# PILAR – Users' Manual (2021.2)

June, 2021

# Contenido

# Chapter I – Introduction

## I.1 Summary

Risk analysis is about identifying potential and residual risks in a communications and information system (CIS). Risk is about likely harm on organization's information and services.

Risk analysis provides information for deciding on resource allocation, either technical or other means to protect organization.

Risk analysis is a methodical approach:

1. identify the value to protect
2. identify the CIS elements that support that value, where attacks may cause harm
3. set up security measures to protect against attacks
4. calculate indicators to help decision makers

PILAR implements the methodology Magerit: http://administracionelectronica.gob.es/

## I.2 Installation

### I.2.1 Java environment

You need a

JRE - Java Runtime Environment

- visit [http://java.com]
- and follow the instructions
    - step 1: unloading
    - step 2: installation
    - step 3: test

### I.2.2 PILAR for Windows

You may install PILAR as an administrator or as a plain user. Files may be installed anywhere. If you have administrator privileges, the files may go into "Program Files" for everybody, and the registry may have a number of entries to associate PILAR to .mgr extensions.

- run `pilar_<version>_<profile>_<lang>.exe`
- follow the instructions to install in your preferred directory
  (several languages may share the same installation directory)
- when the installation completes, there will be a file
  `pilar.exe`
  where you decided to install the software.

### I.2.3 PILAR for UNIX, Linux, …

Usually, java is already installed as part of the system software.

- run `pilar_linux_<version>_<profile>_<lang>.jar`

- follow the instructions to install in your preferred directory
  (several languages may share the same installation directory)
- when the installation completes, there will be a file
  `pilar.jar`
  where you decided to install the software.

### I.2.4 PILAR for Mac OS X

Java is already installed as part of the system software.

- run `pilar_mac_<version>_<profile>_<lang>.app`
- follow the instructions to install in your preferred directory
  (several languages may share the same installation directory)
- when the installation completes, there will be a file
  `pilar_<version>.app`

## I.3 Usage

Run `pilar`:

- it will ask for a car (a file with extension .CAR); you may find it in the directory where you installed the software
  e.g. CIS_en.car

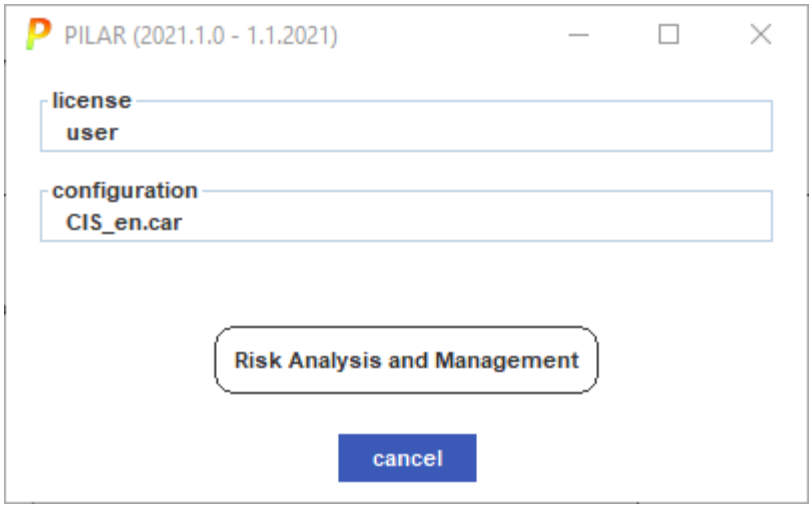
The CAR file specifies some context information for the execution of the software. You may edit it with any text editor.

```
$ find . -name *.car
./PilarBasic_7.3/BASIC_ens.car
./PilarBasic_7.3/BASIC_es.car
./PilarMicro_7.2/MICRO_27000_en.car
./PilarMicro_7.2/MICRO_ens.car
./PilarMicro_7.3/MICRO_27000_en.car
./PilarMicro_7.3/MICRO_27000_es.car
./PilarMicro_7.3/MICRO_eell.car
./PilarMicro_7.3/MICRO_ens.car
./PILAR_5.4/STIC_ens.car
./PILAR_6.3/STIC_ens.car
./PILAR_7.1/STIC_ens.car
./PILAR_7.2/CIS_en.car
./PILAR_7.2/STIC_ens.car
./PILAR_7.2/STIC_es.car
./PILAR_7.3/STIC_ens.car
./PILAR_7.3/STIC_es.car
```

For further information, see “personalisation” at

https://www.pilar-tools.com/en/tools/pilar/doc.html

### I.3.1 On the first screen




**license**

Displays current license, including expiration date if any.

Click to select a license.

**configuration**

Displays the current configuration file (CAR).

Click to select a different configuration.

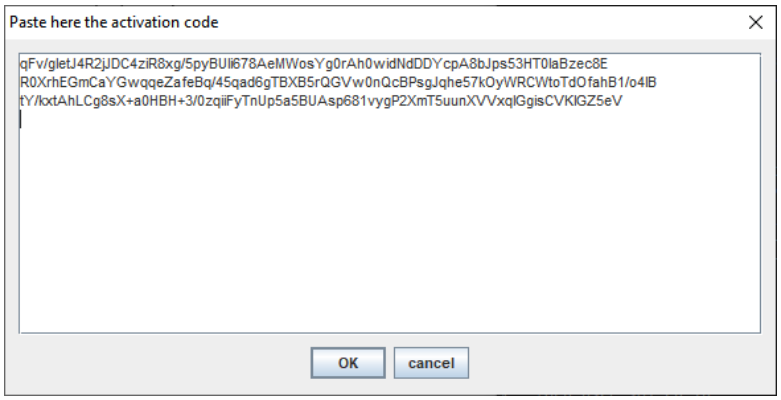
Select “Risk Analysis and Management” to start.

### 1.3.2. License

When right-click on “license” box you are presented with the following options

**activation code**

If you received an activation code, paste it!




NOTE: Activation codes require an Internet connection to get a valid license.

**license file**

If you received a LIC file, choose it!

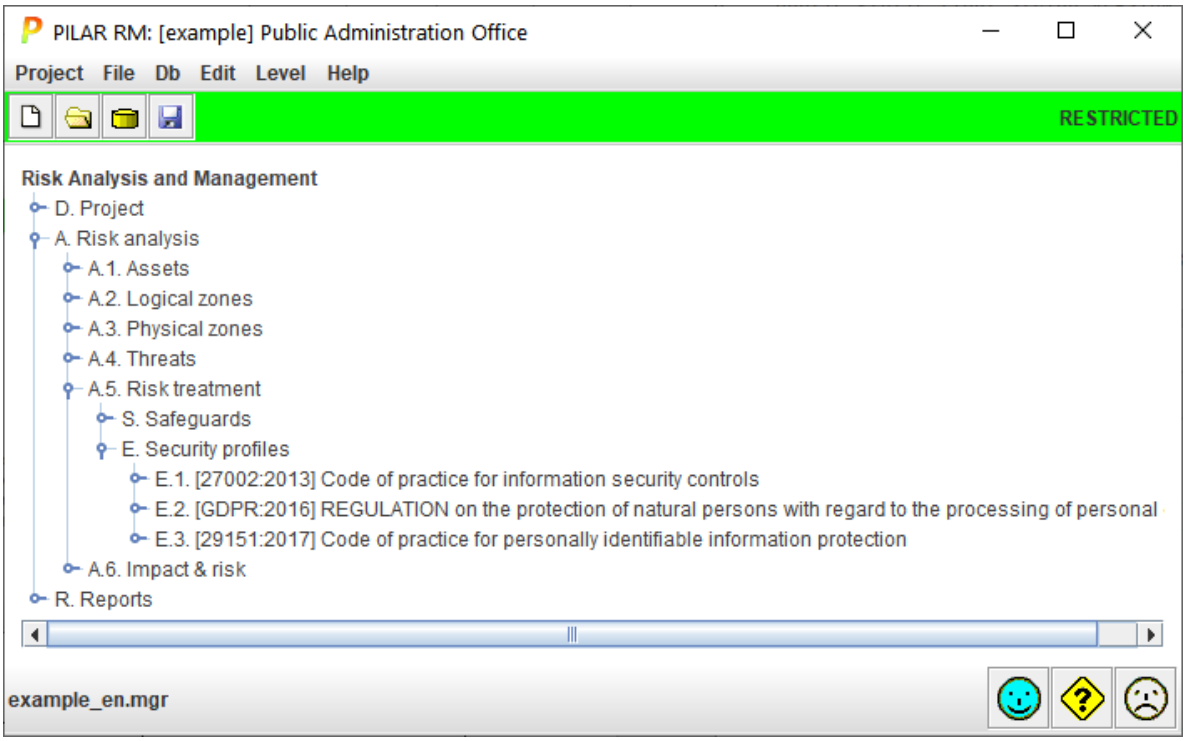
**evaluation license**

You may auto-generate a temporary evaluation license for 30 days.

**reset**

Select this option for PILAR to forget last selection and restart license validation.

# Chapter II – Basic user




## II.1 Configuration options

These are the most frequently used options:

| Edit > options | select | |
|---|---|---|
| valuation | assets + domains | you rate essential assets distributed in security domains |
| threats | automatic | PILAR applies a standard attack profile |
| project phases | linked | the rating in one phase is copied into next phases, unless modified |
| likelihood | level | optional: changes presentation |
| effects | percent | optional: changes presentation |
| maturity | maturity | optional: changes presentation |
| phases | check PILAR | PILAR recommends reasonable values |
| cross dimension value transfer | check cross dimension value transfer | PILAR transfer requirements from one security dimension to another(s) as appropriate |

## II.2. Essential assets

### II.2.1. Essential assets

Essential assets are those information and services managed by the information system. They represent the requirements of the risk owners: the security requirements. Essential assets exist before any implementation is detailed by means of supporting assets.

