ISO/IEC 27005:2011

10.6.2015

How to perform risk analysis and management using PILAR

1 References

ISO/IEC 27005:2011

Information technology -- Security techniques -- Information security risk management

PILAR

Risk management tool.
http://www.pilar-tools.com

1.1 Other references

ISO Guide 73:2009

Risk management -- Vocabulary

ISO/IEC 27001:2013

Information technology -- Security techniques -- Information security management systems – Requirements

ISO/IEC 27002:2013

Information technology -- Security techniques -- Code of practice for information security controls

ISO 31000:2009

Risk management -- Principles and guidelines

MAGERIT

Methodology for Information Systems Risk Analysis and Management
V3, October, 2012
http://administracionelectronica.gob.es/

2 Overview

2.1 27005

Copied from ISO 27005:2011 introduction:

> This International Standard provides **guidelines** for information security risk management in an organization, supporting in particular the requirements of an information security management (ISMS) according to ISO/IEC 27001. However, this International Standard **does not provide any specific method** for information security risk management. It is up to the organization to define their approach to risk management, depending for example on the scope of the ISMS, context of risk management, or industry sector. **A number of existing methodologies can be used** under the framework described in this International Standard to implement the requirements of an ISMS.

The 27005 standard doesn't specify, recommend or even name any specific risk management method. It does however imply a continual process consisting of a structured sequence of activities, some of which are iterative:

- Establish the risk management context (e.g. the scope, compliance obligations, approaches/methods to be used and relevant policies and criteria such as the organization's risk tolerance or appetite);
- Quantitatively or qualitatively assess (i.e. identify, analyze and evaluate) relevant risks, taking into account the information assets, threats, existing controls and vulnerabilities to determine the likelihood of incidents or incident scenarios, and the predicted business consequences if they were to occur, to determine a 'level of risk';
- Treat (i.e. modify [use information security controls], retain [accept], avoid and/or share [with third parties]) the risks appropriately, using those 'levels of risk' to prioritize them;
- Keep stakeholders informed throughout the process; and
- Monitor and review risks, risk treatments, obligations and criteria on an ongoing basis, identifying and responding appropriately to significant changes.

Extensive appendices provide additional information, primarily examples to demonstrate the recommended approach.

2.2 PILAR

PILAR is a software tool. It was designed to implement the methodology MAGERIT, quite similar to 27005.

This document shows how to use this tool to manage risk according to ISO 27005.

2.3 Activities

All risk management activities are presented from Clause 7 to Clause 12.

- Clause 7 – Context establishment
- Clause 8 – Risk assessment
- Clause 9 – Risk treatment
- Clause 10 – Risk acceptance
- Clause 11 – Risk communication and consultation
- Clause 12 – Risk monitoring and review

3 Context establishment

Clause 7 and Annex A.

There are a number of administrative tasks that are out of scope of the tool.

For tool's sake:

- Identify essential assets: the value to protect. In Annex B, these essential assets are called "primary".
- Identify other assets in your information system: its scope. PILAR provides a big library of asset classes that may help to qualify your assets. In Annex B, this non-essential assets are called "supporting assets".
- Define boundaries: logical (interconnections) and physical (facilities).
- Valuate essential assets using criteria approved by the management. PILAR provides a big set of usual criteria. You may use a subset, add/or extend the criteria provided.

PILAR combines "risk evaluation criteria" and "impact criteria" into the asset evaluation screen where you determine the level to protect each dimension of security (availability, integrity, confidentiality …)

PILAR does not automate "risk acceptance criteria". These criteria are rules for management to prioritize and determine the treatment to apply to the risks analyzed by PILAR.

4 Risk assessment

Clause 8.

Identification and valuation of assets and impact assessments are discussed in Annex B. Annex C gives examples of typical threats and Annex D discusses vulnerabilities and methods for vulnerability assessment. Examples of information security risk assessment approaches are presented in Annex E. Constraints for risk modification are presented in Annex F.

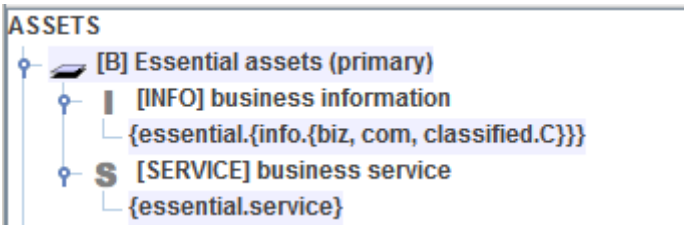
Risk assessment:

