MINISTERIO DE
ADMINISTRACIONES
PÚBLICAS

MAGERIT – version 2

Methodology for Information Systems Risk Analysis and Management

II - Catalogue of Elements

Madrid, 20 June 2006 (v 1.1)
NIPO: 326-06-044-8
Catálogo general de publicaciones oficiales
http://publicaciones.administracion.es

PROJECT TEAM

Director:
Francisco López Crespo
Ministerio de Administraciones Públicas

Miguel Angel Amutio Gómez
Ministerio de Administraciones Públicas

Javier Candau
Centro Criptológico Nacional

External consultant:
José Antonio Mañas
Professor
Universidad Politécnica de Madrid

Index

1. Introduction

This Catalogue of Elements has two purposes in a risk analysis and management project:

1. Firstly, to facilitate the work of the persons carrying out the project by offering them a standard item for quick consultation, concentrating on the specifics of the system being analysed.
2. And secondly, to provide uniform results from the analysis, promoting terminology and criteria that allow the analyses made by different teams to be compared and even integrated.

To achieve these objectives and knowing that technology changes quickly, the following sections describe a catalogue[1] containing guidelines to:

Types of assets, knowing that new types of assets appear continually.

Valuation dimensions, knowing that in specific cases, specific dimensions may appear but with the certainty that the essential items are included.

Valuation criteria, knowing that there is a strong estimation component by the experts but giving first guidelines to uniformity. The purpose is to provide relative values of the assets in their various valuation dimensions so that not only is a scale proposed within a dimension but that also the relationships between the dimensions.

Threats, knowing that not all threats are important to all systems but with a reasonable hope that this catalogue grows slowly.

Safeguards, knowing that this is an extremely complicated area due to the richness of technologies, products and ingenious combinations of basic elements, safeguards are treated with a focus on the “identification of needs” by those responsible for the information systems while providing a focus on the “effectiveness and efficiency controls” by system auditors. There has been an attempt at developing an intermediate language which suits both groups.

Each section includes an XML syntax that will be used to publish the elements in a standard format that can be automatically processed by analysis and management tools.

[1] This catalogue must change according to the development of information systems. This is why an XML notation has been defined for each category of elements, allowing updates to this catalogue to be published easily.

2. Types of assets

The classification of assets provides both interesting information for documenting purposes and a criterion for identifying potential threats and suitable safeguards according to the nature of the asset.

The following table can neither be exhaustive, nor always valid. Consult the references.

The following list classifies the assets within a hierarchy, establishing, for each one, a code that shows its hierarchical position, a name and a brief description of the properties in the section. Note that the fact that an asset belongs to one type does not mean it is excluded from other types, that is, an asset may be of several types simultaneously

2.1. List of types

[S] Services

A function that meets a need of the users (of the service). A series of means is required to provide a service.

Services appear as assets in a risk analysis, either as end services (provided by the organisation to third parties), or as instrumental services (where both users and means are in-house) or as outsourced services (from other organisations that provide them with their own means).

Thus, there are public services provided by the government to meet the needs of the public, business services provided by companies to satisfy the needs of their clients, internal services provided by specialised departments within the organisation and that are used by other departments or employees within it, etc.

As this guide is centred on information and communications technologies security, it is natural that information services, communications services, security services, etc, appear in it without preventing the inclusion of other services required for the effective undertaking of the organisation's mission.

```
    [anon] anonymous (without requiring user identification)
    [pub] for the general public (without any contractual relationship)
    [ext] for clients (with a contractual relationship)
    [int] internal (users and means within the organisation itself)
    [cont] outsourced to third parties (provided with external means)

    [www] World Wide Web
    [telnet] remote access to local account
    [email] e-mail
    [ftp] file transfer
    [edi] electronic data exchange

    [dir] directory service (1)
    [idm] identity management (2)
    [ipm] privilege management
    [pki] PKI - public key infrastructure (3)
```

1. Location of persons (white pages), companies or services (yellow pages), allowing the identification and providing the attributes of the specific element.
2. Services that allow users to be entered and removed from systems, including their classification and activating the supply of services associated with the changes of status with regard to the organisation.
3. Services associated with public key encryption systems, especially including the management of certificates.

[D] Data / Information

Items of information which either individually or grouped together in some way, represent knowledge of something.

Data are the heart that allows an organisation to provide its services. In a certain way they are an abstract asset which will be stored in equipment or information media (normally grouped together in the form of databases) or will be transferred from one place to another by data transmission media.

In an analysis of risks and impacts, the user is normally limited to valuing the data, the other assets being simply servants that must take care of and protect the data entrusted to them.

```
[vr] vital records (1)
[com] data of commercial interest (2)
[adm] data of administrative interest
[source] source code
[exe] object code
[conf] configuration data
[log] log
[test] test data

[per] personal data (3)
  [A] high level
  [M] medium level
  [B] basic level

[label] classified data (4)
  [S] très secret UE / EU top secret
  [R] secret UE
  [C] confidentiel UE
  [DL] restreint UE
  [SC] unclassified
```

1. Said to be those that are essential for the survival of the organisation, that is, those the lack of which or damage to will directly affect the organisation’s existence. It is possible to identify those that are essential for the organisation to survive an emergency situation, those that allow critical missions to be carried out or reconstructed, and those that affect the organisation’s legal nature or financial rights or those of its users.
2. Said to be those that are of value for providing the services of the organisation itself.
3. Said to be any information concerning physical persons who are identified or can be identified. Personal data are regulated by laws and regulations regarding public liberty and fundamental rights of physical persons and especially their honour and personal and family privacy.
4. Said to be those subjected to specific regulations to control access and distribution, that is, those whose confidentiality is especially important. The classifications into which the data may be classified and the standards for their handling, are determined by the sector regulations, by agreements between the organisations or by internal standards.

[SW] Applications (software)

With multiple names (programs, applications, developments, etc.) this section refers to tasks that have been automated and are carried out on a computer. Applications manage, analyse and change data, allowing the information to be used for providing services.

This section is not concerned with the source code or programs that are data of commercial interest, to be valued and protected as such. This code will appear as data.

```
    [prp] in-house development
    [sub] made-to-measure (sub-contracted)
    [std] standard (off the shelf)
      [browser] Web browser
      [www] display servers
      [app] application servers
      [file] file servers
      [dbms] database management systems
      [tm] transactional monitors
      [office] office computing
      [os] operating systems
```

[HW] Computer equipment (hardware)

Said to be material, physical goods, designed to directly or indirectly support the services provided by the organisation, thus being temporary or permanent data depositories, support for the execution of computer applications or the means for processing or transmitting data.

```
[host] large equipment (1)
[mid] midsize equipment (2)
[pc] personal computing (3)
[mobile] mobile computing (4)
[pda] PDAs
[easy] easily replaceable (5)
[data] data storage (6)
[peripheral] peripherals
  [print] print media (7)
  [scan] scanners
  [crypto] encryption devices
[network] network support (8)
  [modem] modems
  [hub] hubs
  [switch] switchers
  [router] routers
  [bridge] bridges
  [firewall] firewalls
```

1. Notable for being few, often only one, financially expensive and requiring a specific environment for their operation. They are difficult to replace in the event of destruction.
2. Notable for being various, of medium cost both for acquisition and for maintenance, and requiring standard conditions for their operating environment. They are not difficult to replace in the event of destruction.
3. Notable for being many, of relatively small cost and with minimum requirements for their operating environment. They are easily replaceable in the event of destruction.
4. Notable as being equipment classified for personal computing which, additionally, is easily moved from one place to another, and can be in the organisation’s own premises or in any other place.
5. Equipment which, in the event of a temporary or permanent fault, may be replaced quickly and economically.
6. Equipment in which data remains for a long period. Specially, this classification includes equipment which contains the data locally, compared to those which only handle data in transit
7. Printers and print servers.
8. Equipment needed for transmitting data: routers, modems, etc.

[COM] Communication networks

Including both dedicated installations and those operating as outsourced communications services but always focusing on the fact that they are the means of transporting data from one place to another.

```
    [PSTN] telephone network
    [ISDN] digital network
    [X25] data network
    [ADSL] ADSL
    [pp] point to point
    [radio] wireless network
    [sat] satellite
    [LAN] local network
    [MAN] metropolitan network
    [Internet] Internet
    [vpn] virtual private network
```

[SI] Media

This section includes physical devices for storing information permanently or, at least, for long periods.

```
    [electronic] electronic
      [disk] disks
      [disquette] diskettes
      [cd] CD-ROM
      [usb] USB devices
      [dvd] DVD
      [tape] magnetic tape
      [mc] memory cards
      [ic] intelligent cards
    [non_electronic] non-electronic
      [printed] printed material
      [tape] paper tape
      [film] micro film
      [cards] punched cards
```

[AUX] Auxiliary equipment

This section includes other equipment that supports information systems without being directly related to data.

```
    [power] power supplies
    [ups] uninterruptible power supplies
    [gen] electrical generators
    [ac] air conditioning
    [cabling] cabling
    [robot] robots
      [tape] ... tapes
      [disk] ... disks
    [supply] essential supplies
    [destroy] information media destruction equipment
    [furniture] furniture: cupboards, etc.
    [safe] safes
```

[L] Installations

This section includes places housing information and communications systems.

```
    [site] site
    [building] building
    [local] premises
    [mobile] mobile platforms
      [car] land vehicle: car, truck, etc.
      [plane] aircraft: airplane, etc.
      [ship] sea transport: ship, boat, etc.
      [shelter] containers
    [channel] channelling
```

[P] Personnel

This section includes persons related to information systems.

```
    [ue] external users
    [ui] internal users
    [op] operators
    [adm] system administrators
    [com] communications administrators
    [dba] database administrators
    [des] developers
    [sub] sub-contractors
    [prov] suppliers
```

2.2. Personal data

The classification of personal data depends on the applicable legislation in each place and circumstance.

2.3. Classified data

The classification of data is an administrative procedure unique to each organisation or sector of activity, that determines the conditions for handling the information depending on the need to preserve its confidentiality.

The European Union is governed by:

- Commission Decision of 29 November 2001, amending its internal Rules of Procedure (2001/844/EC, ECSC, Euratom).
- Council Decision of 19 March 2001, adopting the council’s security regulations (2001/264/EC).

in which the following levels were set:

Très secret UE / EU Top Secret

This classification only applies to information and material whose unauthorised disclosure could cause exceptionally serious damage to the essential interests of the European Union or of one or more of its Member States.