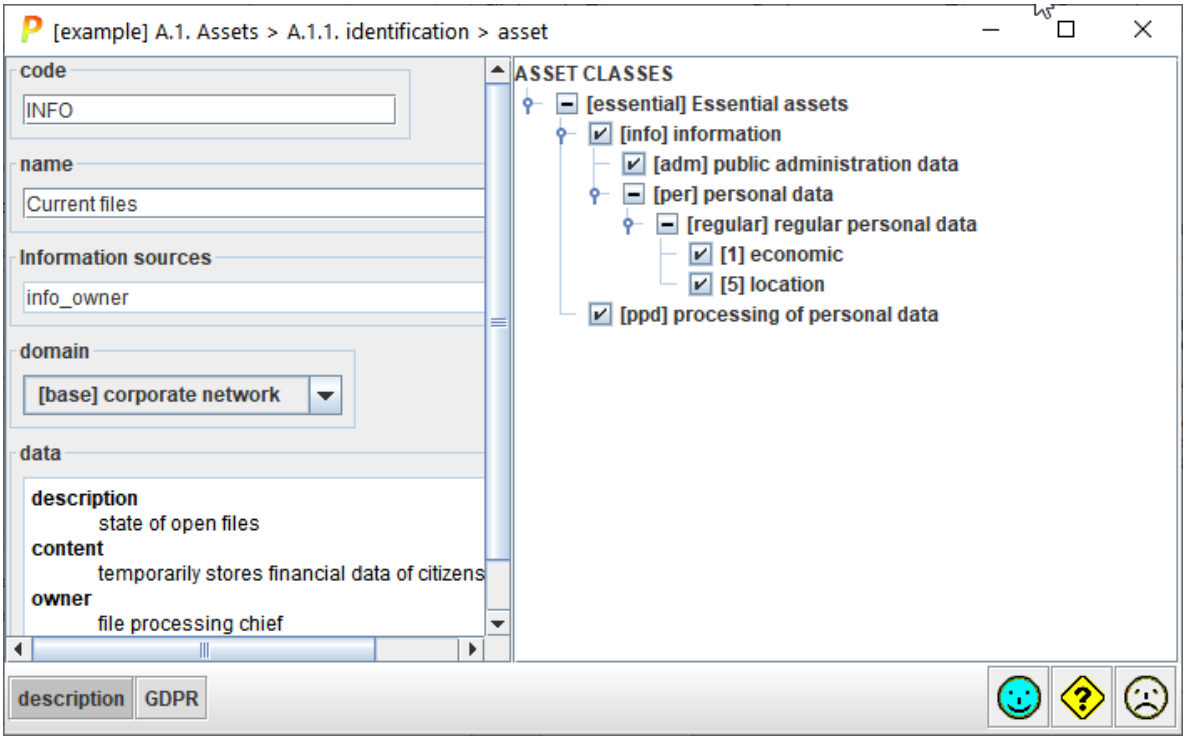
Essential assets may be of the 'information' type, or of the 'service' type, or even a mix of both. What is important is that they are identified by a name and are understood by governance and managerial people.

Essential assets impose security requirements, called levels in PILAR. Information assets typically are concerned with integrity and confidentiality. Service assets are typically concerned with availability. And both can be concerned with authenticity and accountability.

### II.2.2. Identificación & Caracterización

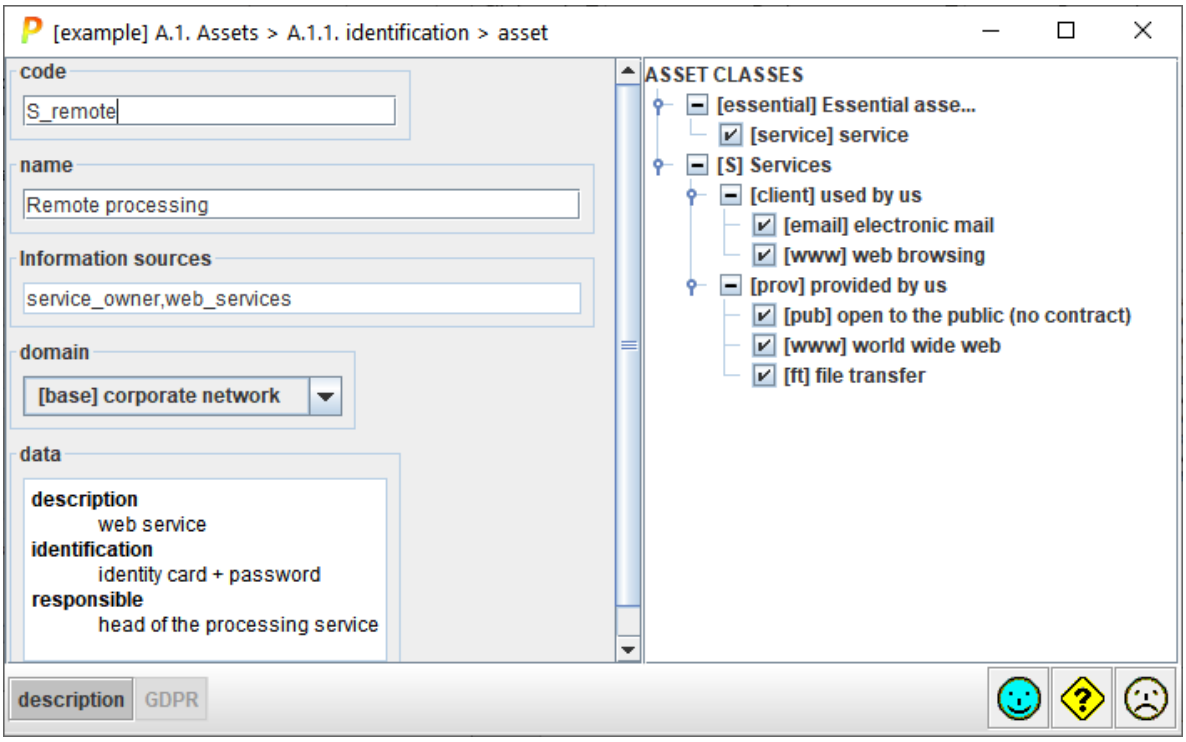
Risk analysis > Assets > Identification

- Layers > New layer
  - [B] Essential assets
- Assets > New asset
  - [INFO] Business information
  - Select classes as appropriate (typically, only under [essential.info]

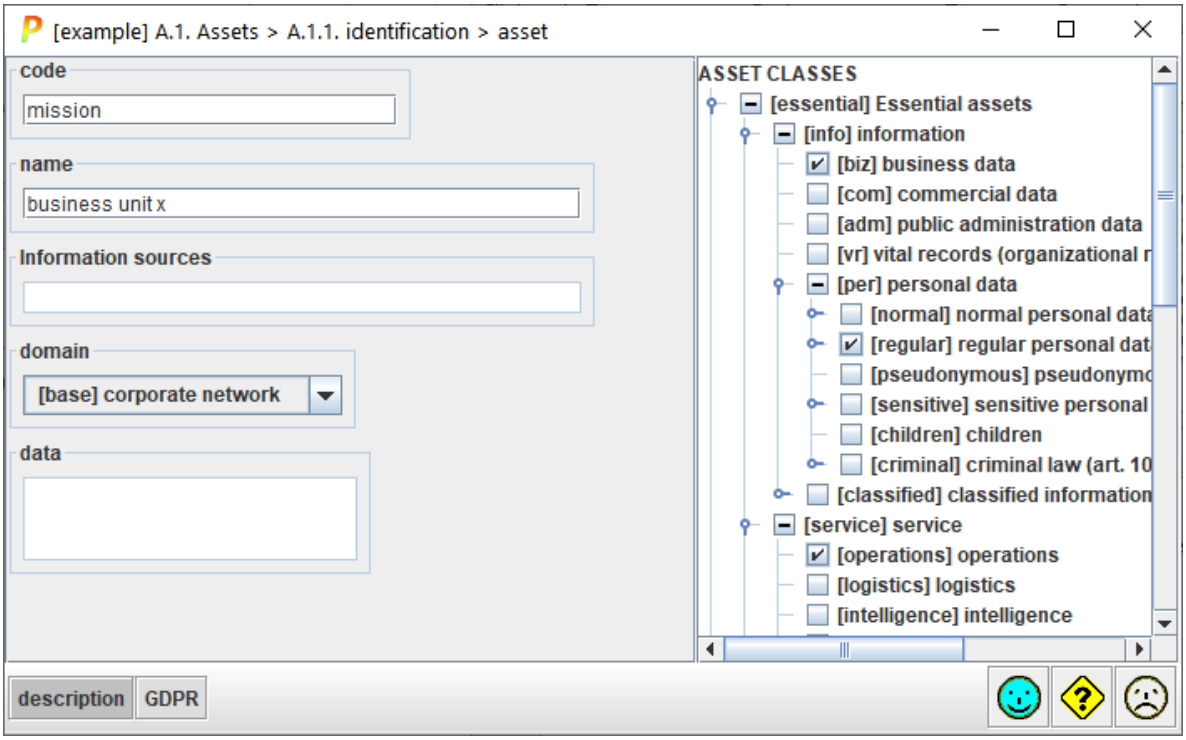



Add information assets as needed to capture all elements that are relevant to managers. You may use aggregate assets that stand for information items with the same rating.

Then, add business services that deal with the information.




You may also combine information and services into one asset.




You are done when there are enough information and service items to talk with management about the security requirements.

### II.2.3. Rating

Risk analysis > Assets > Valuation of domains

For information assets, rate their level of security rating:

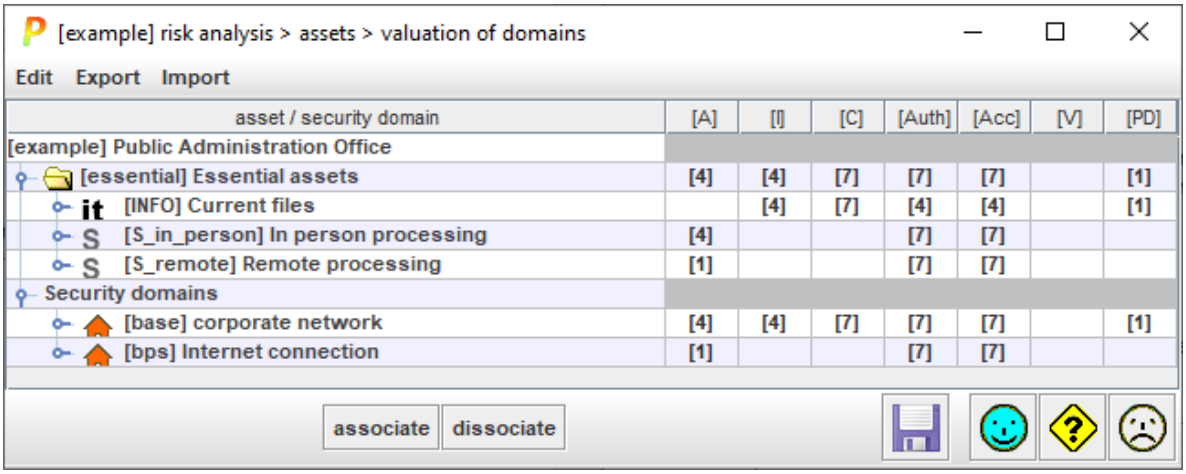
- between 0 (negligible) and 10 (top)
- with respect to confidentiality, integrity, …, authenticity, and accountability
- if no level is specified, PILAR understands that the asset has no requirements (e.g. no confidentiality for public information)

For services:

- availability requirements

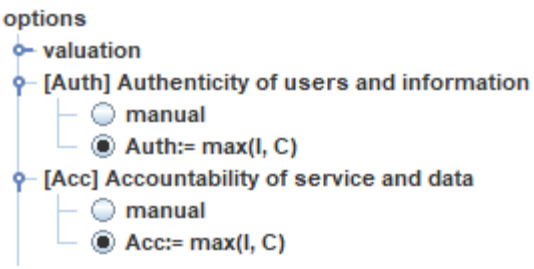
For assets that process personal data:

- privacy requirements (PD)



