoors beyond its control.

Identification and authentication:

- every access to the system requires user identification and authentication according to what has been established; any other access attempt must be blocked;
- identification and authentication mechanisms are protected to prevent hackers from accessing information or using mechanisms that jeopardize its effectiveness.

Access control:

- any access to information and services is previously verified to ensure that the user has all relevant authorizations;

Outsourced services: when part of the system operation is delegated to a third party:

- service contracts must be reviewed;
- completeness of incident reporting and management procedures must be reviewed.

If the system does not reflect the model whose risks have been analysed, it will be rejected and it will not go on to production.

Security documentation must be verified for clarity and accuracy. This includes policies, operational procedures, awareness and training material.

Although comprehensiveness is not possible, the following lines show acceptance testing that it is advisable to implement:

- testing data
  - whether they are real; they must be realistic;
  - if there is no other option but to use real data, copies and access must be kept under control
- operation testing (for security services)
  - attack simulation: verifying that they are detected and reported on;
  - testing during loading: verifying that protection measures are not avoided;
  - monitored intrusion (ethical hacking)
- services inspection / code inspection
  - information leaks: covert channels through registries, etc.;
  - access backdoors;
  - privileges escalation;
  - problems with buffer overflow.

7.2.7. Operation: dynamic analysis and management

Throughout the system operational life span, the operational scenario may change invalidating the risk analysis. Within formal environments, the system requires a re-accreditation in order to continue operating under new circumstances.

New threats

They occur either because new attack methods are devised or because the assessment of attackers' capabilities is modified. In these cases the analysis must be redone, and it must be decided how to deal with the new results.

Unexpected vulnerabilities

There may be, for instance, flaws reported by manufacturers. In these cases the new risk situation must be analysed and the appropriate treatment must be found in order to continue operation. Best

option is to patch the system; however, either because there is no patch available or because implementing it requires resources we do not have, we may find ourselves in a situation where we need to decide on the best way to treat an avoidable risk.

Security incidents

Security incidents could indicate a threat identification or assessment flaw. This calls for a review of the analysis.

A security incident can also involve a change in the system. For instance, an intrusion means that we cannot count on the peripheral defence: we have a new system with an attacker in a new location and having new options.

Changes in the way the system is used

Sometimes an already operational system is not being used as expected:

- new information having different security requirements;
- new services having different security requirements;
- new operational procedures.

In terms of risk analysis this means a new asset or deployed safeguards assessment.

The alteration of the system throughout any of the stages described above may lead to unacceptable risk levels making it necessary to implement a maintenance cycle to redesign the system or part thereof.

7.2.8. Maintenance cycle: marginal analysis

When a new amendment of the system is suggested, new elements should lead to a new risk analysis returning to the iteration cycles for proposals and solutions of the design stage.

7.2.9 Termination

When an information system is withdrawn from service, a number of security tasks should be carried out according to system risks. Specifically:

- protecting the value of information: retention and access control;
- protecting encryption and authentication keys: retention and access control.

Anything that does not need to be kept will be destroyed in a secure way:

- operational data;
- backup copies;
- system configuration.

7.2.10 Security documentation

Security documentation evolves throughout the system life cycle:

stage	security documentation
context	security policy is reviewed security policies are reviewed
specification	security policies are adapted
design	security operational procedures index is designed
development	security operational procedures are prepared
acceptance and implementation	security operational procedures are validated
operation	security operational procedures are updated
maintenance	security operational procedures are updated

Table5. Security documentation along software application lifecycle

7.3. DPS – Development Process Security

The information in this section applies to each one of Métrica's processes and sub-processes: PSI, EVS, ASI, DSI, CSI, IAS and MSI.

Métrica's security interface identifies up to four tasks that are repeated in each process. Here they are dealt with all together:

Assets to be taken into account

Each process requires a specific risk analysis taking into account:

- data:
  - systems specifications and documentation;
  - source code;
  - operator's and user's manuals;
  - testing data;
- software development environment:
  - document processing tools: creating, editing, document control, etc.;
  - code processing tools: creating, compiling, version control, etc.;
- development hardware: mainframes, workstations, archiving hardware, etc.;
- development communications;
- facilities;
- personnel involved: developers, maintenance personnel and users (testing).