- risk identification
- risk analysis
- risk evaluation

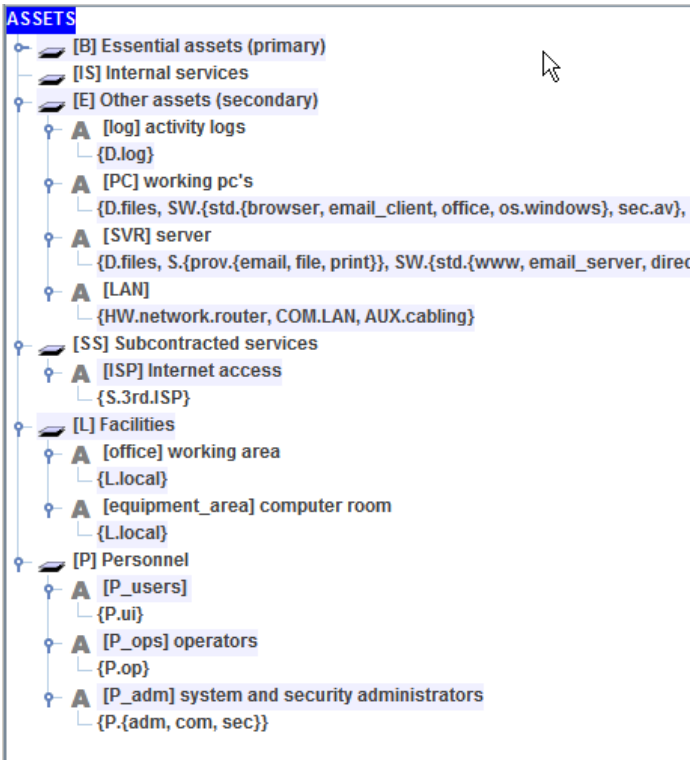
4.1 Risk identification

4.1.1 Identification of assets

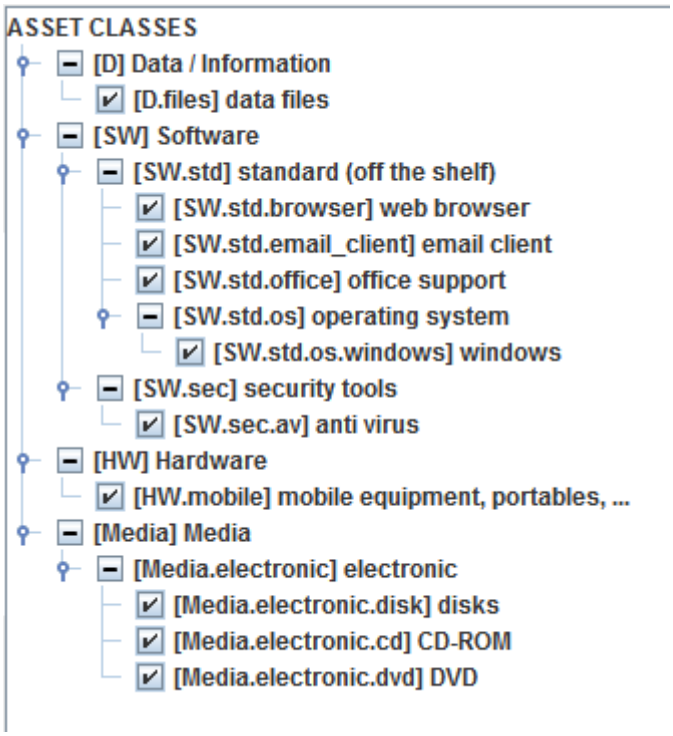
Identify essential assets: the value to protect; the primary assets according to Annex B.



Identify other assets supporting your information system: its scope. PILAR provides a big library of asset classes that may help to qualify your assets.



Assets may be qualified to a large extend specifying characteristics that may influence risk analysis. For instance, for workers' portable computers:



PILAR translates the valuation of the essential assets into the valuation of every asset, either using security domains (coarse grain) or dependencies (fine grain).

asset / security domain	[A]	[I]	[C]	[Auth]	[Acc]
[example]					
[essential] Essential assets	[4]	[5]	[7]	[5]	[4]
[INFO] business information		[5]	[7]	[5]	[4]
[SERVICE] business service	[4]				
Security domains					
[base] Base	[4]	[5]	[7]	[5]	[4]

asset	[A]	[I]	[C]	[Auth]	[Acc]
ASSETS					
[B] Essential assets (primary)					
[INFO] business information	[4]	[5]	[7]	[5]	[4]
[SERVICE] business service	[4]	[5]	[7]	[5]	[4]
[IS] Internal services					
[E] Other assets (secondary)					
[log] activity logs		[4]		[4]	
[PC] working pc's	[n.a.]	[5]	[7]	[5]	[4]
[SVR] server	[4]	[5]	[7]	[5]	[4]
[LAN]	[4]	[5]	[7]	[5]	[4]
[SS] Subcontracted services					
[ISP] Internet access	[4]	[5]	[7]	[5]	[4]
[L] Facilities					
[office] working area	[4]	[5]	[7]	[5]	[4]
[equipment_area] computer room	[4]	[5]	[7]	[5]	[4]
[P] Personnel					
[P_users]	[4]	[5]	[7]	[5]	[4]
[P_ops] operators	[4]	[5]	[7]	[5]	[4]
[P_adm] system and security administrators	[4]	[5]	[7]	[5]	[4]

4.1.2 Identification of threats

PILAR provides a catalog of standard threats. This catalog may be adjusted either adding new threats, of discarding some threats of the catalog. PILAR can be operated in “automatic mode” where she applies a standard profile, that is perfect for a first approach, and may be adjusted later on for system specific circumstances.