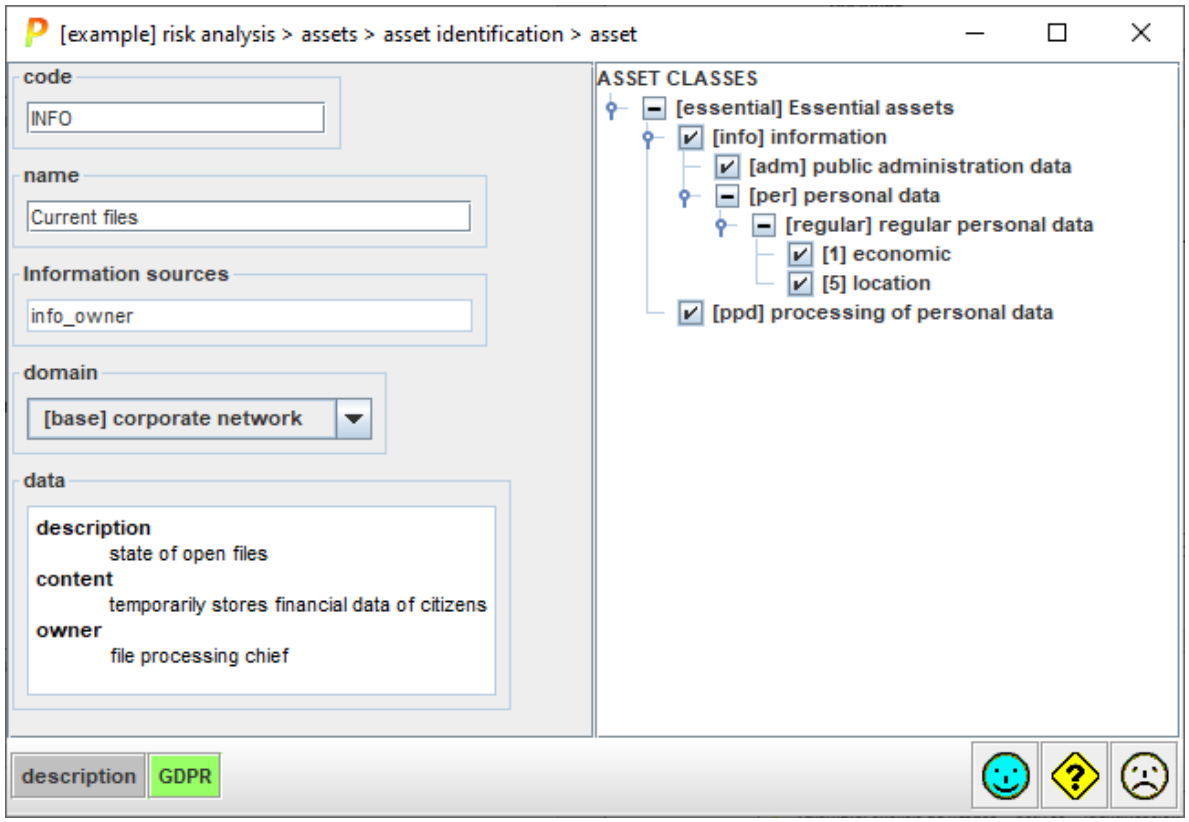

So far, all assets are in the same security domain, base, which security requirements are the maximum levels in each security dimension.

Valuation for [Auth] and [Acc] may be delegated to PILAR that has an option to use the highest of [I] and [C] if [Auth] or [Acc] are left blank. This behavior is controlled in Options:

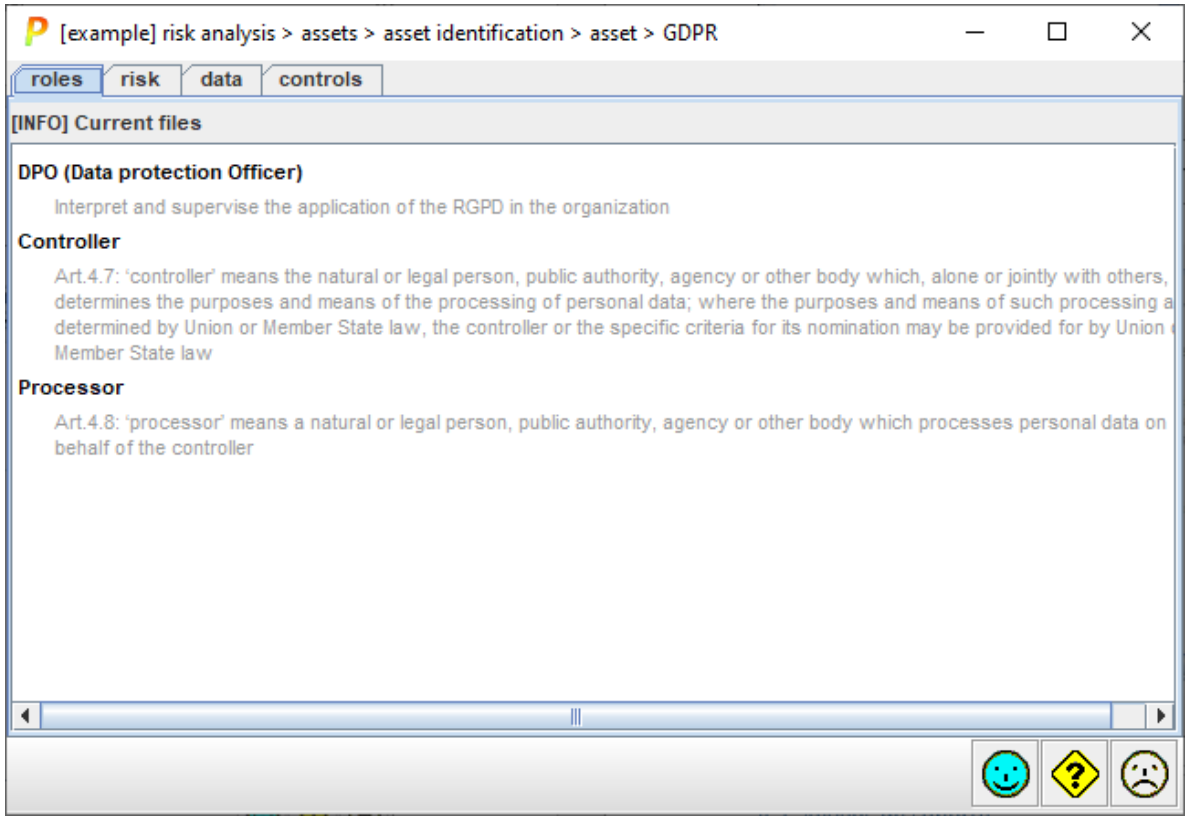



### II.2.4. Personal information

When treating personal information, you have to describe its type, and its processing




Through the GDPR button, you may describe the legal aspects of the asset:

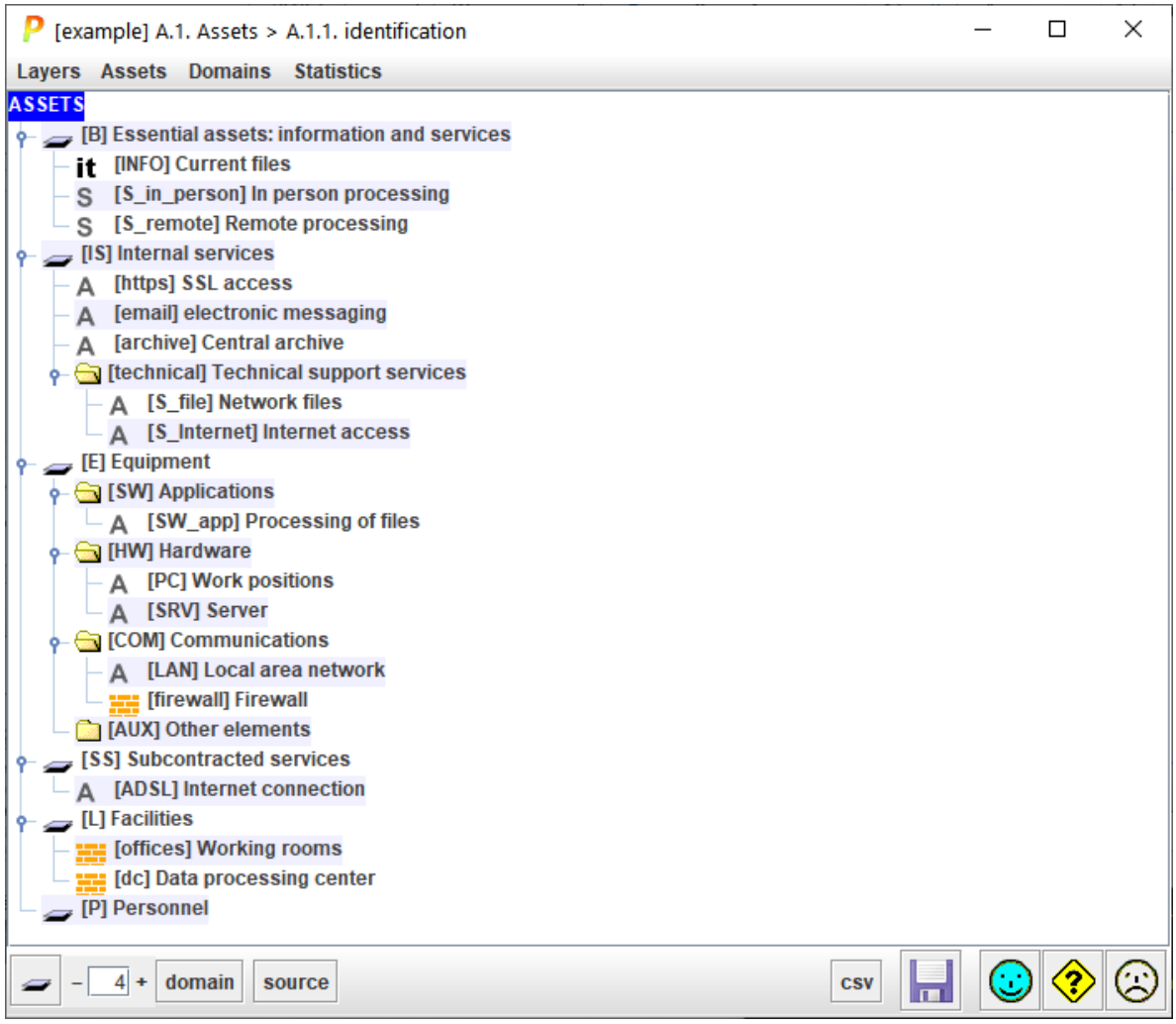


The collected information is carried onto the system documentation (reports).