Activities

The following steps are followed:

1. the development team presents the involved elements through the project leader;
2. the risk analysis team receives from the security manager the information about the assets involved;
3. the risk analysis team does the analysis;
4. the risk analysis team submits through the security officer the status of risks suggesting measures to be taken;
5. the development team prepares a report on the cost of the suggested measures including development costs and deviations in delivery times;

6. the Management assesses the risk and decides on what safeguards are to be implemented taking into account the joint risk analysis and suggested solutions cost report;
7. the risk analysis team prepares the reports on the solutions chosen;
8. the security team prepares the relevant security policies;
9. the Management adopts the plan to implement the system with the required security.

Risk analysis and management findings

In all instances:

- recommended safeguards;
- information processing policies and procedures.

Other considerations

Although the various processes require a specific risk analysis, it is true that models are extremely similar, and therefore the greatest effort will be made with the first model made because the others will be an adaptation of that first model.

Throughout the first processes, particularly for PSI, high level contributions may occur that will affect the Organisation's security policies and even the corporation security policy itself.

The need for document classification regulations and processing procedures are some of the arising rules and procedures that need to be highlighted.

Special attention to the personnel involved is required throughout all processes. As a basic rule it is convenient to:

- identify roles and people;
- describe the security requirements for each post and add them to the selection criteria and contract terms;
- restrict access to information: just when needed;
- separate tasks; in particular avoid tasking one single person with all those applications or part of an application supporting a high risk.

7.4. References

- "Seguridad de las Tecnologías de la Información. La construcción de la confianza para una sociedad conectada", E. Fernández-Medina y R. Moya (editores). AENOR, 2003.
- Metodología de Planificación, Desarrollo y Mantenimiento de sistemas de información. Métrica v3. Consejo Superior de Informática y para el Impulso de la Administración Electrónica, 2000.

8. 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.

8.1. Reach and depth

Magerit covers a very broad spectrum of users’ interests. The design of these guidelines has been based on a “maximum” criteria dealing with all kinds of assets, all kinds of security aspects; in short, all kinds of situations. In practice, the user may find situations where the analysis is more limited. Following are some common practical examples:

- only a review of files subject to personal data legislation is required;
- only a review of information confidentiality is required;
- only a review of communications security is required;
- only a review of outer perimeter security is required;
- only a review of services availability is required (usually because the development of a contingency plan is sought);
- seeks approval or accreditation system or product
- a project for security metrics is to be launched where items to be controlled must be identified as well as the likelihood and detail;
- etc.

These frequent situations result in an adjustment of the scope of the analysis. A common strategy is to identify as a service to be provided the environment we wish to analyse in detail, and use it as outer perimeter, requiring security levels inferred from the information being dealt with and the quality expected to be obtained from the service.

Besides covering a more or less broad analysis, situations may arise requiring analysis with a different depth:

- an urgent analysis to identify critical assets;
- an overall analysis to identify general measures
- a detailed analysis to identify specific safeguards for certain elements of the information system;
- a detailed quantitative analysis to determine the benefit of an expensive safeguard;
- ...

Summing up, the following tasks must be adjusted

- horizontally to the scope required (See RAM.1);
- vertically to the appropriate depth.

8.2. 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:

- Reputation or good image.
- Accumulated knowledge.
- Independence of criterion or action.
- Personal privacy.
- Safety of persons.

These elements can be included in the risk analysis as assets[23] or as evaluation elements[24]. 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[25].

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?

The information being handled and the services being provided are always the essential assets. It is sometimes of interest to single out the various information and services, while in other occasions we can group together several pieces of information or services that are equivalent as security requirements are concerned. It is even common to make batches {information + services } considered by the managers as one.

It is not always clear what an asset is individually.