[SVR] server		100%	100%	100%	100%	100%
[N.1] Fire	L	100%				
[N.2] Water	L	50%				
[N.*] Other natural disasters	L	100%				
[I.5] Hardware or software failure	M	50%				
[I.6] Power interruption	M	100%				
[I.7] Unsuitable temperature or humidity cond	M	100%				
[I.10] Media degradation	M	100%				
[E.1] User errors	M	1%	5%	10%		
[E.2] System / Security administrator errors	M	20%	20%	20%		
[E.8] Malware diffusion	M	10%	10%	10%		
[E.18] Destruction of information	M	100%				
[E.19] Information leaks	M			10%		
[E.20] Software vulnerabilities	M	1%	20%	20%		
[E.21] Defects in software maintenance / upd	H	1%	1%			
[E.23] Defects in hardware maintenance / upd	M	100%				
[E.24] System failure due to exhaustion of res	H	50%				
[E.25] Equipment loss	M	10%		50%		
[A.5] Masquerading of identity	M		50%	50%	100%	
[A.6] Abuse of access privileges	M	10%	10%	50%	100%	
[A.7] Misuse	M	1%	1%	1%		
[A.8] Malware diffusion	M	100%	100%	100%		
[A.11] Unauthorised access	M	10%	1%	50%	100%	
[A.13] Repudiation (denial of actions)	H					100%
[A.15] Deliberate alteration of information	H		100%			
[A.18] Destruction of information	M	100%				
[A.19] Disclosure of information	M			10%		
[A.22] Software manipulation	M	50%	100%	100%		
[A.23] Hardware manipulation	L	50%		50%		
[A.24] Denial of service	M	100%				
[A.25] Theft	M	10%		100%		
[A.26] Destructive attack	M	10%				

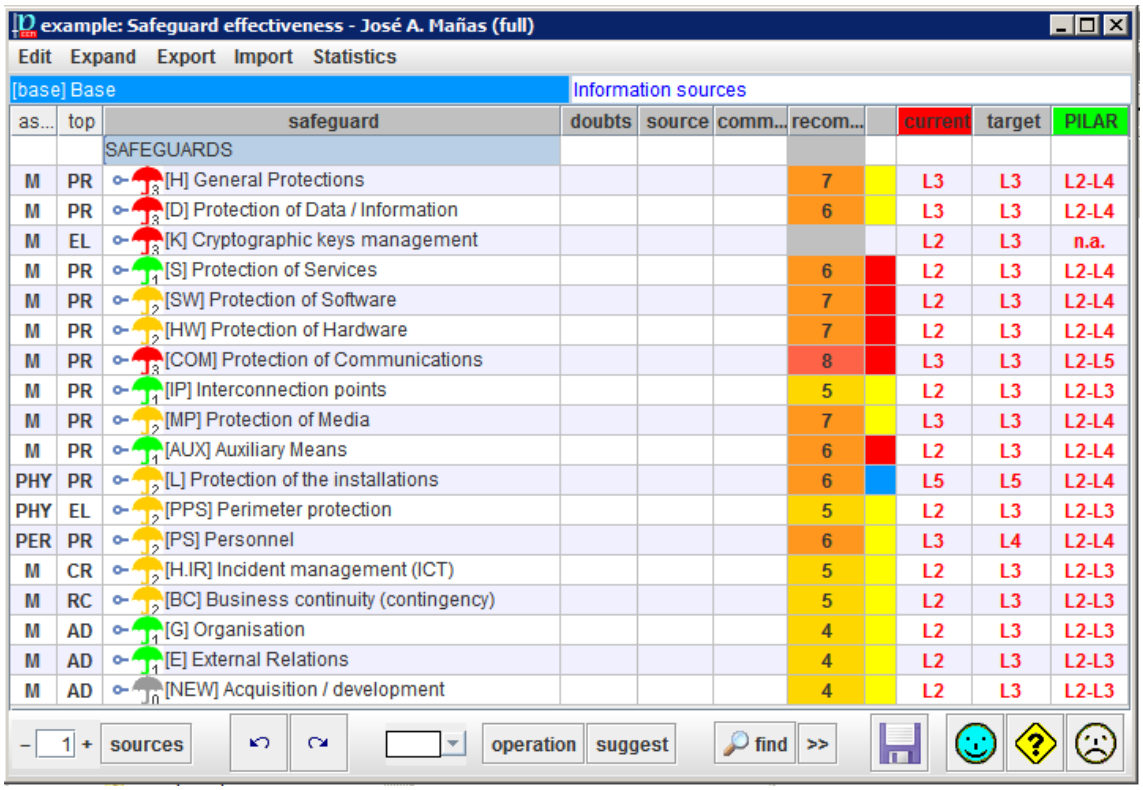
4.1.3 Identification of existing controls

PILAR provides a large catalog of safeguards that are mapped onto controls as provided in ISO 27002.Either one or the other view can be used to input information about the security measures in service.