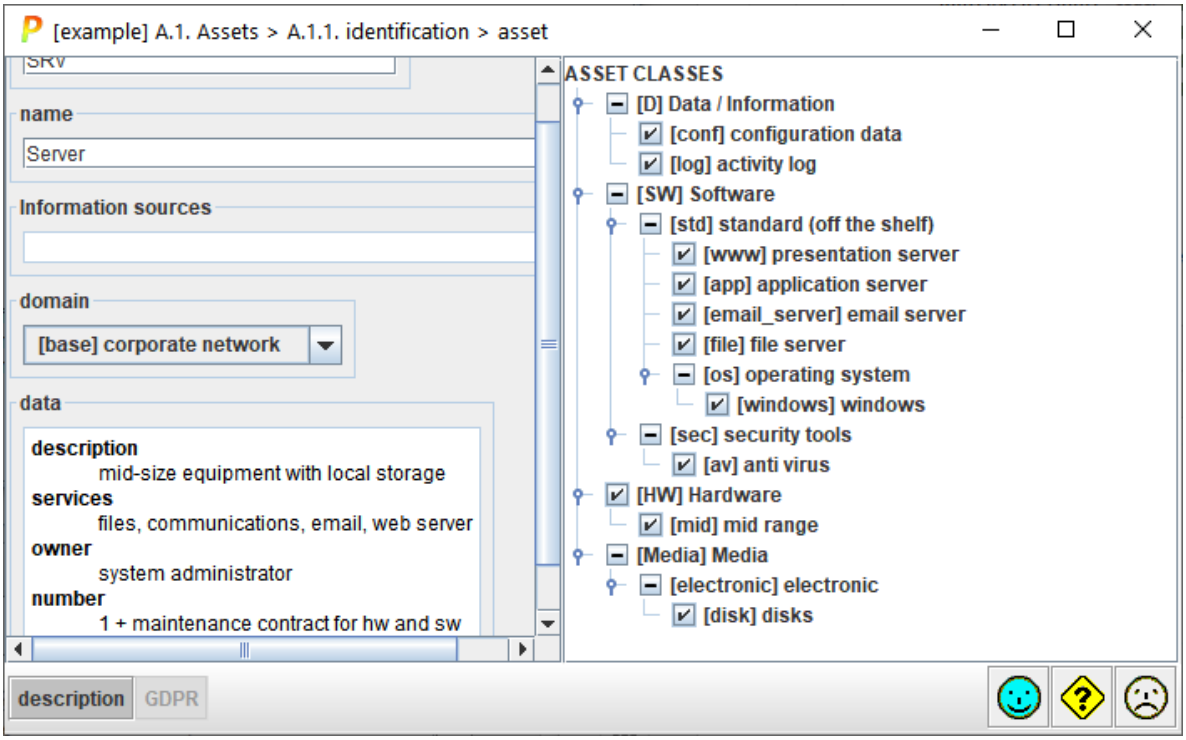
## II.3. Support assets

Risk analysis > Assets > Identification

Add other assets, either material or intangible, which make up the information system. You may organize into layers and groups for clarity, but PILAR only cares about the assets.



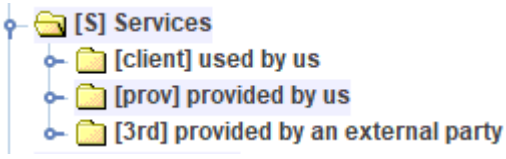
Each asset is qualified with classes that are used by PILAR to guess options for potential attackers, and propose countermeasures.




Granularity of assets can range from very precise assets to assets that are a whole subsystem themselves. We must find a balance between a sufficiently detailed to know what risks we are talking system and a description compact enough to avoid getting lost in the details. Typically, somewhere between a few tens up to a few hundreds.

## II.4. Services

PILAR lists a number of services with respect to which, our system may be consumer, direct provider, or subcontract it to a third party.




Each of those qualifiers fires the corresponding safeguards to treat risks.

Services used by us and services provided by us, are usually associated to essential services or support services.

Services provided by an external party are usually associated to support services.

## II.5. Automation

PILAR takes care of translating security requirements (levels) from essential into supporting assets; you may revise and refine manually adjusting individual assets

Risk analysis > Assets > Valuation of assets

PILAR applies a standard attack profile; that is

- identifies typical threats
- proposes standard ratings for likelihood and consequences (estimated as a fraction of the value translated from the essential assets)

Altogether, PILAR elaborates a risk map: the risks that are inherent to your system (potential risk) that you may consult

- technical view:
  Risk analysis > Impact & risk > Accumulated values > …
- business view:
  Risk analysis > Impact & risk > Deflected values > …

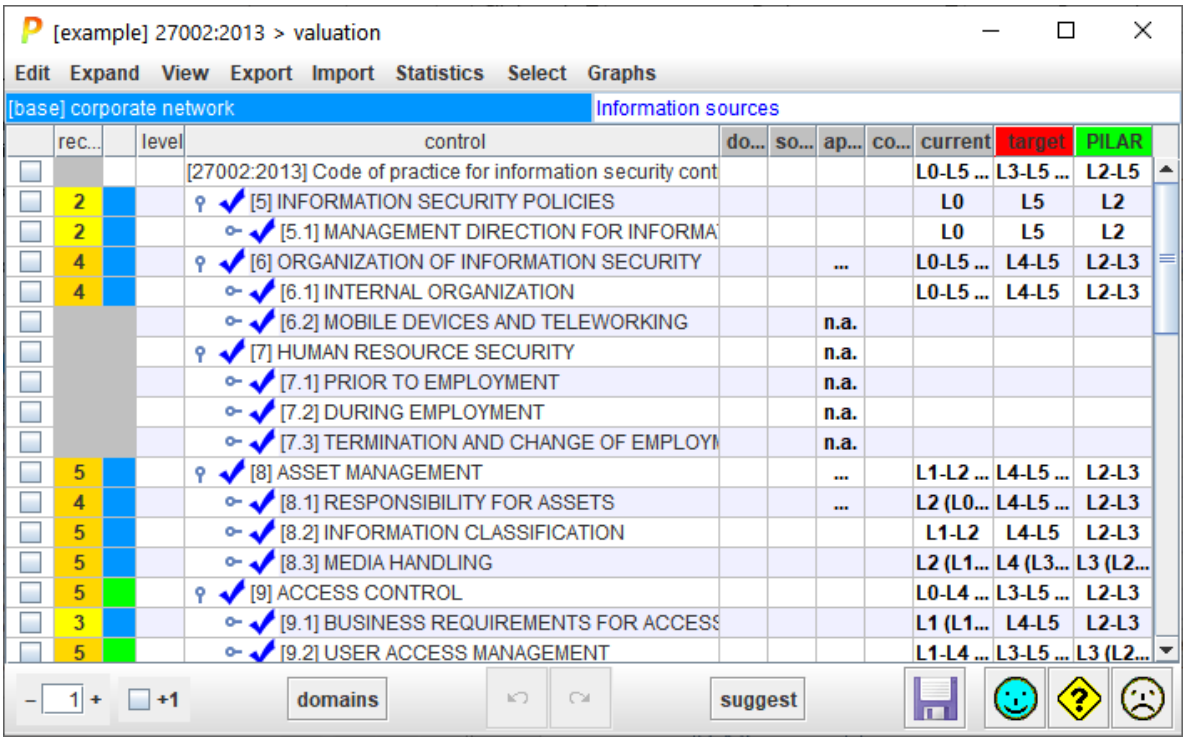
## II.6. Security profiles

Security profiles are collections of countermeasures, both technical and procedural. PILAR may load one or more to help users

- to treat technical risks by means of countermeasures
- to comply with accreditation bodies

Security profiles > 27002:2013 > Valuation

This screen presents the compliance to a given security profile, composed of security controls ( ) that may be expanded or mapped onto safeguards ( ).




### II.6.1 Recommendation

For each security measure, column [recommendation] is an estimate of PILAR on the relative importance of the row.

It is a rank in the range [null .. 10], estimated by PILAR taking into account the assets, the security dimensions, and the level of risk addressed by this safeguard.

The cell is grey if PILAR finds no reason to recommend this row. That is, PILAR does not know which risk this row is good for.

(o) - PILAR thinks it is an overkill (“too much”).

(u) - PILAR thinks it is an under kill (“not enough”).

### II.6.2. Applicability

In column [applies] you may say that some row does not apply. Please, note that some security profiles make some controls mandatory, for compliance. PILAR marks the control as M. Even for theoretically mandatory controls, you may conclude that it does not apply to your information system (either because you do not meet the requirements, or because you have alternative compensating controls).

For instance, if you have no server (e.g., when it is outsourced as a cloud service), there is nothing to do to protect the non-existing server. PILAR greys out the recommendation.

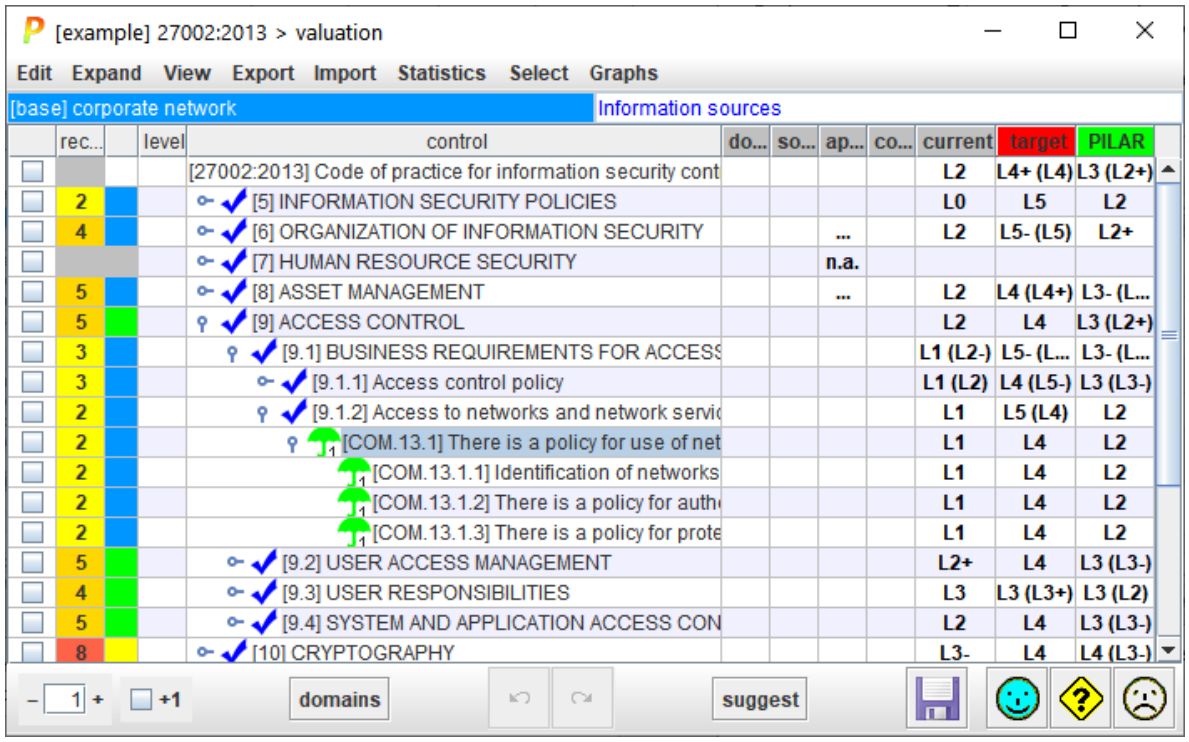
It may happen as well that the measure applies, but you have a better measure.

Some measures may be an overkill, and you may argue its use is not justified. It does not make the measure inapplicable. If you decide to skip (L0) a measure that is not justified, the risk remains, and PILAR presents it. A non-justified measure matches a low accepted risk. When a mandatory control is marked as “not applies”, the cell remains colored, to remember that you are expected to justify it.

You may use column [recommendation], as a guide; but by the end of the day, it is your best judgement that decides. Be aware that an inspector will need a good explanation for removing a row. The explanation may be written down as a comment in column [comment].