— For instance, if your unit has 300 PC's, all with identical configurations and dealing with the same data, it is not useful to analyse 300 identical assets. It is sufficient to analyse a generic PC that represents them all; grouping simplifies the model.
— Identifying subsystems is commonplace and practical. A typical subsystem is a computer comprising hardware, information medium (disks), peripherals, operating system and basic software such as desktop applications and antivirus software. If possible, this conglomerate should be dealt with as a single asset.

23 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.
24 See "Catalogue of Elements", chapter 4. Valuation criteria".
25 See Magerit version 1.0, "Procedures guide" / "3. Elements sub-module" / "3.4. Impacts" / "3.4.3. Types"

— For instance, if your unit has 300 PC, all of them identical in their configuration and data, it is not convenient to assess 300 identical assets. Analysing a generic PC that will represent them all should be enough. Unifying will simplify the model. A good idea is to have as many assets as configuration profiles for personal equipment.
— 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.

During the assets identification stage, it is not uncommon to have expansion cycles in which complex assets break down into more simple ones, and compression stages in which many assets are merged into a single asset (it is frequent to speak about sub-systems). These cycles are recurrently repeated until

- The assets group is sufficiently detailed so as not to forget anything
- The number of assets is not as large as to get lost
- The name of assets is not ambiguous and uses the usual terminology of the Organisation

In short, the model must be **easy to explain** to the people who will make decisions from our conclusions.

8.3. Discovering and modelling the dependencies between assets

To start, information and services should be always put at the top. The circumstances will determine whether information or services will come first; but most frequently, the value in the information must be respected by the services that handle it; therefore, information is on top, and services just below.

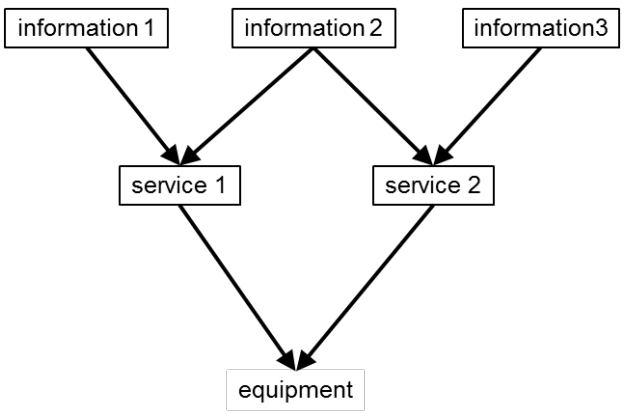

Figure 18. Top level dependencies

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”[26] 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[27]. 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.

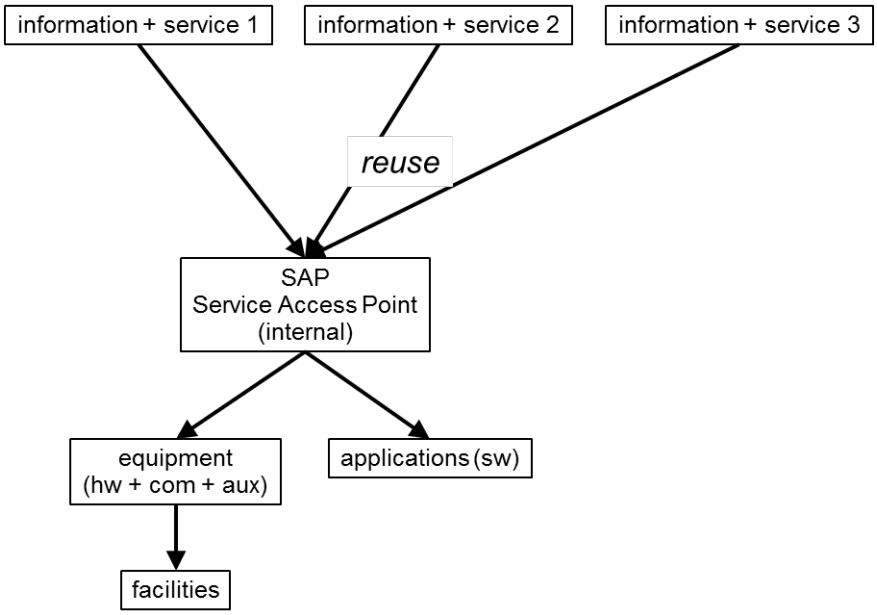

Figure 19. Internal or intermediate services

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.