PILAR uses maturity model to qualify the safeguards:

level	name
L0	non existent
L1	initial / ad hoc
L2	repeatable, but intuitive
L3	defined process
L4	managed and measurable
L5	optimized

In PILAR



4.1.4 Identification of vulnerabilities

Vulnerabilities may be of two types

technical vulnerabilities

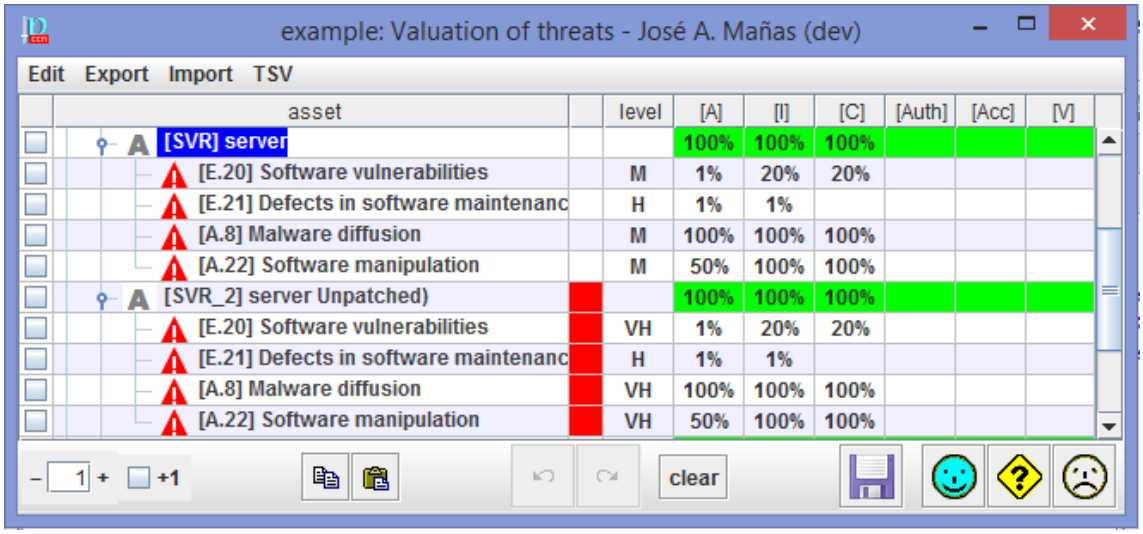
> weakness of an asset; e.g. lack of software patching

organizational vulnerabilities

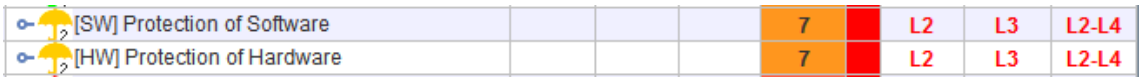
> weakness of a control; e.g. weak authentication of users

Both types are discovered by inspection, either with the help of some vulnerability scanning tool, or manually.

Technical vulnerabilities are collected in PILAR as increased likelihood that a thread occurs. For instance, if we have two servers, one of them is up-to-date, while the other one is missing some OS updates:



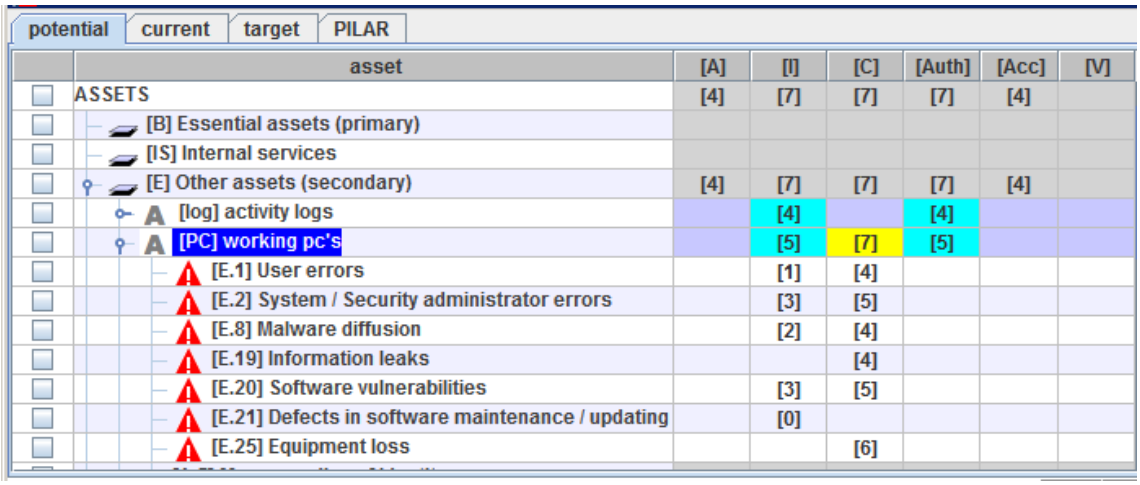
Organizational vulnerabilities are identified in PILAR as countermeasures that are applicable, but which maturity is not high enough.