When you select a control row and click “n.a.”, every control under it becomes “n.a.”. Applicability of controls and safeguards is not automated by PILAR. It may happen that something below does apply, and something does not: you will have to check / uncheck manually.

### II.6.3. Rating




Last columns present phases (time snapshots) to evaluate the safeguards and observe security evolution. Typically, there are 2 user phases: current and target, and a special phase, PILAR, that is calculated: what PILAR proposes as a wise target.

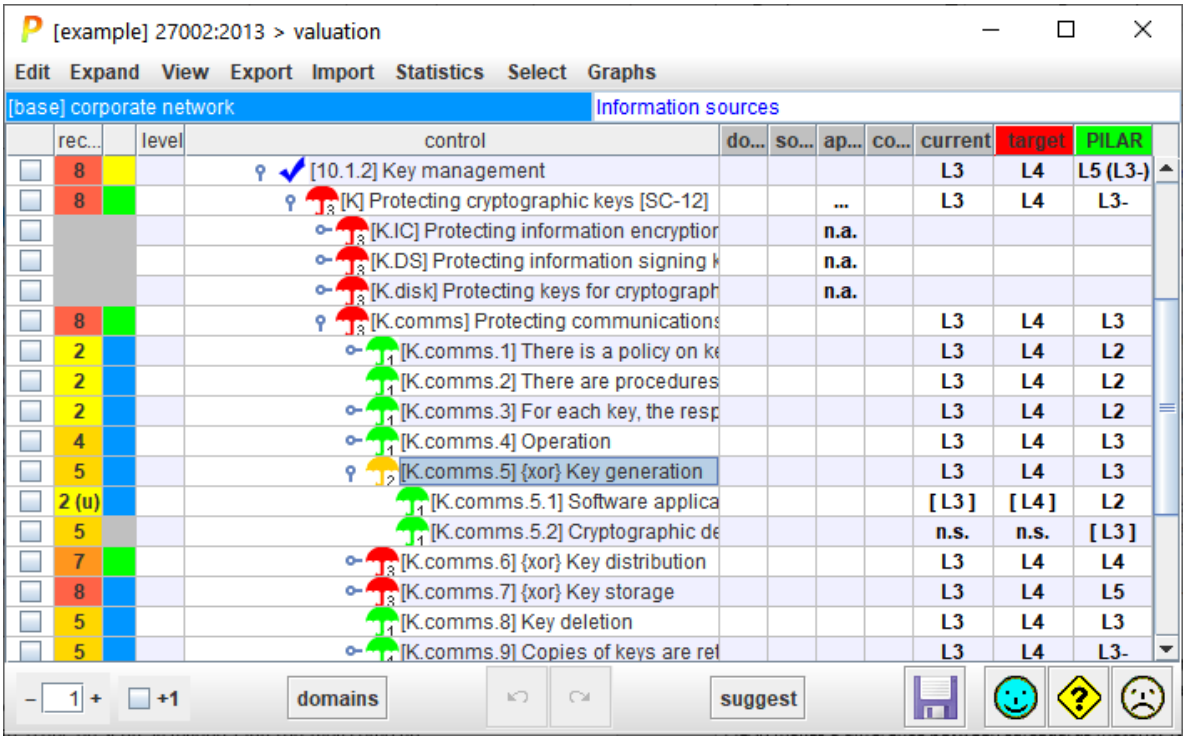
Rating of controls is done by means of maturity levels (see Annex A). For single controls, you have a single maturity value between L0 and L5. For controls composed of other controls, you may have a range (min-max). There is an option to present an approximate maturity value that takes into account the “average” maturity of the children.

You are expected to provide maturity levels for each security measure that applies (either control or safeguard) for each phase. There are some tricks to simplify data input:

- IMPORT: if you have already done the evaluation exercise, you may import it.
- SUGGESTION: start with a general valuation on top level, and then dig into children for fine adjustment
- the value in one phase is carried on to the next phase unless there is a manual input
- if you input a value in a row, it is propagated to the children (tree branches below)
- if you have values in children the value is collected into the father as a range

When a tree branch is labelled as XOR, you may choose which one of its children is the one to consider. PILAR marks as n.s. [not selected] those rows that are not used. Only the selected option is valuated for maturity.

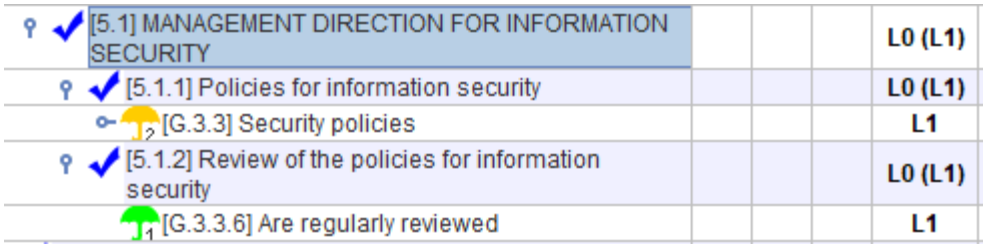
right-click > select




**Presentation.**

You may choose in [top menu bar] whether PILAR presents maturity levels, of a percentage of maturity, or the actual maturity compared to the proposal of PILAR.

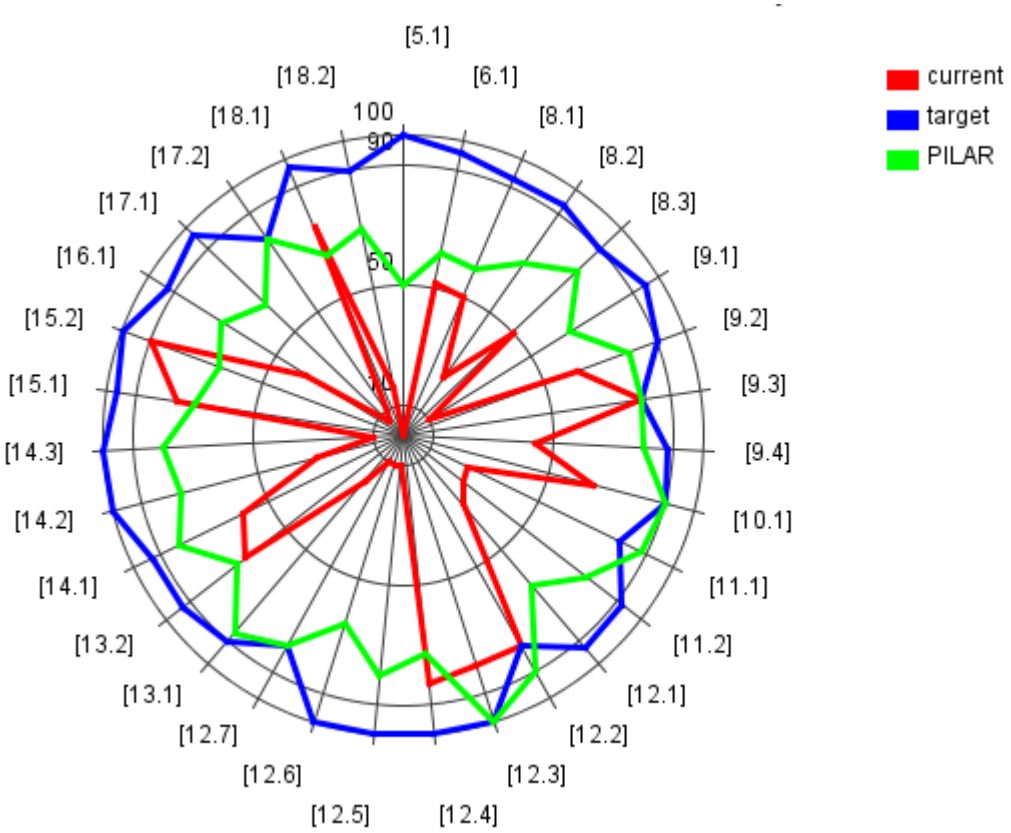
PILAR makes a difference between safeguards maturity (technical) and controls maturity (formal). Both are presented simultaneously, if different



The value between parenthesis is the one derived from safeguards below. You may “pull up” the value of the safeguards to evaluate the associated control (right click).

**Graphical presentation.**

Choose in [column 1] the rows to show. Click graph




## II.6.4 Traffic light

The traffic light [third column] compares valuation in reference phase (RED) with valuation in target phase (GREEN), and shows a color:

| | |
|---|---|
| RED | reference phase value is far below target phase value |
| YELLOW | reference phase value is close below target phase value |
| GREEN | reference phase value is equal to target phase value |
| BLUE | reference phase value is higher than target phase value |
| GREY | not applies |

Click with the mouse on phase column headers to select reference and target phases.

## II.6.5. Doubts and comments

In column [doubts] you may mark a row with a question mark to remember that there are doubts to resolve with respect to this row.

Column [comment] may host additional information explaining something with respect to the row.

## II.7. Reporting

PILAR is distributed with a few predefined reports. Some reports are hardwired (text and graphs) while other are generated by means of templates. Templates use the RTF format, that can be edited by most word processors.


Graphs are useful to cut and page for presentations to be crafted manually.

Some textual reports are valuable by themselves, either as final reports or as working material for meeting asset owners and request information or validate current data.

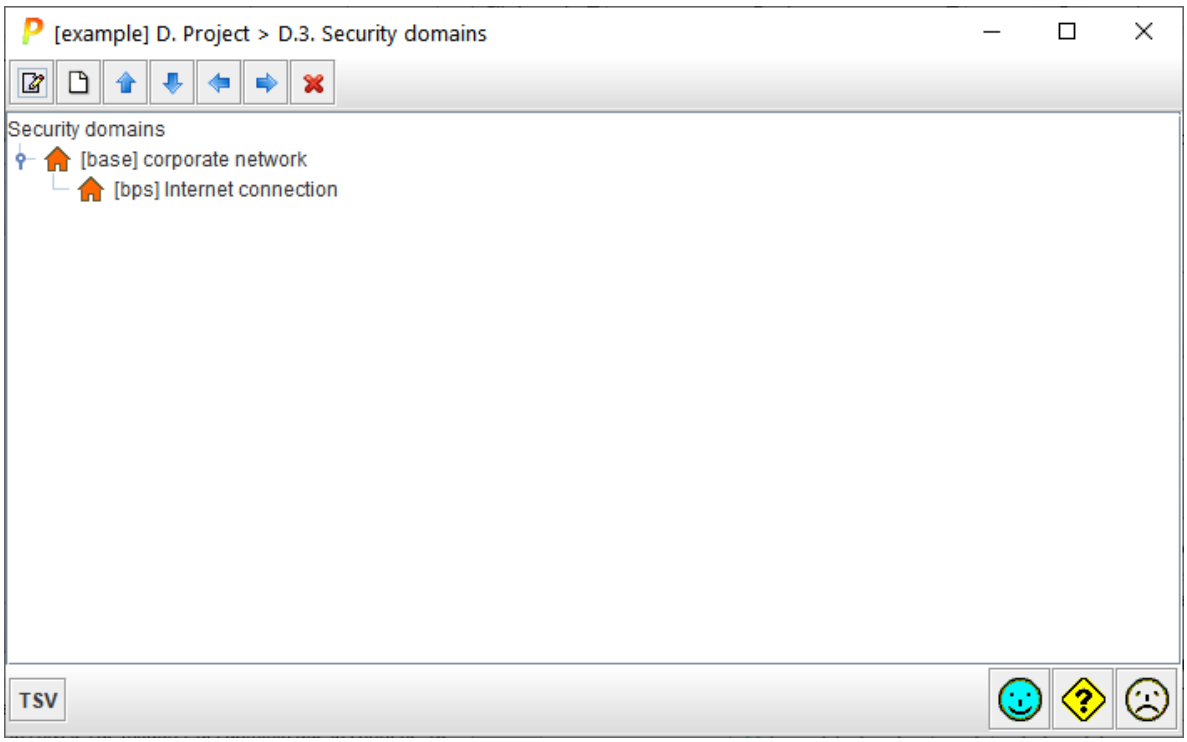
# Chapter III – Average user

## III.1. Security domains

Assets may be distributed in security domains. Each security domain may have a specific attack profile, and specific security measures.