In some organisations, the information that must be handled is very well defined, so we can identify the services dealing with it and the deployed equipment.

Other organisations are more focused on the services they provide, so they can start from a series of services and then associate the information they manage and the deployed equipment.

Sometimes, the analysis starts by listing the equipment and then looking for provided services and information treated in the system.

26 See “Guide of techniques”, section 2.3.
27 The "Guide of techniques" contains the algorithmic model for calculating the total dependencies between assets on the basis of the direct dependencies.

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 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*
application → data	information → application

Table 9. Dependencies between Information and software applications

In this context, sometimes a distinction must be made between the data and the information. The information is essential, while the data are an ICT implementation of the information. The information is valuable, and the rest only as long as it contains information.

The information handled by a system is either above the services or grouped:

- information → services → equipment (including data, applications, equipment, …)
- { information + services } → equipment (including data, applications, equipment, …)

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

Table 10. Dependencies about services

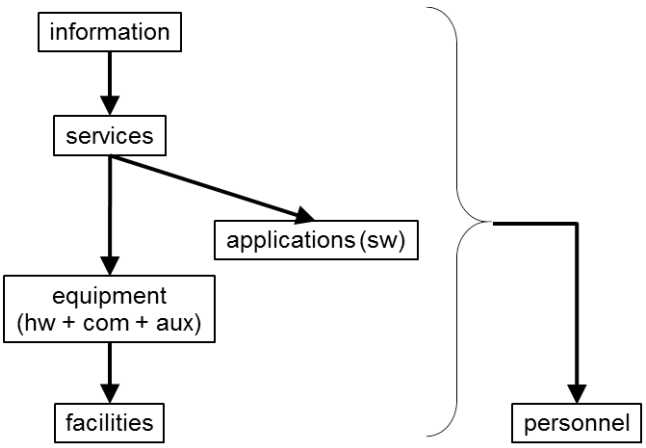

Figure 20. Dependency hierarchy

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.

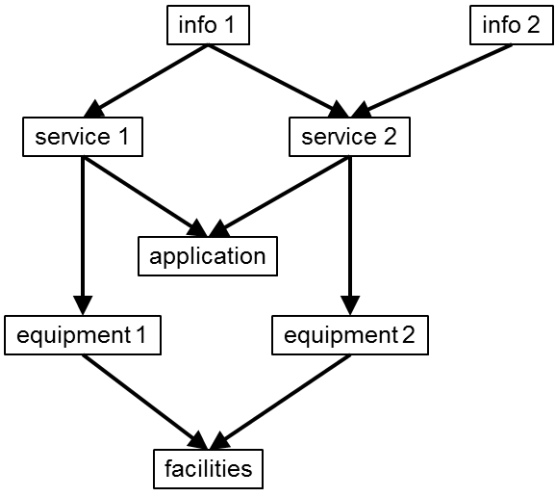

Figure 21.Dependencies between assets for the provision of some services

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.

In other words, to see if dependencies are well established, study the accumulated value.

8.4. Valuing assets

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

If essential 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 incident. Therefore, risk management methodologies require the Organisation to establish valuation criteria, which are organisation-wide and must be approved by the governing bodies that evaluate the system and receive the results of the analysis.

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 defective, 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[28]**:** 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[29].

The most realistic way to deal with 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.

8.5. 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 role plays 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. Role plays 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.

Typically, risk analysis support tools provide standard profiles to help this task.

---

28 See "Guide of techniques", chapter 3.7.

29 The evaluation of privacy related 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 cause of a fine.

8.6. Valuing threats

The task is demoralising: determine the degree of degradation that would be caused and the likelihood 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.[30]
- The attacker does not need a great investment in equipment.[31]
- 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.

Starting from a standard value, it is necessary to increase or reduce the classifications for likelihood 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 likelihood 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 likelihood does not affect the impact so that studying the impact allows the degradation to be adjusted and then studying the risk allows the likelihood to be adjusted. An unjustified degradation value must never be accepted in the hope of its being compensated with the likelihood 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.