If materials marked TRÈS SECRET UE/EU TOP SECRET are in danger, this would be likely to:

- Directly threaten the internal stability of the EU or of one of its Member States or of friendly countries.
- Cause exceptionally serious damage to relationships with friendly governments.
- Directly cause the general loss of human lives.
- Cause exceptionally serious damage to the capacity to function effectively or to the secu-

rity of the forces of the Member States or to those of other contributors or cause damage to the continuing effectiveness of highly valuable security or intelligence operations.

- Cause serious long-term damage to the economy of the EU or of the Member States.

Secret UE

This classification only applies to information and material whose unauthorised disclosure could cause serious prejudice to the interests of the European Union or of one or more of its Member States.

If materials marked SECRET UE are in danger, this would be likely to:

- Raise international tensions.
- Cause serious prejudice to relationships with friendly governments.
- Place lives directly in danger or seriously damages public order or individual security or liberty.
- Cause exceptionally serious damage to the capacity to function effectively or to the security of the forces of the Member States or to those of other contributors or cause damage to the continuing effectiveness of highly valuable security or intelligence operations.
- Cause considerable material damage to the financial, monetary, economic or commercial interest of the EU or of one of its Member States.

Confidentiel UE

This classification applies to information and material whose unauthorised disclosure could cause prejudice to the interests of the European Union or of one or more of its Member States.

If materials marked CONFIDENTIEL UE are in danger, this would be likely to:

- Cause prejudice to diplomatic relationships, that is, causes a formal protest or other sanctions.
- Prejudice individual security or liberty.
- Prejudice the capacity to function effectively or the security of the forces of the Member States or to those of other contributors or reduce the effectiveness of highly valuable security or intelligence operations.
- Notably reduce the financial viability of important organisations.
- Impede the investigation or facilitate the commission of serious offences.
- Notably reduce the financial, economic and commercial interests of the EU or of its Member States.
- Cause serious obstacles to the development or functioning of priority policies of the EU.
- Interrupt or noticeably disturb important activities of the EU.

Restreint UE

This classification applies to information and material whose unauthorised disclosure could be disadvantageous to the interests of the European Union or of one or more of its Member States.

If materials marked RESTREINT UE are in danger, this would be likely to:

- Unfavourably affect diplomatic relationships.
- Cause considerable suffering to individuals.
- Make it difficult to maintain the operational effectiveness or security of the forces of the Member States or of other contributors.
- Cause financial losses or facilitate unfair gains or advantages to individuals or companies.

- Breach proper undertakings to maintain the reserve of information facilitated by third parties.
- Breach legal restrictions on the disclosure of information.
- Make investigation difficult or facilitate the commission of offences.
- Place the EU or its Member States at a disadvantage in commercial negotiations or in actions of other types with third parties.
- Place obstacles to the development or to the effective functioning of priority policies of the EU.
- Reduce the appropriate management of the EU and of its operations.

2.4. XML Syntax

The types of assets can be expected to develop over time to adapt to technological developments. For this reason, XML grammar is given below that allows updates for the types described above to be published periodically.

The notation is described in Appendix 1.

```
types ::=
  <types>
    { type }*
  </types>

type ::=
  <type code>
    #name#
    [ description ]
    { type }*
  </type>

description ::=
  <description>
    #text#
  </description>
```

Atributos

Attribute	***Example***	***Description***
code	C="X"	X is a unique identifier that allows the type referred to to be determined unequivocally.

2.5. References

There are many sources that identify assets within the area of information and communications technologies.

- GMITS, ISO/IEC IS 13335-1:2004, "Information technology - Security techniques - Guidelines for the management of IT security - Part 1: Concepts and models for information and communications technology security management".
- SP 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categories", NIST, June 2004.

  http://csrc.nist.gov/publications/nistpubs/index.html
- UNE-ISO/IEC 17799:2002, "Tecnología de la Información. Código de Buenas Prácticas de la Gestión de la Seguridad de la Información". 2002.
- "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/

- GMITS, ISO/IEC TR 13335-5: 2001, “Information technology - Security techniques - Guidelines for the management of IT security - Part 5: Management guidance of network security”
- GMITS, ISO/IEC TR 13335-4: 2000, “Information technology - Security techniques - Guidelines for the management of IT security - Part 4: Selection of safeguards”
- GMITS, ISO/IEC TR 13335-3:1998, “Information technology - Security techniques - Guidelines for the management of IT security - Part 3: Techniques for management of IT security”.
- MAGERIT, “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”, MAP, versión 1.0, 1997

  http://www.csi.map.es/csi/pg5m20.htm
- GMITS, ISO/IEC TR 13335-2:1997, “Information technology - Security techniques - Guidelines for the management of IT security - Part 2: Managing and planning IT security”.

3. Valuation dimensions

These are the features or attributes that make an asset valuable. A dimension is a facet or an aspect of an asset, independent of other facets. Risks may be analysed by focusing on a single facet, regardless of what happens with other aspects[2]

Dimensions are used to evaluate the consequences of the appearance of a threat. The valuation of an asset in a certain dimension is the measurement of the prejudice the organisation may suffer if the asset is damaged in that dimension.

3.1. List of dimensions

[D] availability
Assurance that the authorised users have access when they require it to the information and its associated assets.
How important would it be if the asset was not available?
An asset has a great value from the point of view of availability when the consequences of a threat affecting its availability are serious. On the other hand, an asset has no appreciable value from the point of view of availability when no damage is caused if it is frequently unavailable for long periods. Availability is a property that affects all types of assets. Often, availability requires treatment in steps because the cost of non-availability increases non-linearly with the duration of the stoppage, from short interruptions without importance, and interruptions that cause considerable damage to irrecoverable interruptions: the organisation is finished.

[I] data integrity
A guarantee of the exactness and completeness of the information and the methods for processing it.
What would be the importance of the data being changed uncontrollably?
Data is attributed a high value from the point of view of integrity when their alteration, intentional or unintentional would cause serious damage to the organisation. Likewise, data have little crucial value from the point of view of integrity when their alteration is of no concern.

[C] data confidentiality
Assurance that the information is accessible only to those who are authorised to have access.
What would be the importance of the data becoming known to unauthorised persons?
Data are attributed a high value from the confidentiality point of view when their disclosure would cause serious damage to the organisation. Likewise, data have no appreciable value from the point of view of confidentiality when their becoming known to anyone is of no concern.

[2] As is the typical case known as business impact analysis (BIA) that seeks to determine the cost of system stoppages and to develop contingency plans to put a limit to the organisation's downtime. In this case, a sectarian analysis of the availability is carried out.

[A_S] authenticity of service users
Assurance of identity or origin.
What would be the importance of the person accessing the service not being the real one?
The authenticity of the users of a service counters the opportunity for fraud or unauthorised use of a service. Consequently, a service is attributed a high value from the point of view of authenticity when its provision to false users would cause serious prejudice for the organisation. Likewise, a service lacks appreciable value from the authenticity point of view when its access by anyone is of no concern.

[A_D] authenticity of data origin
Assurance of the identity or origin.
What would be the importance of the data not really originating from where they are thought to?
Data are attributed a high value from the point of view of origin authenticity when an imputation defect would cause serious damage to the organisation. Typically, the opportunity for repudiation is given. Likewise, data have little appreciable value from the point of view of origin authenticity when not knowing the source is irrelevant.

[T_S] accountability of service use
Assurance that who did what and when, is known at all times.
What would be the importance of not having a record of the use of the service?
This would open the door to fraud, preventing the organisation from tracing offences and may involve the non-compliance with legal obligations.

[T_D] accountability of data access
Assurance that who did what and when, is known at all times.
What would be the importance of having no record of the access to the data?
This would open the door to fraud, preventing the organisation from tracing offences and may involve the non-compliance with legal obligations.

3.2. XML Syntax

The valuation dimensions will continue to develop over time to adapt to technological developments. For this reason, XML grammar is given below that allows updates for the dimensions described above to be published periodically.

The notation is described in Appendix 1.

```
dimensions ::=
  <dimensions>
    { dimension }*
  </dimensions>

dimension ::=
  <dimension code>
    #name#
    [ description ]
  </dimension>
```

```
description ::=
  <description>
    #text#
  </description>
```

Atributos

Attribute	***Ejemple***	***Description***
code	C="X"	X is a unique identifier that allows the dimension referred to to be determined unequivocally.

3.3. References

- ISO/IEC 13335-1:2004, "Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management", 2004.
- C. Alberts and A. Dorofee, "Managing information Security Risks. The OCTAVE Approach", Addison Wesley, 2003.

  http://www.cert.org/octave/
- FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems", December 2003.

  http://csrc.nist.gov/publications/fips/index.html
- ISO/IEC 17799:2000, "Information technology -- Code of practice for information security management", 2000.
- Ministerio de Administraciones Públicas, "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
- ISO 7498-2:1989, "Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture", 1989.

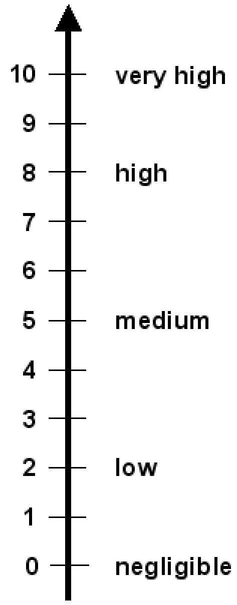
4. Valuation criteria

Theoretically, any value scale can be used to value the assets. However, for practical purposes, it is important that:

- A common scale is used for all dimensions, allowing risks to be compared.
- A logarithmic scale is used, centred on relative value differences, and not on absolute differences [3].
- A uniform criterion is used that allows the comparison of analyses made separately.

If the valuation is financial, there is little more to be said, but, frequently, the valuation is qualitative, and at the user's discretion, that is, according to subjective criteria.

A detailed scale of 10 values has been chosen, with zero being a minimal value (for the purposes of risk). If a risk analysis is a made with little detail, a simplified table of five levels could be used. . Both scales - detailed and simplified - are correlated as shown below:



value		***criterion***
10	very high	very serious damage to the organisation.
7-9	high	serious damage to the organisation.
4-6	medium	important damage to the organisation.
1-3	low	small damage to the organisation.
0	minimal	irrelevant for practical purposes.

The following table is intended as a guide in greater detail for users uniformly valuing assets whose value is important for different reasons after taking account of:

- The security of persons.
- Personal information[4]
- Obligations arising from the law, from the regulatory framework, from contracts, etc.
- Capacity for following up offences.
- Commercial and financial interests.

[3] Thus it is equally relevant that an asset is twice as valuable as some other, regardless of its absolute value. On other hand, it would be unusual to consider that an asset is twice as valuable as some other without considering its absolute value, just as it would be unusual to consider that the step from 0.1 to 2.1 is the same as going from 1,000,000 to 1,000,002.