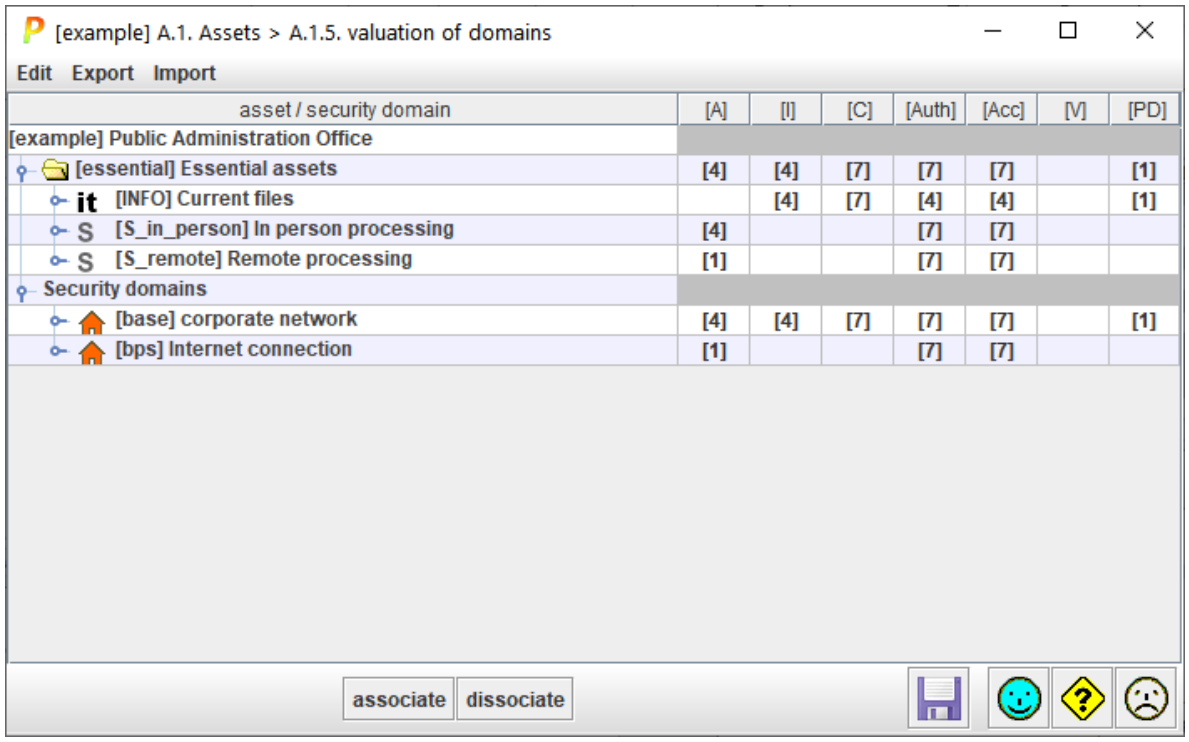
Project > Security domains

To identify security domains.




Security domains may be nested: one domain appearing as a child of another domain. The nesting is used in the rating of safeguards and security profiles. Nested domains inherit the maturity level from the covering domain. In such a way that you have to rate the base domain, and then refine as needed in nested domains.

In order to rate assets, you have to rate essential assets, and their value is translated to every asset in the same domain, and also to other domains to which the essential asset is associated.

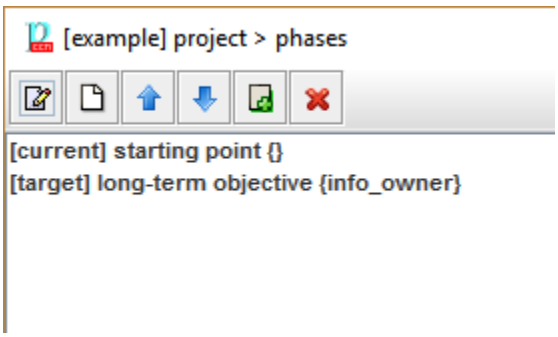


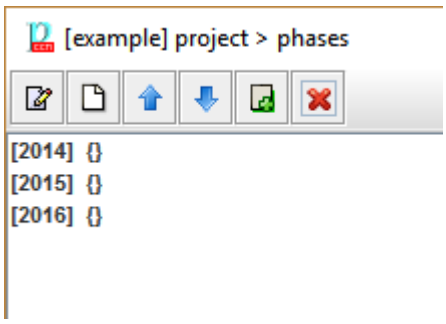

## III.2. Project phases

Security measures may evolve in time. Phases are project snapshots to analyze evolution. E.g. yearly.

Project > Project phases

To identify and order phases in a list




Phases are used when rating safeguards and controls. The rating in one phase is silently translated into the next phase unless modified

## III.3. Safeguards

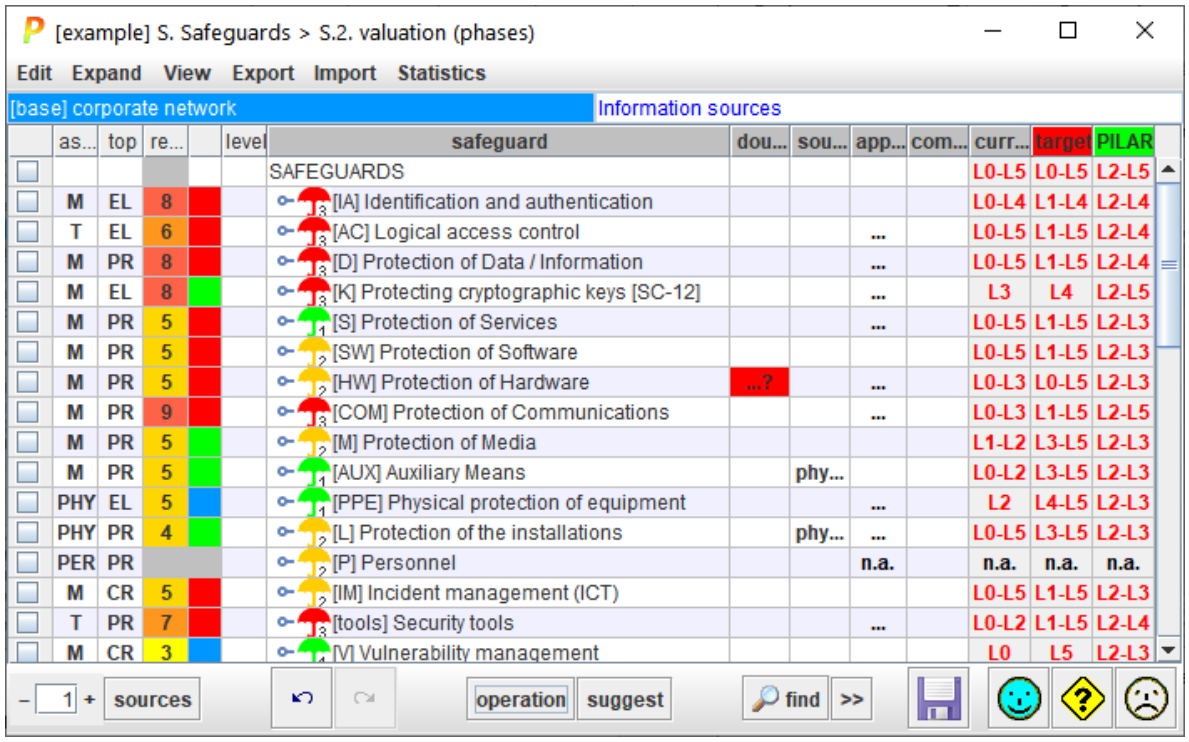
PILAR has a large catalogue of security measures under the name safeguards. Safeguards are organized as a tree, where top safeguards are refined into detailed safeguards.

Safeguards are selected by security domains: each security domain may have different safeguards.

PILAR calculates a recommendation level (0 to 10) for each safeguard in each domain, taking into account

- the classes of the assets in the domain
- the level of security required, directly or indirectly, for each dimension for each asset in the domain
- the ability of each safeguard to protect each security dimension
- the inherent power (strength) of the safeguard

First you may choose the subset of safeguards that apply by marking (as n.a.) those that do not:




Column [aspect] presents M for 'management', T for 'technical', PHY for 'physical security', and PER for 'personnel'.

Column [top] presents the type of protection provided by the safeguard:

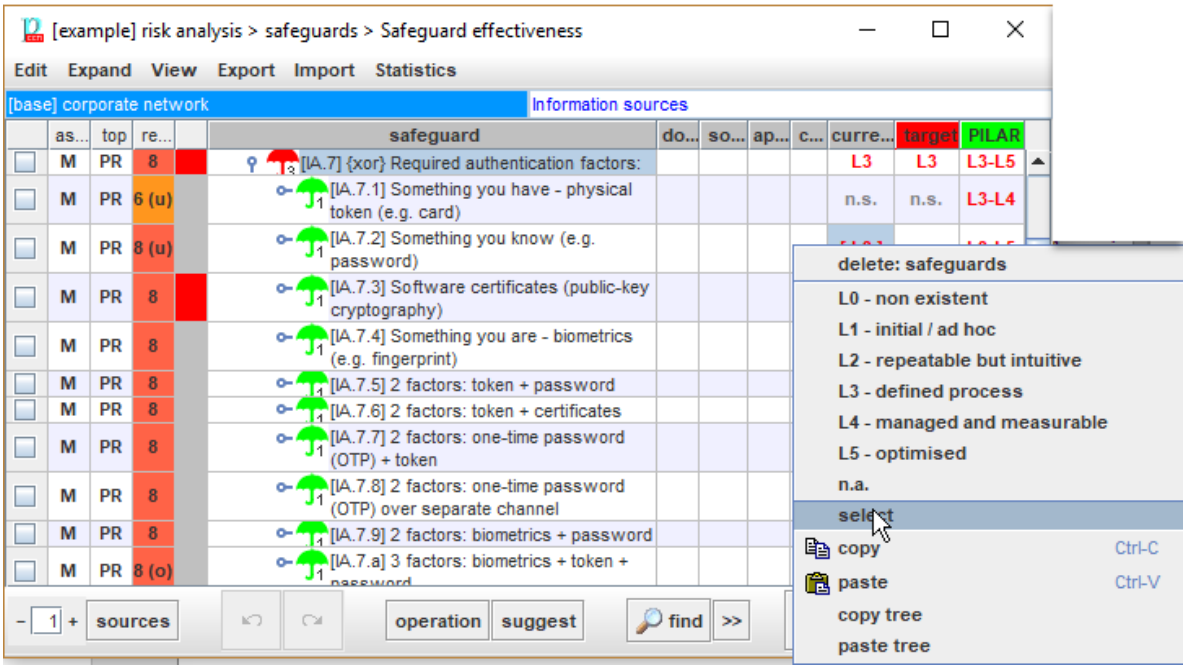
- PR – prevention
- DR – deterrence
- EL – elimination
- IM – impact minimization
- CR – correction
- RC – recovery
- AD – administrative
- AW – awareness
- DC – detection
- MN – monitoring
- std – standard policies
- proc – procedures
- cert – certified or accredited