Typically, risk analysis support tools provide standard profiles to help this task.

30 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 may become very likely).

31 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.

8.7. Choosing safeguards

Probably the only way is to use a catalogue. You can also use an expert (system) to propose solutions 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.

8.8. Successive approximations

Risk analysis may be very laborious, requiring time and effort. It is also necessary to introduce many elements that are not objective but 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 coarse-grained 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 it is adequately managed. 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.

8.8.1. 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 27002:2013.
- National standards, for example the “Spanish National Security Framework”.
- 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 types of 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.

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 v3 have been chosen and are shown in bold. When the definition comes from a source, this is quoted.

1.1. Terms

Accreditation	Formal declaration by a designated approving authority that a system is approved to operate in a particular security mode using a prescribed set of safeguards [ISO/IEC 21827:2008] NOTE This definition is generally accepted within the security community; within ISO the more generally used definition is: Procedure by which an authoritative body gives formal recognition that a body or person is competent to carry out specific tasks [ISO/IEC Guide 2].
Accountability	Property that ensures that the actions of an entity may be traced uniquely to the entity. [ISO/IEC 7498-2:1989]
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 likelihood of occurrence.
Accumulated value	Considers the value of the asset itself and that of the assets that depend on it.
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.
Attack	Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset [ISO/IEC 27000:2014]
Authenticity	Property that an entity is what it claims to be [ISO/IEC 27000:2014]
Availability	Property of being accessible and usable upon demand by an authorized entity [ISO/IEC 27000:2014] The property of being accessible and usable upon demand by an authorized entity. [7498-2:1989]
Certification	Process, producing written results, of performing a comprehensive evaluation of security features and other safeguards of a system to establish the extent to which the design and implementation meet a set of specified security requirements [ISO/IEC 21827:2008] NOTE This definition is generally accepted within the security community; within ISO the more generally used definition is: Procedure by which a third party gives written assurance that a product, process or service conforms to specified requirements [ISO/IEC Guide 2].
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [7498-2:1989]
Control	See safeguard.
Statement of applicability	A formal document for a group of safeguards that states whether they apply to the information system being studied or whether they are meaningless.

Countermeasure	See safeguard.
Deficiencies report (vulnerabilities report)	Report: Absence or weakness of the safeguards that are considered appropriate to reduce 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 likelihood of occurrence, both measured on the assets on which it depends.
Degradation	The loss of the value of an asset as a result of the occurrence 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 expected rate of occurrence of a threat. See “likelihood”. ARO: Annualized Rate of Occurrence
Impact	Impact level: The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability [CNSS 4009:2010] Consequence: outcome of an event [ISO/IEC Guide 73:2002]
Impact analysis	Business Impact Analysis (BIA): process of analysing operational functions and the effect that a disruption might have upon them [ISO/IEC 27031:2011]
Incident	information security incident: single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security [ISO/IEC 27000:2014]
Information system	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information . [CNSS 4009:2010]
Integrity	Property that data has not been modified or deleted in an unauthorised and undetected manner. [ISO/IEC 19790:2012]
Likelihood	See “probability”.
Probability	Extent to which an event (3.1.4) is likely to occur [ISO/IEC Guide 73:2002]
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. Residual risk: risk remaining after risk treatment [ISO /IEC Guide 73:2002]
Risk	Risk: combination of the probability of an event and its consequence [ISO/IEC Guide 73:2002]
Risk analysis	Systematic use of information to identify sources and to estimate the risk. [ISO/IEC Guide 73:2002]
Risk management	Coordinated activities to direct and control an organisation with regard to risk. [ISO/IEC Guide 73:2002]
Risk treatment	Risk treatment: process of selection and implementation of measures to modify risk [ISO/IEC Guide 73:2002]