[4] Personal information is classified in two ways: administrative and valued. The administrative way consists of indicating the level to which the datum in question belongs, this being a qualitative decision; the safeguards to be used are independent of the value of the datum itself for the organisation. The valued way assigns a level to the consequences for the organisation of the deterioration of the datum. Thus, there is a distinction between the legal obligations and the prejudices to the service, without omitting either aspect since they are both important.

- Financial losses.
- Interruption of the service.
- Public order.
- Corporate policy.
- Other intangible values.

The most usual situation is that an asset receives a simple valuation in each dimension in which it is valuable. This system should and must be enriched in the case of more complex dimensions such as that of availability, in which the consequences vary according to the duration of the interruption. In that event, the dimension does not receive a single qualification, but as many as there are steps that are considered relevant. The following criteria are applied in each step, while the reason may vary[5].

4.1. Standard scale

value	***criteria***	
10	[olm]	Is likely to cause exceptionally serious damage to the operational effectiveness or security of the Operations / Logistics mission
	[iio]	Is likely to cause exceptionally serious damage to the continuing effectiveness of extremely important intelligence or information operations
	[si]	Security: is likely to lead to an exceptionally serious breach of security, or prejudice the investigation of an exceptionally serious security incident
	[ps]	Personal safety: is likely to lead directly to the widespread loss of life
	[po]	Public order: is likely to threaten directly the internal stability of the country
	[ir]	Is likely to cause exceptionally serious impact on international relations
	[lbl]	Labelled data: Secret / Cosmic Top Secret

[5] For example, a brief interruption may cause dissatisfaction among users while a long one could give rise to penalties for the non-compliance with administrative obligations.

value	*criteria*	
9	[da]	Is likely to cause exceptionally serious disruption of activities within an organisation and with serious impact on other organizations
	[adm]	Administration & management: is likely to seriously impede the efficient operation of the entire organisation, or shut down the organisation
	[lg]	Is likely to result in widespread adverse publicity for exceptionally seriously adversely affecting relations ...
		[lg.a] relations with other organisations
		[lg.b] relations with the public
		[lg.c] relations with other countries
	[olm]	Is likely to cause serious damage to the operational effectiveness or security of the Operations / Logistics mission
	[iio]	Is likely to cause serious damage to the continuing effectiveness of highly important intelligence or information operations
	[cei]	Commercial and economic interests:
		[cei.a] be of exceptionally high interest to a competitor
		[cei.b] be of very high commercial value
		[cei.c] cause exceptionally high financial loss
		[cei.d] facilitate very significant improper gain or advantage for individuals or organisations
		[cei.e] constitute an exceptionally serious breach of contractual undertakings to maintain the security of information provided by third parties
	[lro]	Legal and regulatory obligations: is likely to lead to an exceptionally serious breach of a legal or regulatory obligation
	[si]	Security: is likely to lead to a serious breach of security, or prejudice the investigation of a serious security incident
	[ps]	Personal safety: is likely to lead directly to death of an individual or group of individuals
	[po]	Is likely to seriously prejudice public order
	[ir]	Is likely to cause serious impact on international relations
	[lbl]	Labelled data: Secret
8	[ps]	onal safety: is likely to prejudice individual security/liberty (for example, is likely to lead to the life of an individual or group of individuals being threatened)
	[crm]	Would impede the prosecution of crimes, or easy their commission
	[lbl]	Labelled data: Confidential

value	*criteria*
7	[da] Is likely to cause major disruption to activities within an organisation and with major impact on other organisations
	[adm] Administration & management: is likely to impede the efficient operation of the entire organisation
	[lg] Is likely to result in widespread adverse publicity
	[lg.a] seriously adversely affect relations with other organisations
	[lg.b] seriously adversely affect relations with the public
	[lg.c] seriously adversely affect relations with other countries
	[olm] Is likely to cause damage to the operational effectiveness or security of the Operations / Logistics mission
	[iio] Is likely to cause major damage to the continuing effectiveness of important intelligence or information operations
	[cei] Commercial and economic interests:
	[cei.a] be of high interest to a competitor
	[cei.b] be of high commercial value
	[cei.c] cause high financial loss
	[cei.d] facilitate significant improper gain or advantage for individuals or organisations
	[cei.e] constitute a serious breach of contractual undertakings to maintain the security of information provided by third parties
	[lro] Legal and regulatory obligations: is likely to lead to a major breach of a legal or regulatory obligation
	[si] Security: is likely to lead to a major breach of security, or prejudice the investigation of a major security incident
	[ps] Personal safety: is likely to lead to more than minor injury to several individuals
	[ir] Is likely to cause significant impact on international relations
	[lbl] Labelled data: Confidential
6	[pi1] Personal information: is likely to cause significant distress to a group of individuals
	[pi2] Personal information; is likely to cause a significant breach of a legal regulatory requirement for personal information
	[ps] Personal safety: is likely to lead to more than a minor injury, restricted to an individual
	[po] Is likely to cause demonstrations, or significant lobbying
	[lbl] Labelled data: Restricted

value	*criteria*
5	[da] Is likely to cause disruption to activities within an organisation and with some impact on other organisations [adm] Administration & management: is likely to lead to the inefficient operation of more than one part of an organisation [lg] Is likely to result in limited adverse publicity [lg.a] adversely affect relations with other organisations [lg.b] adversely affect relations with the public [olm] Is likely to make it more difficult to maintain the operational effectiveness or security of the Operations / Logistics mission beyond a local level [iio] Is likely to cause damage to the continuing effectiveness of important intelligence or information operations [pi1] Personal information: is likely to cause significant distress to an individual [pi2] Personal information: is likely to cause significant distress to an individual [lro] Legal and regulatory obligations: is likely to lead to a breach of a legal or regulatory obligation [ir] Is likely to cause an impact on international relations [lbl] Labelled data: Restricted
4	[pi1] Personal information: is likely to cause distress to a group of individuals [pi2] Personal information: is likely to cause a breach of a legal or regulatory requirement for personal information [ps] Personal safety: is likely to lead to minor injury to several individuals [crm] Impede the prosecution or ease the commission of crimes [lbl] Labelled data: Restricted

value	***criteria***
3	[da] Is likely to cause disruption to activities within an organisation
	[adm] Administration & management: is likely to lead to the inefficient operation of one part of an organisation
	[lg] Is likely to adversely affect relations within an organisation
	[olm] Is likely to make it more difficult to maintain the operational effectiveness or security of the Operations / Logistics mission at a local level
	[iio] Is likely to cause minor damage to the continuing effectiveness of important intelligence or information operations
	[cei] Commercial and economic interests:
	[cei.a] be of moderate interest to a competitor
	[cei.b] be of moderate commercial value
	[cei.c] cause financial loss, or loss of earning potential
	[cei.d] facilitate improper gain or advantage for individuals or organisations
	[cei.e] constitute a minor breach of contractual undertakings to maintain the security of information provided by third parties
	[pi1] Personal information: is likely to cause distress to an individual
	[pi2] Personal information: is likely to cause a breach of a legal or regulatory requirement for personal information
	[lro] Legal and regulatory obligations: is likely to lead to a minor / technical breach of a legal or regulatory obligation
	[si] Security: is likely to lead to a breach of security, or prejudice the investigation of a security incident
	[ps] Personal safety: is likely to lead to a minor injury to an individual
	[po] Is likely to cause limited or localised protest
	[ir] Is likely to cause minor impact on international relations
	[lbl] Labelled data: Restricted
2	[lg] Is likely to cause minor loss of goodwill within an organisation
	[cei] Commercial and economic interests:
	[cei.a] be of low interest to a competitor
	[cei.b] be of little commercial value
	[pi1] Personal information: could cause minor distress to an individual
	[pi2] Personal information: could cause a minor breach of legal or regulatory requirements for personal information
	[ps] Personal safety: could lead to minor injury to several individuals
	[lbl] Labelled data: Unclassified

value	*criteria*
1	[da] Could cause disruption to activities within an organisation [adm] Administration & management: could lead to the inefficient operation of one part of an organisation [lg] Could cause minor loss of goodwill within an organisation [olm] Could it make make it more difficult to maintain the operational effectiveness or security of the Operations / Logistics mission at a local level [iio] Could cause minor damage to the continuing effectiveness of important intelligence or information operations [cei] Commercial and economic interests: [cei.a] be of little interest to a competitor [cei.b] be of little commercial value [pi1] Personal information: could cause minor distress to an individual [lro] Legal and regulatory obligations: could cause a minor / technical breach of a legal or regulatory obligation [si] Security: could lead to a breach of security, or prejudice the investigation of a security incident [ps] Personal safety: could lead to minor injury to an individual [po] Could cause localised or community level protest [ir] Could cause a minor impact on international relations [lbl] Labelled data: Unclassified
0	[1] would not affect personal safety [2] would cause no significant harm [3] would cause minimal economical loss [4] would cause minimal loss of goodwill

4.2. XML Syntax

The types of assets can be expected to develop over time to adapt to technological developments. For this reason, XML grammar is given below that allows updates for the types described above to be published periodically.

The notation is described in Appendix 1.

```
valuation ::=
  <valuation>
    { level }*
  </valuation>

level ::=
  <level value code>
    { ítem }*
  </level>

ítem ::=
  <item>
    #description#
  </item>
```

Attributes

Attribute	***Example***	***Description***
value	V=”X”	X is an index between 0 and 10 for the qualitative valuation of assets.
code	C=”X”	X is a unique code to identify the criterion, ; the paragraph in the above table must be given; for example, “7.4.c”.

4.3. References

- SP 800-60, “Guide for Mapping Types of Information and Information Systems to Security Categories”, NIST, June 2004.
  http://csrc.nist.gov/publications/nistpubs/index.html
- HMG, “Residual Risk Assessment Method”, INFOSEC Standard No. 1. 2003.
- C. Alberts and A. Dorofee, “Managing information Security Risks. The OCTAVE Approach”, Addison Wesley, 2003.
  http://www.cert.org/octave/

5. Threats

The following is a catalogue of possible threats to the assets in an information system. Each threat is shown in a table as follows:

[code] short description of what may happen	
Types of assets: ▯ that may be affected by this threat	**Dimensions:** 1. [of security] that may be damaged by this threat; sorted by relevance
Description: longer presentation of what may happen	

5.1. [N] Natural disasters

Events that may occur without being directly or indirectly caused by human beings.

[N.1] Fire	
Types of assets: ▯ [HW] computer equipment (hardware) ▯ [COM] communication networks ▯ [SI] media ▯ [AUX] auxiliary equipment ▯ [L] installations	**Dimensions:** 1. [D] availability 2. [T_S] accountability of service use 3. [T_D] accountability of data access
Description: Fires: possibility that the fire destroys system resources.	