Both types of vulnerability lead to higher risks.

4.1.5 Identification of consequences

PILAR estimates the consequences of a threat on an asset, both potentially (without taking safeguards into consideration), and present (taking into account the existence of safeguards or its absence or vulnerability).



4.2 Risk analysis

For the threats in the catalog, PILAR provides standard vales of likelihood and impact, taking into account the identified assets, their attributes, and the value each asset has to protect. PILAR can be operated in “automatic mode” where she applies a standard profile, that is perfect for a first approach, and may be adjusted later on for system specific circumstances.

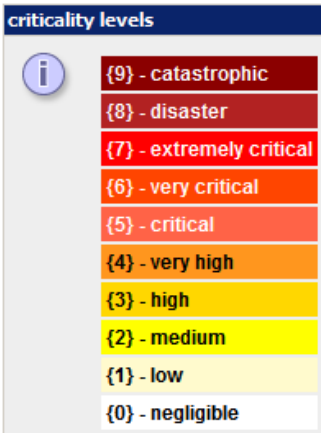
PILAR evaluates the risk associated to each threat on each asset, and provides a risk-level that is a combination of the likelihood and the consequences of the occurrence of each threat on each asset. Risk items are sorted by relevance to focus on most important ones.

PILAR may use a qualitative model or a quantitative mode. The user selects.

4.3 Risk evaluation

PILAR does not automate evaluation since this is a management activity. PILAR provides information on the risk level of each potential threat, both on each asset (accumulated risk level) and translated onto the essential assets of the organization (deflected risk levels) with the corresponding backtracking to trace the point of attack onto the final consequences for the business.

PILAR provides detailed information on the facts. It is the responsibility of the management bodies to interpret the consequences of incidents on the business.



potential | current | target | PILAR

asset	[A]	[I]	[C]	[Auth]	[Acc]	[V]
ASSETS	{3.7}	{5.1}	{5.4}	{5.1}	{3.9}	
[B] Essential assets (primary)						
[IS] Internal services						
[E] Other assets (secondary)	{3.7}	{5.1}	{5.1}	{5.1}	{3.9}	
[log] activity logs		{4.5}		{4.2}		
[PC] working pc's		{4.5}	{5.1}	{3.9}		
[E.1] User errors		{1.6}	{3.3}			
[E.2] System / Security administrator errors		{2.7}	{3.8}			
[E.8] Malware diffusion		{2.1}	{3.3}			
[E.19] Information leaks			{3.3}			
[E.20] Software vulnerabilities		{2.7}	{3.8}			
[E.21] Defects in software maintenance / updating		{1.2}				
[E.25] Equipment loss			{4.5}			

5 Risk treatment

Clause 9.

Risk treatment is an art where you may opt between several, non-exclusive, alternatives:

risk modification

> The level of risk should be managed by introducing, removing or altering controls so that the residual risk can be reassessed as being acceptable.
> PILAR permits to change the level or maturity of the safeguards, or to change the protection means when there are several alternative options (e.g. identification and authentication mechanism).

risk retention

> The decision on retaining the risk without further action should be taken depending on risk evaluation.
> In PILAR, just do nothing.