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. Synonymous with security controls and countermeasures. [CNSS 4009:2010]
Safeguards evaluation	Report: Evaluation of the effectiveness of the existing safeguards in relation to the risks they face.
Security	"Network and information security" means the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency
Security audit	Audit: Independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures. [CNSS 4009:2010]
Security plan	Security Program Plan. Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management security controls and common security controls in place or planned for meeting those requirements. [CNSS 4009:2010]
Threat	Potential cause of an incident which may result in harm to a system or organisation. [ISO/IEC 27000:2014]
Value	Of an asset. An estimate of the consequences of the occurrence of a threat.
Value model	Report: A description of the value of the assets for the organisation as well as the dependencies between the assets.
Vulnerability	Weakness of an asset or control that can be exploited by one or more threats. [ISO/IEC 27000:2014] Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited. [CNSS 4009:2003]
Vulnerability report	See “Deficiencies report”

References

[CNSS 4009:2010]
Committee on National Security Systems. CNSS Instruction No. 4009. National Information Assurance (IA) Glossary

[ISO/IEC 7498-2:1989]
Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture

[ISO/IEC 19790:2012]
Information technology -- Security techniques -- Security requirements for cryptographic modules

[ISO/IEC 21827:2008]
Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®)

[ISO/IEC 27000:2014]
Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary

[ISO/IEC 27031:2011]
Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity

[ISO/IEC Guide 2:2004]
Standardization and related activities -- General vocabulary

[ISO/IEC Guide 73:2002]
Risk management -- Vocabulary

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

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.

A4.1. Information security management systems (ISMS)

“Management system” is the collection of activities performed by the organisation to manage its processes, to ensure that manufactured products or services provided meet the targets set by the organisation, typically:

- Satisfying the quality demanded by the customers
- Fulfilling the legal, regulatory and contractual obligations

Within an Organisation’s management system, the “information security management system” (ISMS) is related to information security. It is usually understood that management systems must be adapted to the Denning (PDCA) cycle, which is commonly used in quality management systems:

P – Plan – Objectives are set and plans prepared to achieve them. This includes evaluating the situation of the Organisation: where are we and where do we want to be?

D – Do – Plans are executed.

C – Check –The results obtained are evaluated to determine to what extent objectives have been achieved.

A – Act – For continuous improvement, plans are updated.

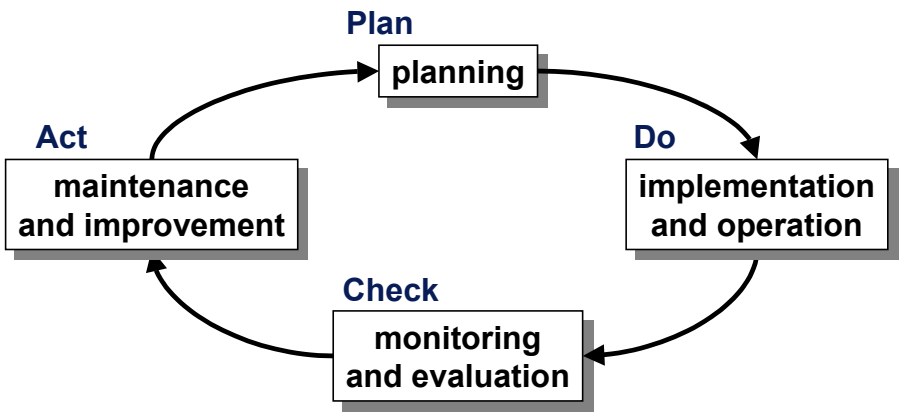

Figure 22. PDCA cycle

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 to derive consequences from experience itself and from similar 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.

A4.1.1. 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". There is a scope 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 outcome of the risk analysis allows 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.

A4.1.2. 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.

A4.1.3. Terminology

The following lists the terms used in information systems certification activities, as understood in this context.

Accreditation

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.

Management system

Set of interrelated or interacting elements of an organisationto establish policies and objectives and processes to achieve those objectives

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.

A4.2. 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 allows:

1. The definition of security functions[32] 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”[33].

32 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.

33 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.

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[34] that sets the administrative and regulatory framework under which the certification is carried out.