[N.2] Water damage	
Types of assets: ▯ [HW] computer equipment (hardware) ▯ [COM] communication networks ▯ [SI] media ▯ [AUX] auxiliary equipment ▯ [L] installations	**Dimensions:** 1. [D] availability 2. [T_S] accountability of service use 3. [T_D] accountability of data access
Description: Floods: possibility that the water destroys system resources.	

[N.*] Natural disasters	
Types of assets: ▯ [HW] computer equipment (hardware) ▯ [COM] communication networks ▯ [SI] media ▯ [AUX] auxiliary equipment ▯ [L] installations	**Dimensions:** 1. [D] availability 2. [T_S] accountability of service use 3. [T_D] accountability of data access
Description: Other incidents that occur without human involvement: lightning, electric storm, earthquake, cyclones, avalanche, landslide, etc. ... This excludes specific disasters such as fires (see [N.1]) and floods (see [N.2]). This excludes personnel for whom there is a specific threat [E.31] to cover involuntary non-availability of personnel without going into its causes.	

5.2. [I] Of industrial origin

Events that may occur accidentally arising from human activity of an industrial type. These threats may be accidental or deliberate.

[I.1] Fire	
Types of assets: ▯ [HW] computer equipment (hardware) ▯ [COM] communication networks ▯ [SI] media ▯ [AUX] auxiliary equipment ▯ [L] installations	**Dimensions:** 1. [D] availability 2. [T_S] accountability of service use 3. [T_D] accountability of data access
Description: Fire: possibility that the fire destroys the system’s resources.	

[I.2] Water damage	
Types of assets: ▯ [HW] computer equipment (hardware) ▯ [COM] communication networks ▯ [SI] media ▯ [AUX] auxiliary equipment ▯ [L] installations	**Dimensions:** 1. [D] availability 2. [T_S] accountability of service use 3. [T_D] accountability of data access
Description: Escapes, leaks, floods: possibility that the water destroys the system’s resources.	

[I.*] Industrial disasters	
Types of assets: ▯ [HW] computer equipment (hardware) ▯ [COM] communication networks ▯ [SI] media ▯ [AUX] auxiliary equipment ▯ [L] installations	**Dimensions:** 1. [D] availability 2. [T_S] accountability of service use 3. [T_D] accountability of data access
Description: Other disasters due to human activity: explosions, collapses, ... ❑ chemical pollution, ... ❑ electrical overloads, electrical fluctuations, ... ❑ traffic accidents, etc. This excludes specific threats such as fire (see [I.1]) and flood (see [I.2]). This excludes personnel for whom there is a specific threat [E.31], to cover involuntary non-availability of personnel without going into its causes.	

[I.3] Mechanical pollution

Types of assets:

- [HW] computer equipment (hardware)
- [COM] communication networks
- [SI] media
- [AUX] auxiliary equipment

Dimensions:

1. [D] availability
2. [T_S] accountability of service use
3. [T_D] accountability of data access

Description:

Vibrations, dust, dirt, etc.

[I.4] Electromagnetic pollution

Types of assets:

- [HW] computer equipment (hardware)
- [COM] communication networks
- [SI] media (electronic)
- [AUX] auxiliary equipment

Dimensions:

1. [D] availability
2. [T_S] accountability of service use
3. [T_D] accountability of data access

Description:

Radio interference, magnetic fields, ultraviolet light, etc.

[I.5] Hardware or software failure

Types of assets:

- [SW] software
- [HW] computer equipment (hardware)
- [COM] communication networks
- [SI] media
- [AUX] auxiliary equipment

Dimensions:

1. [D] availability
2. [T_S] accountability of service use
3. [T_D] accountability of data access

Description:

Failures in the equipment and/or programs. May be due to a defect in origin or may have arisen during the operation of the system.

In specific-purpose systems, it is sometimes difficult to know whether the failure is of physical or logical origin, but this difference is not usually relevant in terms of consequences.

[I.6] Power interruption

Types of assets:

- [HW] computer equipment (hardware)
- [COM] communication networks
- [SI] media (electronic)
- [AUX] auxiliary equipment

Dimensions:

1. [D] availability
2. [T_S] accountability of service use
3. [T_D] accountability of data access

Description:

Cut in the power supply.

[I.7] Unsuitable temperature and / or humidity conditions	
Types of assets: ▯ [HW] computer equipment (hardware) ▯ [COM] communication networks ▯ [SI] media ▯ [AUX] auxiliary equipment	**Dimensions:** 1. [D] availability 2. [T_S] accountability of service use 3. [T_D] accountability of data access
Description: Deficiencies in the air conditioning of the premises that exceed the working limits for the equipment: excess heat, excess cold excess humidity, etc.	

[I.8] Communications services failure	
Types of assets: ▯ [COM] communication networks	**Dimensions:** 1. [D] availability
Description: A cut in the capability to transmit data from one place to another. This is typically due to the physical destruction of the physical transport media or to detention in the switching centres, either due to destruction, detention or simple lack of capacity to handle the current traffic.	

[I.9] Interruption of other services and essential supplies	
Types of assets: ▯ [AUX] auxiliary equipment	**Dimensions:** 1. [D] availability
Description: Other services or resources on which the operation of the equipment depends, for example, printer paper, toner, coolant, etc.	

[I.10] Media degradation	
Types of assets: ▯ [SI] media	**Dimensions:** 1. [D] availability 2. [T_S] accountability of service use 3. [T_D] accountability of data access
Description: As the result of the passing of time.	

[I.11] Electromagnetic radiation	
Types of assets: • [HW] computer equipment (hardware) • [COM] communication networks • [L] installations	**Dimensions:** 1. [C] confidentiality
Description: The fact of making internal data available to third parties by radio.. It is a threat in which the issuer is the passive victim of the attack. Almost all electrical devices emit radiation to the exterior that can be intercepted by other equipment (radio receivers) causing a leak of information. This threat is frequently but inaccurately called, a TEMPEST attack (“Transient Electromagnetic Pulse Standard”). Although abusing the original meaning, it is frequent to hear of equipment described as having “TEMPEST protection”, meaning that it is designed not to emit electromagnetically anything of interest in case somebody receives it. This threat does not include emissions for the needs of communication media: wireless networks, microwave links, etc. that may be threatened by interception.	

5.3. [E] Errors and unintentional failures

Unintentional failures caused by persons.

The numbering is not consecutive, but follows deliberate attacks, often similar to unintentional errors, and differing only in the subject’s purpose.

[E.1] Users’ errors	
Types of assets: • [S] services • [D] data / information • [SW] software	**Dimensions:** 1. [I] integrity 2. [D] availability
Description: Mistakes by persons when using the services, data, etc.	

[E.2] Administrator errors	
Types of assets: • [S] services • [D] data / information • [SW] software • [HW] computer equipment (hardware) • [COM] communication networks	**Dimensions:** 1. [D] availability 2. [I] integrity 3. [C] confidentiality 4. [A_S] autenticidad del servicio 5. [A_D] authenticity of data origin 6. [T_S] accountability of service use 7. [T_D] accountability of data access
Description: Mistakes by persons with responsibilities for installation and operation.	

[E.3] Monitoring (logging) errors

Types of assets:	**Dimensions:**
- [S] services - [D] data / information - [SW] software	1. [T_S] accountability of service use 2. [T_D] accountability of data access

Description:
Unsuitable activity records: lack of records, incomplete records, incorrectly dated records incorrectly attributed records, etc.

[E.4] Configuration errors

Types of assets:	**Dimensions:**
- [S] services - [D] data / information - [SW] software - [HW] computer equipment (hardware) - [COM] communication networks	1. [D] availability 2. [I] integrity 3. [C] confidentiality 4. [A_S] authenticity of service users 5. [A_D] authenticity of data origin 6. [T_S] accountability of service use 7. [T_D] accountability of data access

Description:
The entry of erroneous configuration data.
Almost all assets depend on their configuration and this depends on the diligence of the administrator: access privileges, activity flows, activity records, routing, etc.

[E.7] Organisational deficiencies

Types of assets:	**Dimensions:**
- [P] personnel	1. [D] availability

Description:
When it is not clear who must do exactly what and when, including taking measures on the assets or reporting to the management hierarchy.
Uncoordinated actions, errors by omission, etc.

[E.8] Malware diffusion

Types of assets:	**Dimensions:**
- [SW] software	1. [D] availability 2. [I] integrity 3. [C] confidentiality 4. [A_S] authenticity of service users 5. [A_D] authenticity of data origin 6. [T_S] accountability of service use 7. [T_D] accountability of data access

Description:
Innocent propagation of viruses, spy ware, worms, Trojans, logic bombs, etc.

[E.9] [Re-]routing errors

Types of assets:

- [S] services
- [SW] software
- [COM] communication networks

Dimensions:

1. [C] confidentiality
2. [I] integrity
3. [A_S] authenticity of service users
4. [T_S] accountability of service use

Description:

The sending of information via a system or network, accidentally. These may be messages between persons using an incorrect route with information passing through or reaching the incorrect place. These could be messages between persons, between processes or between both.

The case of a routing error involving a delivery error, with the information ending up in the hands of someone unexpected is particularly notable.

[E.10] Sequence errors

Types of assets:

- [S] services
- [SW] software
- [COM] communication networks

Dimensions:

1. [I] integrity

Description:

The accidental alteration of the order of the messages sent.

[E.14] Information leaks

Types of assets:

- [D] data / information
- [SW] software
- [COM] communication networks

Dimensions:

1. [C] confidentiality

Description:

The information accidentally reaches persons who should not have knowledge of it, without the information itself being altered.

[E.15] Information alteration

Types of assets:

- [D] data / information

Dimensions:

1. [I] integrity

Description:

The accidental alteration of the information.

This threat is only identified for data in general, since there are specific threats when information is stored on a computer medium.

[E.16] Entry of incorrect information

Types of assets:

- [D] data / information

Dimensions:

1. [I] integrity

Description:

The accidental entry of incorrect information.

This threat is only identified for data in general since there are specific threats when information is stored on a computer medium.

[E.17] Information degradation	
Types of assets: ▯ [D] data / information	**Dimensions:** 1. [I] integrity
Description: Accidental degradation of the information. This threat is only identified for data in general since there are specific threats when information is stored on a computer medium.	

[E.18] Destruction of information	
Types of assets: ▯ [D] data / information	**Dimensions:** 1. [D] availability
Description: Accidental loss of information. This threat is only identified for data in general since there are specific threats when information is stored on a computer medium.	