risk avoidance

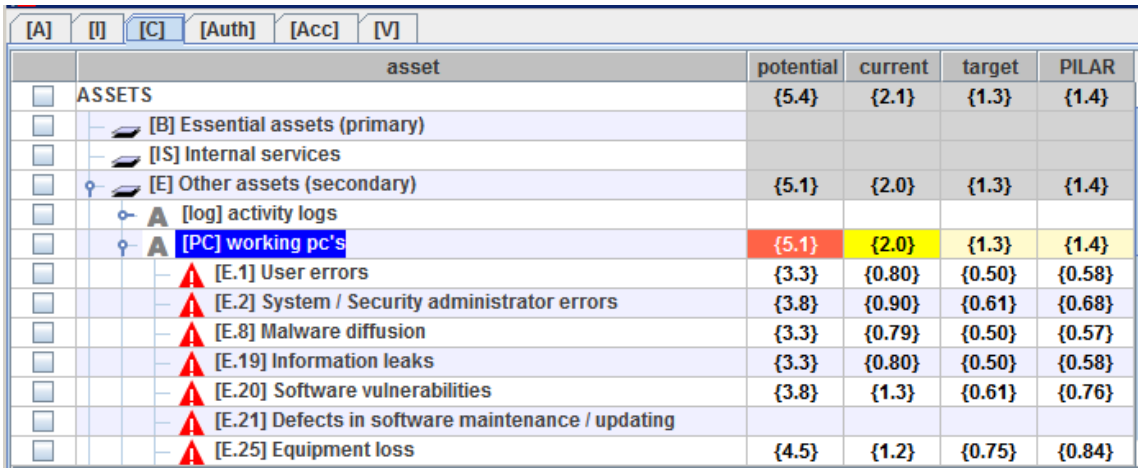
> The activity or condition that gives rise to the particular risk should be avoided.
> Usually this means changing the collection of assets, removing from our system those that we are not ready to protect sufficiently.

risk sharing

> The risk should be shared with another party that can most effectively manage the particular risk depending on risk evaluation.

In PILAR this means moving assets from material elements to protect onto external contracts to manage (that is externalizing assets). Or it means changing the valuation of consequences from being supported entirely by us onto being only partly supported (e.g. insurance)

PILAR provides a concept of “phases” where you can show along a timeline the changes in safeguards. This is especially useful for risk modification activities where residual risk evolves as security plans are executed.



asset	potential	current	target	PILAR
ASSETS	{5.4}	{2.1}	{1.3}	{1.4}
[B] Essential assets (primary)				
[IS] Internal services				
[E] Other assets (secondary)	{5.1}	{2.0}	{1.3}	{1.4}
[log] activity logs				
[PC] working pc's	{5.1}	{2.0}	{1.3}	{1.4}
[E.1] User errors	{3.3}	{0.80}	{0.50}	{0.58}
[E.2] System / Security administrator errors	{3.8}	{0.90}	{0.61}	{0.68}
[E.8] Malware diffusion	{3.3}	{0.79}	{0.50}	{0.57}
[E.19] Information leaks	{3.3}	{0.80}	{0.50}	{0.58}
[E.20] Software vulnerabilities	{3.8}	{1.3}	{0.61}	{0.76}
[E.21] Defects in software maintenance / updating				
[E.25] Equipment loss	{4.5}	{1.2}	{0.75}	{0.84}

6 Risk acceptance

Clause 10.

PILAR provides detailed information on the facts, both potential and residual risk levels. It is the responsibility of the management bodies to take the decisions.

7 Risk communication

Clause 11.

Risk communication is an activity to achieve agreement on how to manage risks by exchanging and/or sharing information about risk between the decision-makers and other stakeholders. The information includes, but is not limited to the existence, nature, form, likelihood, severity, treatment, and acceptability of risks.

PILAR provides the capability of reporting the results of the risk analysis and treatment plan. You have both prebuilt report templates, and a template language to produce personalized reports. Analysis can be exported to excel, xml, and SQL databases for further elaboration.

8 Risk monitoring

Clause 12.

Risks are not static. Threats, vulnerabilities, likelihood or consequences may change abruptly.

PILAR is an automated tool where you can introduce changes in assets, threats, or safeguarding architecture to calculate updated risk levels.

9 Annexes

Additional information for information security risk management activities is presented in the annexes. The context establishment is supported by Annex A (Defining the scope and

boundaries of the information security risk management process). Identification and valuation of assets and impact assessments are discussed in Annex B. Annex C gives examples of typical threats and Annex D discusses vulnerabilities and methods for vulnerability assessment. Examples of information security risk assessment approaches are presented in Annex E.

All annexes are informative.