Not every safeguard is equally important:

| | | |
|---|---|---|
| 3 | highest weight | critical |

| | | |
|---|---|---|
|  | high weight | very important |
|  | normal weight | important |
|  | low weight | interesting |
|  | assurance: certified components | |

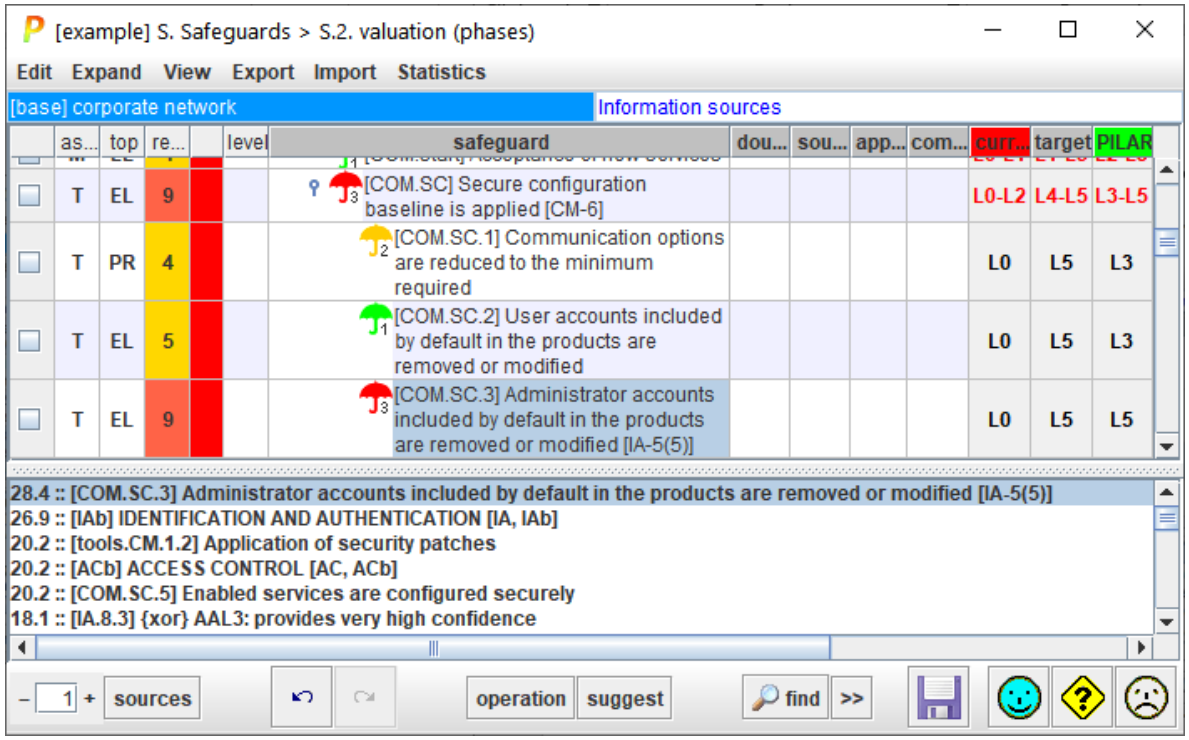
Some safeguards have different ways of implementing them, options are alternative and are labeled as XOR. In each security domain only one of those options is applied, leaving the others marked as n.s. (not selected). You have to select the one that you have implemented, using the right mouse button



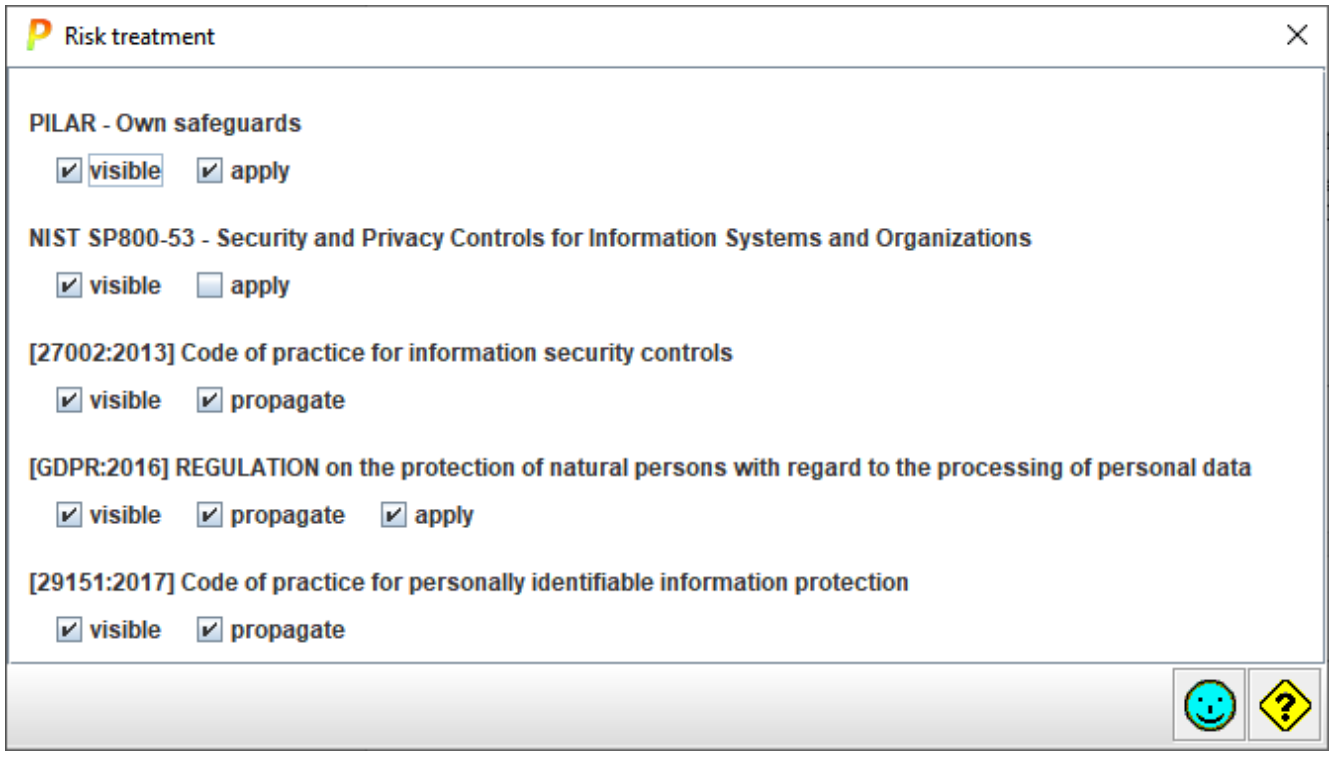

The selected option appears [in brackets]. The selection is not inherited between security domains: they are independent.

Then you may rate the maturity level of the retained safeguards, by security domain, by project phase. Take into account that values in one security domain are inherited by nested domains unless changed. And values in one phase are carried on to next phases unless changed.

PILAR may be asked to suggest safeguards for one security domain and phase, taking into account security needs and the specific strength of the safeguard




## III.4 Risk treatment



You may select the security measures you use to treat risk, and the security measures you use for compliance.

For PILAR collection of safeguards,

- users may completely ignore them
- or see them, but do not use them to treat risk
- or see, and apply them to treat risk

For NIST 800-53 rev.5 collection of safeguards,

- users may completely ignore them
- or see them, but do not use them to treat risk
- or see, and apply them to treat risk

Some EVL security profiles may be directly used to treat risk

- users may completely ignore them
- or see, and apply them to treat risk
- furthermore, control valuation may be propagated onto associated safeguards

Some EVL security profiles are only available for compliance

- users may completely ignore them
- furthermore, control valuation may be propagated onto associated safeguards

Many EVL profiles link controls to safeguards, and users may valuate both in parallel.

Previous version of PILAR used ONLY PILAR collection of safeguards to treat risk and used EVL profiles for compliance. You may fall back to that working mode selecting options like this

- PILAR: visible + apply
- NIST SP800-53: invisible
- *evl*: visible + propagate

# Chapter IV – Advanced user

## IV.1. Dependencies

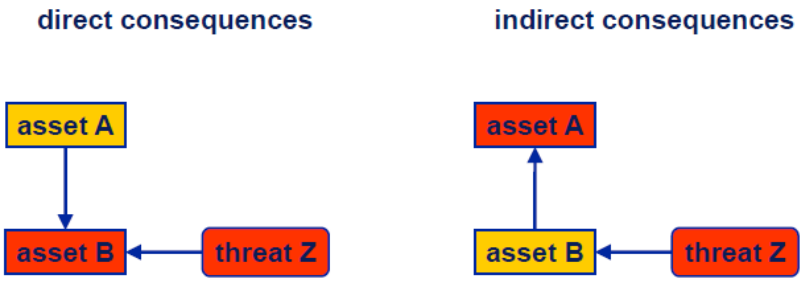
Applying the save security requirements to every asset in a single security domain is a quick approach; but sometimes it is too coarse. For instance, when each information and service relies only on a subset of the equipment in the domain.

Fine grain translation of requirements may be achieved by means of dependencies.

You need to activate it

Edit > Options > Valuation > assets + dependencies

Now you may state that an asset A depends on another asset B.

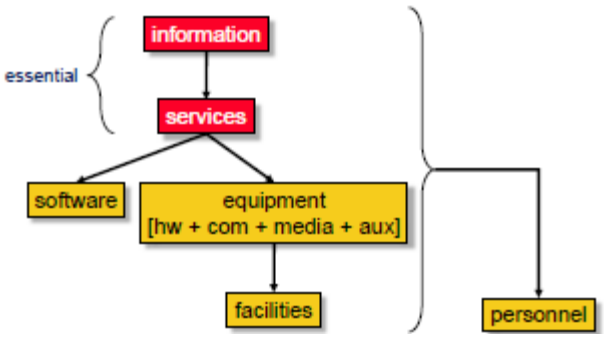



- security requirements (value levels) in asset A are transferred onto asset B
- attacks on asset B have a direct effect on the accumulated value on B
- attacks on asset B have an indirect (deflected) effect on the value of A

Establishing a correct set of dependencies is time consuming and difficult to maintain; but provides the best risk analysis.