[E.19] Disclosure of information	
Types of assets: ▯ [D] data / information	**Dimensions:** 1. [C] confidentiality
Description: Disclosure due to indiscretion. Verbal indiscretion, electronic media, hard copies, etc.	

[E.20] Software vulnerabilities	
Types of assets: ▯ [SW] software	**Dimensions:** 1. [I] integrity 2. [D] availability 3. [C] confidentiality
Description: Defects in the code that cause a defective operation without intention on the part of the user but with consequences to the data integrity or to its capacity to operate.	

[E.21] Defects in software maintenance / updating	
Types of assets: ▯ [SW] software	**Dimensions:** 1. [I] integrity 2. [D] availability
Description: Defects in the procedures or controls for updating the code that allow programs with known defects that have been repaired by the manufacturer to continue to be used.	

[E.23] Defects in hardware maintenance / updating	
Types of assets: ▯ [HW] computer equipment (hardware)	**Dimensions:** 1. [D] availability
Description: Defects in the procedures or controls for updating equipment that allow its continued use after the normal life time.	

[E.24] System failure due to exhaustion of resources	
Types of assets: ▯ [S] services ▯ [HW] computer equipment (hardware) ▯ [COM] communication networks	**Dimensions:** 1. [D] availability
Description: The lack of sufficient resources causes the system failure when the workload is excessive.	

[E.28] Staff shortage	
Types of assets: ▯ [P] internal personnel	**Dimensions:** 1. [D] availability
Description: Accidental absence from the work post: illness disturbances in public order, bacteriological warfare , etc	

5.4. [A] Wilful attacks

Deliberate failures caused by persons.

The numbering is not consecutive to match the unintentional errors, which are often similar to deliberate attacks, the only difference being the subject's purpose.

[A.4] Manipulation of the configuration	
Types of assets: ▯ [S] services ▯ [D] data / information ▯ [SW] software ▯ [HW] computer equipment (hardware) ▯ [COM] communication networks	**Dimensions:** 1. [I] integrity 2. [C] confidentiality 3. [A_S] authenticity of service users 4. [A_D] authenticity of data origin 5. [T_S] accountability of service use 6. [T_D] accountability of data access 7. [D] availability
Description: Almost all assets depend on their configuration and this in turn depends on the diligence of the administrator: access privileges, activity flows, activity record, routing, etc.	

[A.5] Masquerading of user identity

Types of assets:	**Dimensions:**
- [S] services - [SW] software - [COM] communication networks	1. [C] confidentiality 2. [A_S] authenticity of service users 3. [A_D] authenticity of data origin 4. [I] integrity

Description:

When attackers manage to appear as authorised users, they enjoy the users' privileges for their own purposes.

This threat may be perpetrated by internal personnel, by persons outside the organisation or by persons contracted temporarily.

[A.6] Abuse of access privileges

Types of assets:	**Dimensions:**
- [S] services - [SW] software - [HW] computer equipment (hardware) - [COM] communication networks	1. [C] confidentiality 2. [I] integrity

Description:

Each user enjoys a level of privileges for a specific purpose. When users abuse their privilege level to carry out tasks that are not their responsibility, there are problems.

[A.7] Misuse

Types of assets:	**Dimensions:**
- [S] services - [SW] software - [HW] computer equipment (hardware) - [COM] communication networks - [SI] media - [AUX] auxiliary equipment - [L] installations	1. [D] availability

Description:

The use of system resources for unplanned purposes, typically of personal interest: games, personal searches on the Internet, personal databases, personal programs, storage of personal data, etc.

[A.8] Malware diffusion

Types of assets:	**Dimensions:**
- [SW] software	1. [D] availability 2. [I] integrity 3. [C] confidentiality 4. [A_S] authenticity of service users 5. [A_D] authenticity of data origin 6. [T_S] accountability of service use 7. [T_D] accountability of data access

Description:

The intentional propagation of viruses, spy ware, worms, trojans, logic bombs, etc.

[A.9] [Re-]routing of messages

Types of assets:

- [S] services
- [SW] software
- [COM] communication networks

Dimensions:

1. [C] confidentiality
2. [I] integrity
3. [A_S] authenticity of service users
4. [T_S] accountability of service use

Description:

The sending of information to an incorrect destination via a system or network, with information passing through or reaching the incorrect place. These may be messages between persons, between processes or between both.

An attacker may force a message to travel through a specific node in the network where it can be intercepted.

Particularly notable is the case in which the routing attack causes a fraudulent delivery, with the information reaching the hands of an unauthorised person.

[A.10] Sequence alteration

Types of assets:

- [S] services
- [SW] software
- [COM] communication networks

Dimensions:

1. [I] integrity

Description:

The alteration of the order of the messages sent. The idea is that the new order changes the meaning of the group of messages, prejudicing the integrity of the affected data.

[A.11] Unauthorised access

Types of assets:

- [S] services
- [D] data / information
- [SW] software
- [HW] computer equipment (hardware)
- [COM] communication networks
- [SI] media
- [AUX] auxiliary equipment
- [L] installations

Dim1nsiones:

1. [C] confidentiality
2. [I] integrity
3. [A_S] authenticity of service users

Description:

The attacker manages to access the system’s resources without authorisation for doing so, typically taking advantage of a failure in the identification and authorisation system.

[A.12] Traffic analysis

Types of assets:

- [COM] communication networks

Dimensions:

1. [C] confidentiality

Description:

Without needing to analyse the contents of communications, the attacker can reach conclusions based on the analysis of the origin, destination, volume and frequency of the exchanges.

This is sometimes called “traffic monitoring”.

[A.13] Repudiation

Types of assets:	Dimensions:
[S] services	1. [T_S] accountability of service use

Description:

The later rejection of actions or undertakings acquired in the past.

Repudiation of origin: denial of being the sender or origin of a message or communication.

Repudiation of receipt: denial of having received a message or communication.

Repudiation of delivery: denial of having received a message for delivery to others.

[A.14] Eavesdropping

Types of assets:	Dimensions:
[D] data / information [SW] software [HW] computer equipment (hardware) [COM] communication networks	1. [C] confidentiality

Description:

Attackers have access to information that is not theirs, without the information itself being altered.

[A.15] Alteration of information

Types of assets:	Dimensions:
[D] data / information	1. [I] integrity

Description:

Intentional alteration of the information to obtain a benefit or cause damage.

This threat is only identified for data in general since there are specific threats when the data is on a computer medium.

[A.16] Entry of false information

Types of assets:	Dimensions:
[D] data / information	1. [I] integrity

Description:

The deliberate entry of false information to obtain a benefit or cause damage.

This threat is only identified for data in general since there are specific threats when the data is on a computer medium.

[A.17] Corruption of information

Types of assets:	Dimensions:
[D] data / information	1. [I] integrity

Description:

The intentional degradation of the information, to obtain a benefit or cause damage.

This threat is only identified for data in general since there are specific threats when the data is on a computer medium.

<table>
<tr><th colspan="2">[A.18] Destruction of information</th></tr>
<tr><td><b>Types of assets:</b>
▯ [D] data / information</td><td><b>Dimensions:</b>
1. [D] availability</td></tr>
<tr><td colspan="2"><b>Description:</b>
The intentional deletion of information, to obtain a benefit or cause damage.
This threat is only identified for data in general since there are specific threats when the data is on a computer medium.</td></tr>
</table>

<table>
<tr><th colspan="2">[A.19] Disclosure of information</th></tr>
<tr><td><b>Types of assets:</b>
▯ [D] data / information</td><td><b>Dimensions:</b>
1. [C] confidentiality</td></tr>
<tr><td colspan="2"><b>Description:</b>
Disclosure of information.</td></tr>
</table>

<table>
<tr><th colspan="2">[A.22] Software manipulation</th></tr>
<tr><td><b>Types of assets:</b>
▯ [SW] software</td><td><b>Dimensions:</b>
1. [C] confidentiality
2. [I] integrity
3. [A_S] authenticity of service users
4. [A_D] authenticity of data origin
5. [T_S] accountability of service use
6. [T_D] accountability of data access</td></tr>
<tr><td colspan="2"><b>Description:</b>
The intentional alteration of the operation of a program to obtain an indirect benefit when an authorised person uses it.</td></tr>
</table>

<table>
<tr><th colspan="2">[A.24] Denial of service</th></tr>
<tr><td><b>Types of assets:</b>
▯ [S] services
▯ [HW] computer equipment (hardware)
▯ [COM] communication networks</td><td><b>Dimensions:</b>
1. [D] availability</td></tr>
<tr><td colspan="2"><b>Description:</b>
The lack of sufficient resources causes the system to fail when the workload is too high.</td></tr>
</table>

[A.25] Theft

Types of assets:

- [HW] computer equipment (hardware)
- [COM] communication networks
- [SI] media
- [AUX] auxiliary equipment

Dimensions:

1. [D] availability
2. [C] confidentiality

Description:

Theft of equipment directly causes a lack of resources to provide the services, that is, non-availability.

All types of equipment may be affected by theft, the most common being theft of equipment and of information media.

Theft may be carried out by internal personnel, persons outside the organisation or persons contracted temporarily, which sets different degrees of ease for accessing the stolen object and different consequences.

In the case of equipment hosting data, a leak of information may also occur.

[A.26] Destructive attack

Types of assets:

- [HW] computer equipment (hardware)
- [COM] communication networks
- [SI] media
- [AUX] auxiliary equipment
- [L] installations

Dimensions:

1. [D] availability

Description:

Vandalism, terrorism, military action, etc.

This threat may be carried out by internal personnel, by persons outside the organisation or by persons contracted temporarily.

[A.27] Enemy over-run

Types of assets:

- [HW] computer equipment (hardware)
- [COM] communication networks
- [SI] media
- [AUX] auxiliary equipment
- [L] installations

Dimensions:

1. [D] availability
2. [C] confidentiality

Description:

When the premises have been invaded and control is lost over the means of work.

[A.28] Staff shortage

Types of assets:

- [P] internal personnel

Dimensions:

1. [D] availability

Description:

Deliberate absence from the work post: such as strikes, labour absenteeism, unjustified absences, the blocking of accesses, etc.

[A.29] Extortion

Types of assets:

- [P] internal personnel

Dimensions:

1. [C] confidentiality
2. [I] integrity
3. [A_S] authenticity of service users
4. [A_D] authenticity of data origin
5. [T_S] accountability of service use
6. [T_D] accountability of data access

Description:

Pressure with threats, on people to oblige them to act in a certain way.