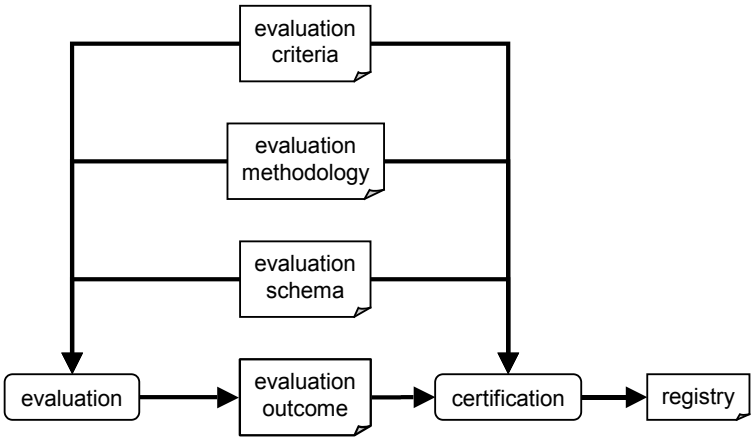

Figure 23. Certification process

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[35]:

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+[36].

34 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/.

35 EAL: Evaluation Assurance Level

36 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.

A4.2.1. 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.

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.

A4.2.2. 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[37].

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[38].

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:

37 A typical example of a PP is one that sets the security features to be required from a firewall.

38 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
  • Organisational 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
	  • Organisational 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

Table 11. Protection profiles and security declarations

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.

A4.2.3. 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	

Table 12. Functional and assurance requirements

A4.2.4. 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.

A4.2.5. 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.

Appendix 5. Tools

The undertaking of a risk analysis and management 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 risk analysis and management 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[39]. 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".

39 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.

- Evaluate the residual impact and risks.

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 Security Agency 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:

- Spanish National Security Framework
- ISO/IEC 27002 Security management systems
- Spanish RD 1720:2007 Personal data protection

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.

Appendix 6. Evolution of Magerit

The first version of Magerit, published in 1997, has generally stood the passage of time, ratifying the main aspects. However, the initial version has been notably improved.

The second version, published in 2005, was meant to be a constructive revision, adapted to the present time and including the experience of the past years.

The third version seeks a new adaptation, considering not only the practical experience but also the evolution of the ISO international regulations that are a mandatory referent.

A6.1. Evolution from Magerit version 2

Version 3 largely maintains the structure of version 2:

- Book I – Method
- Book II – Catalogue of elements
- Techniques

Changes in version 3:

- A better compliance with ISO regulations, looking for integration of the risk analysis task in the organisation risk management framework directed by the governing bodies
- the text is lighter
- less important or less used parts are eliminated
- different activities are normalized
    - RAM – Risk Analysis Method
    - RAP – Risk Analysis Project
    - PS – Security Plan

A6.2. Evolution from Magerit version 1

If you have worked with Magerit v1.0, all the concepts may be familiar to you, though there has been some evolution. In particular, you will recognize the so called sub-model of active elements: assets, threats, vulnerabilities, impact, risks and safeguards. This conceptual part has been endorsed by the passage of time and remains the backbone for analysis and management. The so called “security sub-states” have been renamed “dimensions”. New criteria to measure what is interesting about the assets have been introduced. The sub-model of processes appears under the paragraph “organisation of the risk analysis and management project”.

While Magerit v1.0 has survived in its conceptual part, the same cannot be said about the technical specifications of the information systems with which it works. Now, asset classes, threats, and safeguards are references to external catalogues that may be updated. The method is open, so that if it is clear what to do and how to do it, the details can be adapted at any moment.

The 7 books in Magerit version 1 have evolved:

Magerit version 1	**Magerit version 3**
Book I. On information systems security	Book I – Methodology
Book II. Procedures	Book I – Methodology
Book III. Techniques	Guide of Techniques
Book IV. Guide for application developers	Book I – Methodology / Chapter 7 Development of Information systems
Book V. Guide for the responsible people	Book I – Methodology Book II – Catalogue of Elements
Book VI. Data architecture and data exchange interface	Book II – Catalogue of Elements / XML formats
Book VII. Reference of legal and technical regulations	Book I – Methodology / Annex 3. Legal framework