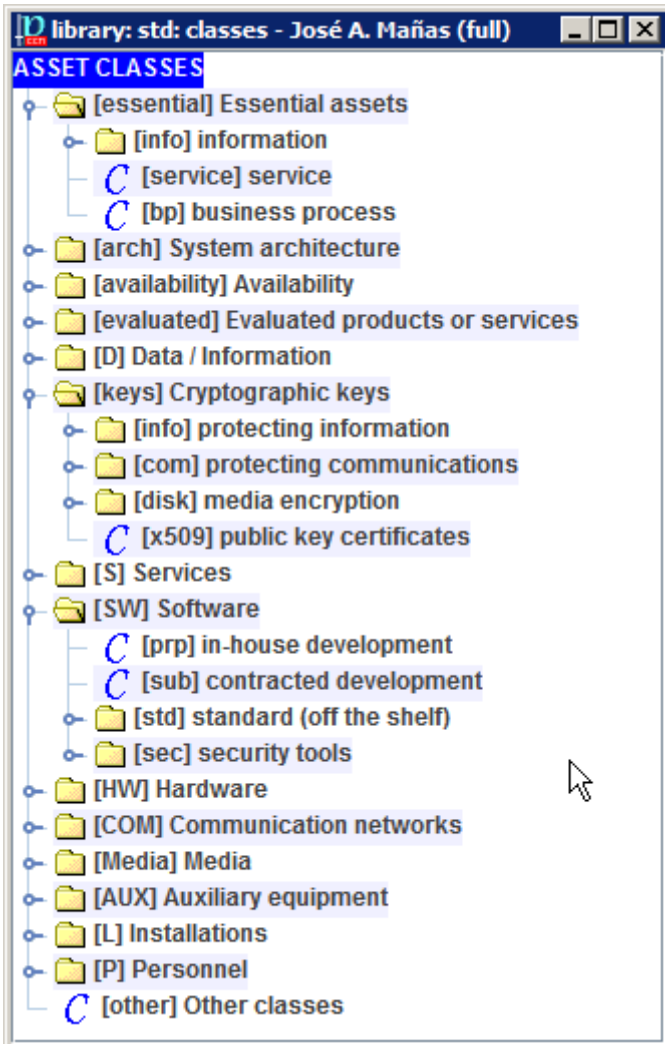
9.1 Annex A – Scope and boundaries

The study of the organization recalls the characteristic elements defining the identity of an organization. This concerns the purpose, business, missions, values and strategies of this organization. These should be identified together with the elements contributing to their development (e.g. subcontracting).

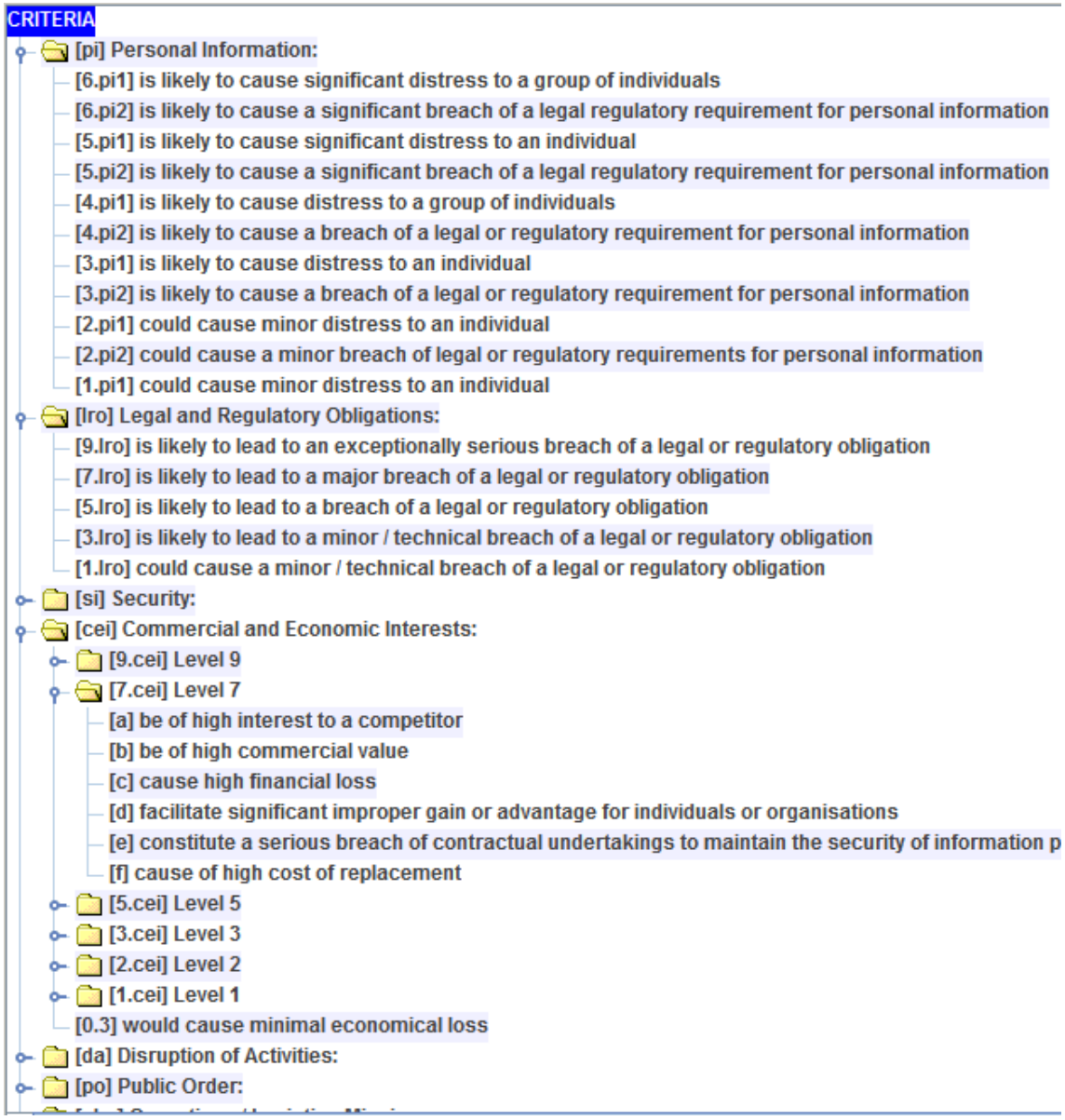
The difficulty of this activity lies in understanding exactly how the organization is structured. Identifying its real structure will provide an understanding of the role and importance of each division in achieving the organization's objectives.