[A.30] Social engineering

Types of assets:

- [P] internal personnel

Dimensions:

1. [C] confidentiality
2. [I] integrity
3. [A_S] authenticity of service users
4. [A_D] authenticity of data origin
5. [T_S] accountability of service use
6. [T_D] accountability of data access

Description:

Taking advantage of the good will of some persons to make them carry out activities of interest to a third party.

5.5. Matching between errors and attacks

Errors and threats are frequently two sides of the same coin: something that could happen to assets without bad intentions or deliberately. There are three possible combinations:

- Threats that may only be errors, but never deliberate attacks.
- Threats that are never errors, they are always deliberate attacks.
- Threats that may occur either by error or deliberately.

To face this situation, the errors and threats have been numbered so that they can be correlated. The following table matches errors with attacks, showing this correlation[6]:

number	*error*	*attack*
1	Users' errors	
2	Administrator errors	
3	Monitoring (logging) errors	
4	Configuration errors	Manipulation of the configuration
5		Masquerading of user identity
6		Abuse of access privileges
7	Organisational deficiencies	Misuse
8	Malware diffusion	Malware diffusion
9	[Re-]routing errors	[Re-]routing of messages
10	Sequence errors	Sequence alteration

[6] The "Attack" column is left blank when the threat is simply an error. The "Error" column is left blank when the threat is always deliberate.

number	error	attack
11		Unauthorised access
12		Traffic analysis
13		Repudiation
14	Information leaks	Eavesdropping
15	Information alteration	Alteration of information
16	Entry of incorrect information	Entry of false information
17	Information degradation	Corruption of information
18	Destruction of information	Destruction of information
19	Disclosure of information	Disclosure of information
20	Software vulnerabilities	
21	Defects in software maintenance / updating	
22		Software manipulation
23	Defects in hardware maintenance / updating	
24	System failure due to exhaustion of resources	Denial of service
25		Theft
26		Destructive attack
27		Enemy over-run
28	Staff shortage	Staff shortage
29		Extortion
30		Social engineering

5.6. Threats by asset type

To complete the above description threat by threat, the following tables group the threats according to the type of asset, showing the dimension in which they could be significantly affected. Note that, due to dependencies between assets, the lower assets support the value of the higher assets, the latter being affected through these.

5.6.1. [S] Services

The following threats may appear to assets of type [S], with consequences for the security of the information system.

[D]	[I]	[C]	[A_*]	[T_*]
E.1 E.2 E.4 E.24	E.1 E.2 E.4 E.9 E.10	E.2 E.4 E.9	E.2 E.4 E.9	E.2 E.3 E.4 E.9
A.4 A.7 A.24	A.4 A.5 A.6 A.9 A.10 A.11	A.4 A.5 A.6 A.9 A.11	A.4 A.5 A.9 A.11	A.4 A.9 A.13

5.6.2. [D] data / information

The following threats may appear to assets of type [D], with consequences for the security of the information system.

[D]	*[I]*	*[C]*	*[A_*]*	*[T_*]*
E.1 E.2 E.3 E.18	E.1 E.2 E.3 E.15 E.16 E.17	E.2 E.3 E.14 E.19	E.2 E.4	E.2 E.3 E.4
A.4 A.18	A.4 A.11 A.15 A.16 A.17	A.4 A.11 A.14 A.19	A.4 A.11	A.4

5.6.3. [SW] software

The following threats may appear to assets of type [SW], with consequences for the security of the information system.

[D]	*[I]*	*[C]*	*[A_*]*	*[T_*]*
I.5				I.5
E.1 E.2 E.4 E.8 E.20 E.21	E.1 E.2 E.4 E.8 E.9 E.10 E.20 E.21	E.2 E.4 E.8 E.9 E.14 E.20	E.2 E.4 E.8 E.9	E.2 E.3 E.4 E.8 E.9
A.4 A.7 A.8	A.4 A.5 A.6 A.8 A.9 A.10 A.11 A.22	A.4 A.5 A.6 A.8 A.9 A.11 A.14 A.22	A.4 A.5 A.8 A.9 A.11 A.22	A.4 A.8 A.9 A.22

5.6.4. [HW] Computer equipment (hardware)

The following threats may appear to assets of type [HW], with consequences for the security of the information system.

[D]	*[I]*	*[C]*	*[A_*]*	*[T_*]*
N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7		I.11		N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7

[D]	[I]	[C]	[A_*]	[T_*]
E.2 E.4 E.23 E.24	E.2 E.4	E.2 E.4	E.2 E.4	E.2 E.4
A.4 A.7 A.24 A.25 A.26 A.27	A.4 A.6 A.11	A.4 A.6 A.11 A.14 A.25 A.27	A.4 A.11	A.4

5.6.5. [COM] Communication networks

The following threats may appear to assets of type [COM], with consequences for the security of the information system.

[D]	[I]	[C]	[A_*]	[T_*]
N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7 I.8		I.11		N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7
E.2 E.4 E.24	E.2 E.4 E.9 E.10	E.2 E.4 E.9 E.14	E.2 E.4 E.9	E.2 E.4 E.9
A.4 A.7 A.24 A.25 A.26 A.27	A.4 A.5 A.6 A.9 A.10 A.11	A.4 A.5 A.6 A.9 A.11 A.12 A.14 A.25	A.4 A.5 A.9 A.11	A.4 A.9

5.6.6. [SI] Media

The following threats may appear to assets of type [SI], with consequences for the security of the information system.

[D]	[I]	[C]	[A_*]	[T_*]
N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7 I.10				N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7 I.10

[D]	*[I]*	*[C]*	*[A_*]*	*[T_*]*
A.7 A.25 A.26 A.27	A.11	A.11 A.25 A.27	A.11	

5.6.7. [AUX] Auxiliary equipment

The following threats may appear to assets of type [AUX], with consequences for the security of the information system.

[D]	*[I]*	*[C]*	*[A_*]*	*[T_*]*
N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7 I.9				N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.6 I.7
A.7 A.25 A.26 A.27	A.11	A.11 A.25 A.27	A.11	

5.6.8. [L] installations

The following threats may appear to assets of type [L], with consequences for the security of the information system.

[D]	*[I]*	*[C]*	*[A_*]*	*[T_*]*
N.1 N.2 N.* I.1 I.2 I.*				N.1 N.2 N.* I.1 I.2 I.*
A.7 A.26 A.27	A.11	A.11 A.27	A.11	

5.6.9. [P] personnel

The following threats may appear to assets of type [P], with consequences for the security of the information system.

[D]	*[I]*	*[C]*	*[A_*]*	*[T_*]*
E.7 E.28				
A.28	A.29 A.30	A.29 A.30	A.29 A.30	A.29 A.30

5.6.10. Availability

The following threats may appear to different types of assets, with consequences for the availability of the information system.

	destruction	*fault*		*saturation*	*lack*
		physical	*logical*		
[S] services			E.1 E.2 E.3 A.4	A.7 E.24 A.24	
[D] data / information	E.1 E.2 E.18 A.18		E.1 E.2 E.4 A.4		
[SW] software			I.5 E.1 E.2 E.4 E.20 E.21 A.4 E.8 A.8	A.7	
[HW] computer equipment (hardware)	N.1 N.2 N.* I.1 I.2 I.* I.3 I.7 A.26 A.27	N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.7	I.4 E.2 E.4 A.4 E.23	A.7 E.24 A.24	I.6 A.25
[COM] communication networks	N.1 N.2 N.* I.1 I.2 I.* I.3 I.7 A.26 A.27	N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.5 I.7	I.4 E.2 E.4 A.4	A.7 E.24 A.24	I.6 I.8 A.25
[SI] media	N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 I.7 I.10 A.26 A.27	N.2 I.2 I.3 I.4 I.5		A.7	I.6 A.25
[AUX] auxiliary equipment	N.1 N.2 N.* I.1 I.2 I.* I.3 I.4 A.26 A.27	N.1 N.2 N.* I.1 I.2 I.2* I.3 I.4 I.5 I.7		A.7	I.6 I.9 A.25
[L] installations	N.1 N.2 N.* I.1 I.2 I.* A.26 A.27	N.1 N.2 N.* I.1 I.2 I.*		A.7	
[P] personnel			E.7		E.28 A.28

5.7. XML syntax

Threats can be expected to develop over time to adapt to technological developments. For this reason, XML grammar is given below that allows updates to the threats described above to be published periodically.

The notation is described in Appendix 1.

```
threats ::=
  <threats>
    { group }*
  </threats>

group ::=
  <group>
    { group | threat }*
    [ description ]
  </group>

threat ::=
  <threat threat_code>
    #name#
    { dimension }+
    [ escription ]
  </threat>

dimension ::=
  <dimension dimension_code>

description ::=
  <description>
    #text#
  </description>
```

Atrributes

Attribute	***Example***	***Description***
threat_code	Z="X"	X is a unique identifier that allows the threat referred to to be identified unequivocally.
dimension_code	D="X"	X is a unique identifier that allows the dimension referred to to be identified unequivocally.

5.8. References

There are many sources that catalogue threats within the area of information and communications technologies.

- GMITS, ISO/IEC IS 13335-1:2004, "Information technology - Security techniques - Guidelines for the management of IT security - Part 1: Concepts and models for information and communications technology security management".
- IT Baseline Protection Manual, Federal Office for Information Security (BSI), Germany. October 2003.

  http://www.bsi.de/gshb/english/etc/index.htm
- 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/
- GMITS, ISO/IEC TR 13335-5: 2001, "Information technology - Security techniques - Guidelines for the management of IT security - Part 5: Management guidance of network security"
- GMITS, ISO/IEC TR 13335-4: 2000, "Information technology - Security techniques - Guidelines for the management of IT security - Part 4: Selection of safeguards"
- GMITS, ISO/IEC TR 13335-3:1998, "Information technology - Security techniques - Guidelines for the management of IT security - Part 3: Techniques for management of IT security"
- MAGERIT, "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información", MAP, versión 1.0, 1997

  http://www.csi.map.es/csi/pg5m20.htm
- GMITS, ISO/IEC TR 13335-2:1997, "Information technology - Security techniques - Guidelines for the management of IT security - Part 2: Managing and planning IT security"

6. Safeguards

Safeguards allow threats to be faced. There are different aspects in which a safeguard can act to achieve the objectives of limiting the impact and/or mitigating the risk:

[PR] procedures, which are always necessary. Sometimes there are sufficient procedures, but sometimes the procedures are one component of a more complex safeguard. Procedures are required both for operating preventive safeguards and for managing incidents and recovering from them. Procedures must cover such diverse aspects as the development of systems to the configuration of the equipment.