9.2 Annex B – Identification and valuation of assets and impact assessment

PILAR provides a catalog of typical assets. Users may extend this catalog to meet specific needs.



PILAR provides a catalog of typical valuation criteria. Users may extend this catalog to meet specific needs:



9.3 Annex C – Examples of typical threats

PILAR provides a catalog of typical valuation criteria. Users may extend this catalog to meet specific needs:

9.4 Annex D – Vulnerabilities and vulnerability assessment

PILAR provides a large catalog of controls on information security, including organizational, technical, physical, and personnel:

9.5 Annex E – Information security risk assessment approaches

PILAR permits a wide range of options to perform a risk analysis

- You may run a very high level analysis where assets are whole subsystems, and there is no fine grain allocation of incidents.
- You may run a very low level analysis, breaking down complex assets into components, and specifying very precisely which information and service depends on each asset.
- Most usually you will run a high level analysis as a first approach to discover hot assets, and later refine those problems with further detail, until the problem is focused and a solution is identified.

- You may use the whole catalogue of threats in PILAR, or you may focus on a few, or extend with further detail. Most usually, you will start with the standard thread, remove those that are not source of high risk to focus the analysis on current issues, and perhaps extend a few for specific concerns or scenarios.

- You may run a qualitative analysis, or a quantitative one. Qualitative analysis is most frequently a must in order to discover where the qualitative problems are. A quantitative analysis may be run later on to take into account the accumulation of risk on single points of failure: assets that do not support any high risk, but do support a large number of small risks.

10 Glossary

asset

anything that has value to the organisation

attack

attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

availability

property of being accessible and usable upon demand by an authorized entity

confidentiality

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

consequence

outcome of an event affecting objectives

control

means of managing risk, including policies, procedures, guidelines, practices or organisational structures, which can be of administrative, technical, management, or legal nature

integrity

property of protecting the accuracy and completeness of assets

level of risk

magnitude of a risk expressed in terms of the combination of consequences and their likelihood

likelihood

chance of something happening

risk

effect of uncertainty on objectives

statement of applicability

documented statement describing the control objectives and controls that are relevant and applicable to the organisation's ISMS

threat

potential cause of an unwanted incident, which may result in harm to a system or organisation

vulnerability

weakness of an asset or control that can be exploited by one or more threats.

11 Annex – Maturity levels

level	name	description
L0	non existent	At maturity level L0 there is nothing.
L1	initial / ad hoc	At maturity level L1, safeguards exist, but are not managed. Success in these organizations depends on good luck. In this case, organizations frequently exceed the budget and schedule. Level L1 success depends on having high quality people.
L2	repeatable, but intuitive	At maturity level L2, safeguards effectiveness depends on good luck and good will on the part of the people. Successes are repeatable, but there is no plan for failures beyond heroic reaction. There is still a significant risk of exceeding cost and time estimates.
L3	defined process	Safeguards are deployed and managed. There are known policies and procedures to guarantee professional reaction to incidents, and due maintenance of the protection services. The chances to survive are high, up to the limits of the unknown. Success is more than good luck: it is deserved.
L4	managed and measurable	Using precise measurements, management can effectively control the effectiveness and efficiency of the safeguards. In particular, management can identify ways to set quantitative quality goals. At maturity level L4, the performance of processes is controlled using statistical and other quantitative techniques, and is quantitatively predictable. At maturity level L3, processes were only qualitatively predictable.

level	name	description
L5	optimized	Maturity level L5 focuses on continually improving process performance through both incremental and innovative technological improvements. Quantitative process-improvement objectives for the organization are established, continually revised to reflect changing business objectives, and used as criteria in managing process improvement. The effects of deployed process improvements are measured and evaluated against the quantitative process-improvement objectives. Both the defined processes and the organization's set of standard processes are targets of measurable improvement activities. Process improvements to address common causes of process variation and measurably improve the organization's processes are identified, evaluated, and deployed. Optimizing processes that are nimble, adaptable and innovative depends on the participation of an empowered workforce aligned with the business values and objectives of the organization. The organization's ability to rapidly respond to changes and opportunities is enhanced by finding ways to accelerate and share learning.