[PER] personnel policy, which is necessary when considering systems attended by persons. The personnel policy must cover from the phases for specifying the work post and selection, to continuous training.

Technical solutions, found frequently in the environment of information technologies and may be:

[SW] applications (software)

[HW] physical devices

[COM] protection of communications

[FIS] physical security, of premises and work areas.

The integral protection of an information system requires a combination of safeguards for the different aspects mentioned, and the final system must:

1. Be balanced in its different aspects.
2. Include suitable safeguards for each type of assets.
3. Take into account the suitable safeguards for the asset’s value dimension.
4. Take into account the suitable safeguards for the threat to be faced.

Safeguards, especially technical ones, vary with technological progress:

- Because new technologies appear.
- Because old technologies disappear.
- Because the [types of] assets to be considered change.
- Because the attackers’ possibilities develop.
- Because the catalogue of available safeguards develops.

As a result, this safeguards catalogue does not go into the choice of packages or products to be installed and is limited to determining requirements that must be met by the chosen practical solution.

6.1. General safeguards

These are those that refer to the good management of security with beneficial effects on all types of assets.

- Organisational security: roles, committees, etc.
- Corporate information security policy.
- Privilege management adjudication, revision and termination.
- Procedures for scaling and managing incidents.
- Procedures for continuity of operations: emergency and recovery.
- Auditing, recording (certification) and accreditation of the system.

6.2. Safeguards to protect the services

Life cycle	*Protection of value*
• Specification of the service • Development of the service • Deployment of the service • Operation of the service • Termination of the service	[A_S] → • Access control [T_S] → • Record of actions • Record of incidents [D] → • Continuity plan

Access control is a recurrent safeguard service that is applied to many types of assets: access to the services, access to the applications, access to the operating system, access to the information media, physical access to the installations, etc. All of these require an identification and authentication system that determines who is entering (whether a person or another program) and co-ordinates with the privilege management system.

There are many identification and authentication mechanisms and they can be combined in different ways; the notable ones include.

- **passwords:** useful for systems with little risk, or to complement other mechanisms.
- **digital certificates:** useful in systems that are exposed to repudiation threats.
- **tokens or cards:** useful in systems that have high risks or urgent availability requirements.
- **biometric features:** useful for identifying persons but not roles.

6.3. Safeguards to protect data/information

Organisation	*Protection of value*
• Personal, where relevant, • security document • Classification, where relevant, • Key management if encryption is used	[A_D] → • Access control • Electronic signature [T_D] → • Record of actions • Record of incidents [D] → • Back-up copies [I] • Detection and recovery [C] • Encryption (preventive) • Marking (prosecution)

6.4. Safeguards to protect applications (software)

Life cycle	***Protection of value***
• Functional and non-functional specification • Development • safe development • protection of source code • Acceptance and commissioning • Operation • changes and configuration management • incidents management • Approval/certification/accreditation	[I] • Protection against harmful code: viruses, Trojans, back doors, etc. [A_S, A_D] → • Access control [T_S, T_D] → • Record of actions

6.5. Safeguards to protect equipment (hardware)

Physical security	***Operating system security***
• Inventory • Control of arrivals and despatches • Destruction • Approval / certification / accreditation	• Configuration • internal equipment • equipment that leaves the premises • Maintenance [I] → • Protection against harmful code: viruses, spies, etc. • intrusion detection • Record of actions • Privilege management • Access control

6.6. Safeguards to protect communications

Life cycle	***Protection of value***
• Capacity planning • Acquisition and maintenance • Configuration • separation of networks • configuration of routers • configuration of firewalls • Key management if encryption is used • Intrusion detection • usage monitoring	• [D] → Continuity plan • [I] → Integrity guarantees • [C] → Encryption • [A_S] → Access control • [T_S] → Record of actions

6.7. Physical security

Protection of installations
• Protection against natural disasters   • earthquakes, floods, fire, storms, etc. • Protection against industrial accidents   • fire, flooding, etc.   • mechanical pollution: dust, vibrations   • electromagnetic pollution • Protection against electromagnetic radiation • Site protection: buildings, premises and work areas   • minimum signposting   • physical barriers   • protection of cabling • Access control: entry and exit of persons, equipment, information media, etc.

6.8. Safeguards for personnel

Life cycle
• Work post specification • Selection of staff. • Contractual conditions: responsibility for security • Continuous training

6.9. Outsourcing

The frontier between security services provided internally and those contracted to third parties is becoming increasingly flexible:

- Development of applications or equipment.
- Applications that are run in other places with remote access (ASP – Application Service Provisioning).
- Maintenance of programs and equipment.
- Managed security: remote monitoring and delegated management of incidents.
- Provision of communications services.
- Provision of data/information safekeeping services.
- Etc.

In all these cases, the aspects of the contractual relationship must be defined:

- SLA: service level agreement, if availability is a value.
- NDA: Non-disclosure agreement, if confidentiality is a value.
- Identification and qualification of the personnel in charge.
- Procedures for incident scaling and resolution.
- Termination procedure (duration of the assumed responsibilities).
- Assumption of responsibilities and penalties for non-compliance.

6.10. References

- “Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades”, MAP, 2004
  http://www.csi.map.es/csi/pg5c10.htm
- Centro Criptológico Nacional. Instrucción Técnica de Seguridad de las TIC (CCN-STIC-302). Interconexión de CIS que manejen información clasificada nacional en la Administración”. Versión 1.2. Marzo de 2004.
- ISO/IEC TR 15446:2004, “Information technology -- Security techniques -- Guide for the production of Protection Profiles and Security Targets”.
- GMITS, ISO/IEC IS 13335-1:2004, “Information technology - Security techniques - Guidelines for the management of IT security - Part 1: Concepts and models for information and communications technology security management”.
- “COBIT Security Baseline”, ISACA, 2004.
  http://www.isaca.org/
- “IT Baseline Protection Manual”, Federal Office for Information Security (BSI), Germany. October 2003.
  http://www.bsi.de/gshb/english/etc/index.htm
- “The Standard of Good Practice for Information Security”, ISF. 2003
  http://www.isfsecuritystandard.com/index_ns.htm
- NIST Special Publication 800-53: “Recommended Security Controls for Federal Information Systems”. 31 October, 2003.
  http://csrc.nist.gov/publications/index.html
- DoD Instruction 8500-2p, “Information Assurance (IA) Implementation”. Feb. 2003.
- UNE-ISO/IEC 17799:2002, “Tecnología de la Información. Código de Buenas Prácticas de la Gestión de la Seguridad de la Información”. 2002.
- “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/
- GMITS, ISO/IEC TR 13335-5: 2001, “Information technology - Security techniques - Guidelines for the management of IT security - Part 5: Management guidance of network security”

- GMITS, ISO/IEC TR 13335-4: 2000, "Information technology - Security techniques - Guidelines for the management of IT security - Part 4: Selection of safeguards"
- ISO/IEC 15408, "Information technology — Security techniques — Evaluation criteria for IT security", 1999.
  http://www.commoncriteriaportal.org/
- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.
- 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

Appendix 1. XML notation

XML formats are described using the following BNF[7] type notation:

- XML labels are shown as such.
- XML attributes are explained in the “attributes” section.
- { ... }* stands for 0 or more.
- { ... }+ stands for 1 or more.
- | separates alternatives.
- [...] means optional (0 or 1).
- #text# is literal contents: a name or a description
- the rest is mandatory

[7] **BNF**: Backus-Naur Form. This is a form of representing the grammar of a language. A BNF grammar consists of a series of production rules in which the left side results in the right side. The right side may explain the final terms or may refer to other production rules.

Appendix 2. Forms

The following sections provide forms for collecting the data in a risk analysis and management project.

For each type of asset:

- [D] data / information
- [S] services
- [SW] software
- [HW] hardware
- [COM] communication networks
- [SI] media
- [AUX] auxiliary equipment
- [L] installations
- [P] personnel

Reproduce the following forms, one per asset, for the relevant type.

[D] Data / information

[D] Data / information	
code:	**name:**
description:	
proprietary:	
responsible:	

type (tick on all those that apply):

- ( ) [vr] vital records
- ( ) [com] data of commercial interest
- ( ) [adm] data interesting for the public administration
- ( ) [int] internal management data
- ( ) [source] source code
- ( ) [exe] executable code
- ( ) [conf] configuration data
- ( ) [log] activity *log*
- ( ) [test] test data

- ( ) [per] personal data
  - ( ) [A] high level
  - ( ) [M] medium level
  - ( ) [B] basic level
- ( ) [label] classified data
  - ( ) [S] TOP SECRET
  - ( ) [R] SECRET
  - ( ) [C] CONFIDENTIEL
  - ( ) [DL] RESTREINT
  - ( ) [SC] UNCLASSIFIED

Valuation of the data/information, typically in the following security dimensions:

[I] integrity

[C] confidentiality

[A_D] authenticity of who accesses the data

[T_D] accountability of who accesses the data, when, and what they do

Valuation		
dimension	***value***	***reason***
[I]		
[C]		
[A_D]		
[T_D]		

Dependencies on assets below (children)	
asset:	**degree:**
why?:	

asset:	**degree:**
why?:	

asset:	**degree:**
why?:	

[S] Services

[S] Services	
code:	**name:**
description:	
responsible:	
type (tick on all those that apply): ( ) [anon] anonymous (no user identification) ( ) [pub] general public (no contract) ( ) [ext] for external users (subject to contract) ( ) [int] internal (internal users, and means) ( ) [cont] provided by a third party (not owned means) ( ) [www] world wide web ( ) [telnet] remote terminal ( ) [email] electronic mail ( ) [ftp] file transfer ( ) [edi] electronic data interchange ( ) [dir] directory service ( ) [idm] identity management ( ) [ipm] privilege management ( ) [pki] PKI – public key infrastructure	

Valuation of the services offered by the organisation to others, typically in the following dimensions:

[D] availability

[A_S] authenticity of who accesses the service

[T_S] accountability of who accesses the service, when and what they do

Valuation		
dimension	***value***	***reason***
[D]		
[A_S]		
[T_S]		

Dependencies on assets below (children)	
asset:	**degree:**
why?:	

asset:	**degree:**
why?:	

asset:	**degree:**
why?:	

[SW] Software

[SW] Software	
code:	**name:**
description:	
responsible:	

type (tick on all those that apply):

- ( ) [prp] in-house development *(in house)*
- ( ) [sub] sub-contracted development
- ( ) [std] standard *(off the shelf)*
    - ( ) [browser] web browser
    - ( ) [www] presentation server
    - ( ) [email_client] email client
    - ( ) [app] application server
    - ( ) [file] file server
    - ( ) [dbms] database management system
    - ( ) [tm] transactional monitor
    - ( ) [office] office computing
    - ( ) [av] anti virus
    - ( ) [backup] backup system
    - ( ) [os] operating system

Valuation (if applicable)		
dimension	***value***	***reason***

Dependencies on assets below (children)	
asset:	**degree:**
why?:	

asset:	**degree:**
why?:	

asset:	**degree:**
why?:	

[HW] Hardware

[HW] Hardware	
code:	**name:**
description:	
responsible:	
location:	
number:	
type (tick on all those that apply): ( ) [host] large equipment ( ) [mid] midsize equipment ( ) [pc] personal computing ( ) [mobile] mobile computing ( ) [pda] PDA ( ) [easy] easy to replace ( ) [data] that stores data ( ) [peripheral] peripheral ( ) [print] printer ( ) [scan] scanner ( ) [crypto] cryptographic device ( ) [network] network device ( ) [modem] model ( ) [hub] hub ( ) [switch] switch ( ) [router] router ( ) [bridge] bridge ( ) [firewall] firewall ( ) [pabx] branch exchange	

Valuation (if applicable)		
dimension	value	reason

Dependencies on assets below (children)	
asset:	**degree:**
why?:	

asset:	**degree:**
why?:	

asset:	**degree:**
why?:	

[COM] Communication networks

[COM] Communication networks	
code:	**name:**
description:	
responsible:	
location:	
number:	
type (tick on all those that apply): ( ) [PSTN] telephone network ( ) [ISDN] ISDN (digital network) ( ) [X25] X25 (data network) ( ) [ADSL] ADSL ( ) [pp] point to point ( ) [radio] wireless network ( ) [sat] satellite ( ) [LAN] local area network ( ) [MAN] metropolitan area network ( ) [Internet] Internet ( ) [vpn] virtual private network	

Valuation (if applicable)		
dimension	***value***	***reason***

Dependencies on assets below (children)	
asset:	**degree:**
why?:	

asset:	**degree:**
why?:	

asset:	**degree:**
why?:	

[SI] Media

[SI] Media	
code:	**name:**
description:	
responsible:	
location:	
number:	

type (tick on all those that apply):

- ( ) [electronic] electronic
  - ( ) [disk] disk
  - ( ) [disquette] diskettes
  - ( ) [cd] (CD-ROM)
  - ( ) [usb] USB devices
  - ( ) [dvd] DVD
  - ( ) [tape] magnetic tape
  - ( ) [mc] memory card
  - ( ) [ic] intelligent cards
- ( ) [non_electronic] non-electronic
  - ( ) [printed] printed paper
  - ( ) [tape] paper tape
  - ( ) [film] microfilm
  - ( ) [cards] punched cards

Valuation (if applicable)		
dimension	***value***	***reason***

Dependencies on assets below (children)	
asset:	**degree:**
why?:	

asset:	**degree:**
why?:	

asset:	**degree:**
why?:	

[AUX] Auxiliary equipment

[AUX] Auxiliary equipment	
code:	**name:**
description:	
responsible:	
location:	
number:	
type (tick on all those that apply): ( ) [power] power supplies ( ) [ups] uninterruptible power supplies ( ) [gen] electrical generators ( ) [ac] air conditioning ( ) [cabling] cabling ( ) [robot] robots ( ) [tape] ... tapes ( ) [disk] ... disks ( ) [supply] essential supplies ( ) [destroy] media destruction equipment ( ) [furniture] furniture: cupboards, , etc ( ) [safe] safe	

Valuation (if applicable)		
dimension	***value***	***reason***

Dependencies on assets below (children)	
asset:	**asset:**
why?:	

asset:	**asset:**
why?:	

asset:	**asset:**
why?:	

[L] Installations

[L] Installations	
code:	**name:**
description:	
responsible:	
location:	
number:	
type (tick on all those that apply): ( ) [site] site ( ) [building] building ( ) [local] premises ( ) [mobile] mobile platform ( ) [car] land vehicle: car, truck, etc. ( ) [plane] aircraft, airplane, etc. ( ) [ship] sea transport: ship, boat, etc. ( ) [shelter] shelter ( ) [channel] channel	

Valuation (if applicable)		
dimension	***value***	***reason***

Dependencies on assets below (children)	
asset:	**degree:**
why?:	

asset:	**degree:**
why?:	

asset:	**degree:**
why?:	

[P] Personnel

[P] Personnel	
code:	**name:**
description:	
number:	
type (tick on all those that apply): ( ) [ue] external users ( ) [ui] internal users ( ) [op] operators ( ) [adm] system administrators ( ) [com] communications administrators ( ) [dba] database administrators ( ) [des] developers ( ) [sub] sub-contractors ( ) [prov] providers	

Valuation (if applicable)		
dimension	***value***	***reason***

Dependencies on assets below (children)	
asset:	**degree:**
why?:	

asset:	**degree:**
why?:	

asset:	**degree:**
why?:	

Appendix 3. Value model

This Appendix describes an XML format for exchanging asset models between tools. This format must be understood as minimal in the sense that the tools may include information additional to this.

The information exchanged includes:

- Identification of the assets, with a code and descriptive name.
- Identification of the type(s) under which the asset is classified.
- Identification of the dependencies between assets.
- Valuation of the assets in different dimensions.

The notation is described in Appendix 1.

3.1. XML Syntax

```
model ::=
  <model>
  { datum }*
  { asset }*
  { dependency }*
  { valuation }*
  </model>

datum ::=
  <data key text />

asset ::=
  <asset code>
  #name#
  { type }+
  { datum }*
  </asset>

type ::=
  <type type />

dependency::=
  <dependency above below degree />

valuation::=
  <valuation asset dimension value />
```

attribute	***example***	***description***
code	`code=”X”`	Acronym that unequivocally identifies an asset in a model; that is, codes may not be repeated.
key	`key=”responsible”`	It appears as additional properties that provide information on the model or asset. Typically, keys appear such as author, organisation, relevant documentation, classification, location, date, version, etc.
text	`text=”JRP”`	Text associated with the key in a property.
type	`type=”T”`	T is the code of some of the defined types. See chapter 2.

attribute	***example***	***description***
above	`upper=”X”`	X is the code of an asset in the model.
below	`lower=”X”`	X is the code of an asset in the model.
degree	`grade=”number”`	A real number between 0.0 and 1.0.
asset	`asset=”X”`	X is the code of an asset in the model.
dimension	`dimension=”D”`	D is the code of one of the defined dimensions. See chapter 3.

value	`value=”[level]”`
	`value=”number”`
		It may be a symbolic level or a real amount, positive.
		See chapter 4.

Appendix 4. Reports

During the risk analysis and management project, a series of reports has been identified, for which an index is proposed below. Often, an executive report that excludes the details can be extracted from these reports.

4.1. Value model

Classification of the value represented by the assets for the organisation as well as the dependencies between the assets.

1. Project identification

   Code, description, owner, organisation.

   Version, date.

   Reference bibliography.
2. Assets

   2.1. Asset tree (dependency relationships)

   2.2. Valuation of the assets (own value)

   Indication of the reason for the valuation given to each asset in each dimension.
3. Detailed description

   For each asset:
   - classification (see chapter 2)
   - higher and lower assets
   - valuation: own value and accumulated value in each dimension

4.2. Risk map

List of the threats to which the assets are exposed.

1. Project identification

   Code, description, owner, organisation.

   Version, date.

   Reference bibliography.
2. Assets

   2.1. Asset tree (dependency relationships)

   2.2. Valuation of the assets (own value)

   Giving the reason for the valuation given to each asset in each dimension.
3. Threats per asset

   For each asset:
   - relevant threats (see chapter 5)
   - estimated degradation in each dimension
   - estimated annual frequency
4. Assets by threat

   For each threat:
   - assets affected
   - estimated degradation in each dimension
   - estimated annual frequency

4.3. Evaluation of safeguards

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

Work with respect to:

- a catalogue of safeguards (see chapter 5)

1. Project identification

   Code, description, owner, organisation.

   Version, date.

   Reference bibliography.

2. Safeguards (see chapter 5)

   An indication of the effectiveness of each safeguard against the risks it faces, at the level of detail considered appropriate.

   Show the historical development and the current planning.

4.4. Risk status

Classification of the assets by their residual risk, that is, what may happen considering the safeguards deployed.

1. Project identification

   Code, description, owner, organisation.

   Version, date.

   Reference bibliography.

2. Assets

   For each asset:

   1. Accumulated impact
   2. Accumulated risk
   3. Deflected impact
   4. Deflected risk

   Show the historical development and the current planning effects as appropriate.

4.5. Deficiencies report

Absence or weakness of the safeguards considered suitable to reduce the risk to the system.

Work with respect to:

- a catalogue of safeguards (see chapter 5)
- an effectiveness threshold

1. Project identification

   Code, description, owner, organisation.

   Version, date.

   Reference bibliography.

2. Safeguards

   An indication of the effectiveness of each safeguard against the risks it faces, for each one whose effectiveness is below a specified threshold, at the level of detail considered appropriate.

   Show the historical development and the current planning as appropriate.

4.6. Security plan

A group of security programmes that put the risk management decisions into action.

1. Reference framework
    - Security policy of the organization
    - List of standards and procedures
2. Persons responsible and their responsibilities (at the organisation level).
3. Security programmes

For each programme:

- generic objective
- priority or urgency
- location in time: when will it be carried out?
- safeguards involved
- unit responsible for carrying it out.
- estimate of costs
- estimate of resources
- estimate of impact for the organisation

When the moment arrives to carry them out, each security programme must detail:

- Its generic objective.
- The specific safeguards to be implemented or improved, detailing their quality, effectiveness and efficiency objectives.
- The list of scenarios for the impact and/or risk faced: assets affected, types of assets, threats faced, valuation of assets and threats and levels of impact and risk.
- The unit responsible for carrying it out.
- An estimate of costs, both financial and in terms of undertaking effort, bearing in mind,
- Acquisition cost (for products), or contracting costs (for services) or development costs (for turnkey solutions), considering that it may be necessary to evaluate various alternatives.
- Costs of initial implementation and maintenance over time.
- Costs of training, for both operators and users, as relevant.
- Operating costs.
- Impact on the organisation’s productivity.
- A list of sub-tasks to be carried out, bearing in mind:
- Changes in standards and development of procedures.
- Technical solution: programs, equipment, communications and premises.
- Deployment plan.
- Training plan.
- An estimate of the undertaking time from start to putting into operation.
- An estimate of the risk status (impact and residual risk on completion).

- A system of effectiveness and efficiency indicators that continuously show the desired quality of the performance of the security function and its development over time.