As general rules

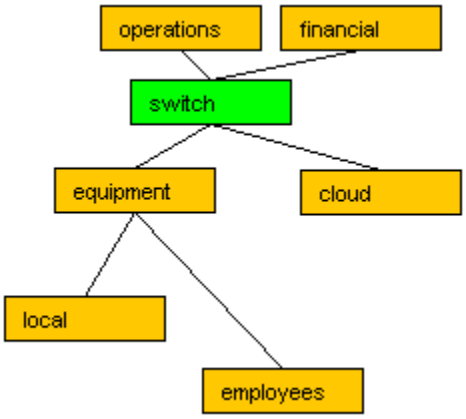
- essential information depends on essential services
- essential services depend on equipment (hw, sw, comms, and media)
- material equipment depends on facilities
- every asset depends on the personnel that may harm it



### IV.1.1. OR nodes

Some assets may be qualified as OR nodes. This implies a special behavior during transfer of value:

- Availability is not transferred to OR-node's children, except for grandchildren shared by every branch on the OR-node.




That is, OR nodes represent alternative provisioning. Every branch must meet information security requirements (confidentiality, integrity, …), but availability. So, assets on only one branch do not inherit availability requirements because there is another branch. Unless common points of failure; that is, assets that support both branches.

## IV.2. Asset by asset valuation

You may skip domain valuation, and not establish any dependency. Now, each asset is to be assigned security requirements individually. It is time consuming, and difficult to maintain when the information system changes. And deflected risks cannot be evaluated.

## IV.3. Threats

By default, PILAR applies a standard attack profiles that establishes which threats are likely for each asset and estimates its likelihood and its consequences. The profile is an external file (either XML o Excel), and the file is referenced from the .CAR configuration file (look for tag TSV).

Users may edit the TSV file. Even, users can have several TSV files, and choose one for each security domain. Editing the external file is the best approach

- to document changes
- to analyze an information system under different attack scenarios

You may also edit threads manually:

**Edit > Options > Threats > Manual**

TSV is disabled, and you control the details.

**Edit > Options > Threats > Mix**

You may mark some assets as manual and avoid TSV for them.
TSV still applies to the others.

## III.4. Security profiles – Compliance

PILAR maps controls onto safeguards, and then changes to controls' maturity are propagated onto connected safeguards, and safeguards' maturity is used to estimate controls' maturity.

This propagation mechanism may be disabled

Edit > Options > Security profile: propagate > No

| current | target | PILAR |
|---|---|---|
| L0-L1 (L0-L5) | L1-L4 (L1-L5) | L3-L5 (L2-L5) |
| L0-L1 (L0-L2) | L2-L4 (L1-L5) | L3-L5 (L2-L5) |
| L1 (L0-L2) | L2 (L1-L5) | L3 (L2-L3) |
| L1 (L1-L2) | L2 (L1-L5) | L5 (L2-L5) |
| L2 | L5 | L3-L5 |
| L1 | L1-L5 | L2-L3 |
| L1 | L1-L5 | L2-L3 |
| L1 | L4 | L3 |
| L1 | L1-L4 | L3 |
| n.a. | n.a. | n.a. |
| L1 | L4 | L3-L4 |
| L0 | L4 | L3 |
| L1 (L0-L5) | L1 (L3-L5) | L3 (L2-L3) |

Now, there is a difference between evaluating controls and evaluating safeguards. The format is

control_maturity (safeguard_maturity)

if both maturity ranges are identical, the safeguards maturity is not presented:

maturity_range

You can still push control rating to safeguards, and pull safeguards rating up to controls, but it is not automated any more.

So, you can present control maturity for compliance, separate from safeguard maturity for risk treatment.

Why? PILAR maps controls onto safeguards. This mapping is neither official, nor perfect. It is not official because security profiles are pieces of work from different sources, unrelated to PILAR. And it is not perfect for several reasons:

- there may be no exact safeguard in PILAR to meet the precise control requirements
- the same safeguard in PILAR may apply to more than one control
- as PILAR evolves, the set of safeguards evolve, asynchronously from security profiles evolution

# Chapter V – Personalization

Users can personalize PILAR editing some files in the library directory.

Here you may find a summary. For details visit

> "Personalization" at https://www.pilar-tools.com/doc/

## V.1 Configuration file

PILAR is distributed with some configuration files, copied onto the directory where you install it.

You may find this file

> CIS_en.car

The file is plain text, and you may edit to change language and/or directories, if you change the standard installation.

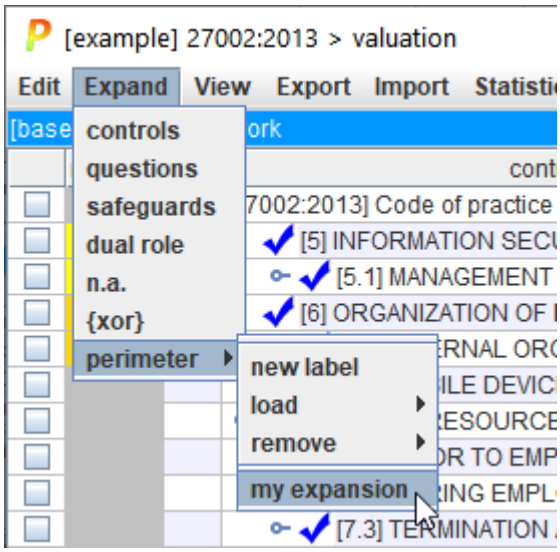
You may tune it:

- add an icon of yourself
- add a splash screen
- change character separator for CSV files
- tune default asset layers, and administrative data
- adapt marking labels
- add new asset classes, new threats
- add new or replace valuation criteria
- adapt threat profile
- …

## V.2. Perimeters

Perimeters are expansion shapes for trees of safeguards and security profiles (evl). Perimeters are useful to define expansions that precisely display the rows that you need for your analysis and presentations.

Some perimeters are part of the standard library. You may add your own ones,




The process is as follows:

1. Create a new label with a name you choose:

   `Expand > perimeter > new label`

2. On the tree (safeguards or security profile) expand the tree as appropriate for your purposes.
3. Load current shape onto the named label

   `Expand > perimeter > load > your label`

4. To change shape, repeat steps 2-3

**To use a label**

`Expand > perimeter > your label`

**To remove a label**

`Expand > perimeter > remove > your label`

## V.3. Report Templates

You may prepare your own report templates.

See “Report templates” at https://www.pilar-tools.com/doc/

You may set your own default reports for PILAR:

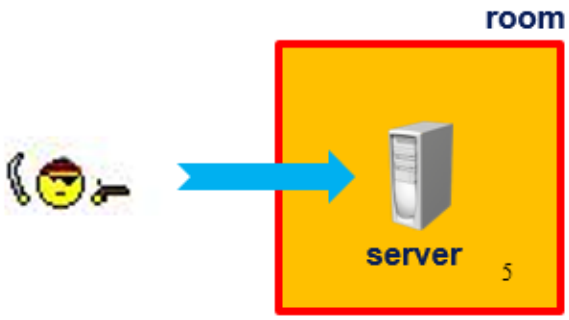
See “Personalization” at https://www.pilar-tools.com/doc/

If you want to prepare your own reports,

- edit a template of yours following the documentation on ‘Report Templates’
- when the template (.RTF) is ready, make it known to PILAR:
  edit “reports.xml” that assigns a name to your pattern file

# Chapter VI - Other topics

## VI.1. Zones




Zones are collections of assets within a perimeter. Zones model defense in depth, where valuable assets are separated from potential attackers.

For instance, an attacker may be outside, while the server is inside.

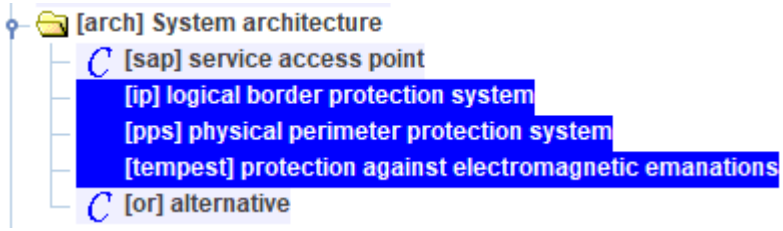
- we have two zones:
  - within the area
  - outside the area
- and one border, the room

The attacker needs to pass over the physical protection system (the protection provided by the room: doors, windows, etc.) and then he can attack the server.

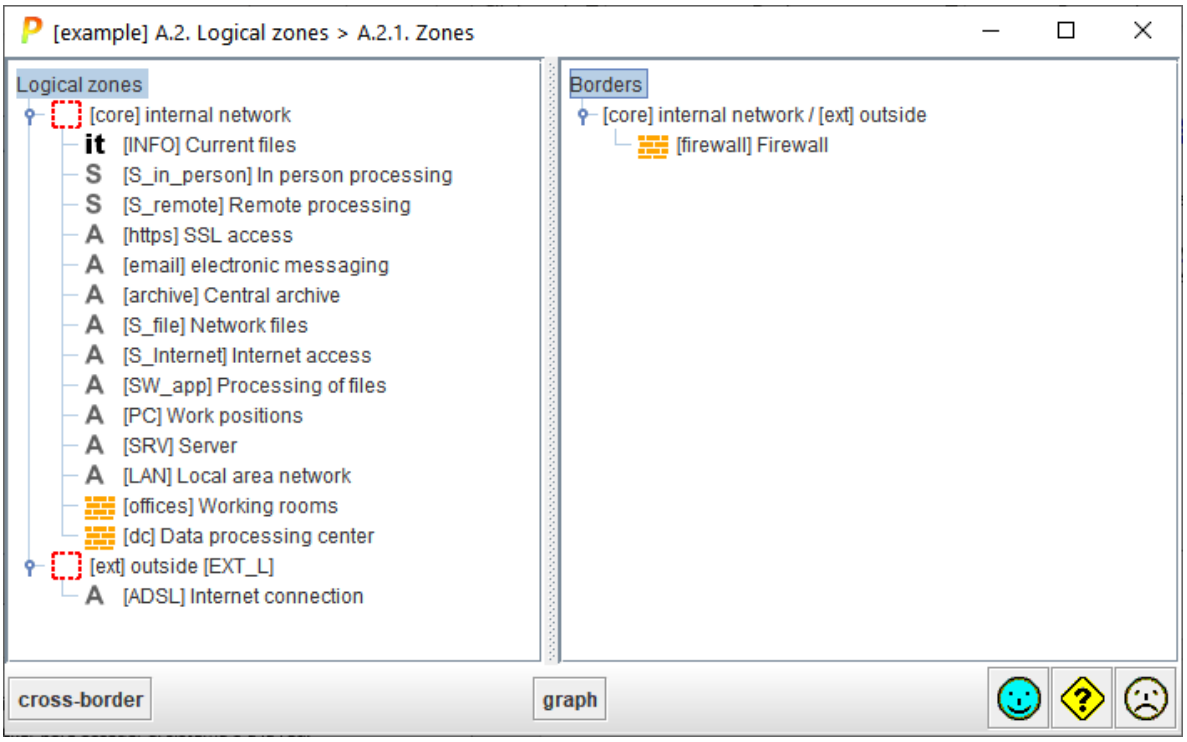
PILAR provides

- logical zones, separating the core network from outside by means of border protection services and devices (e.g. firewalls, and DMZs).
- physical zones, separating inner areas from outside by means of physical protection systems (e.g. doors, windows, etc.)
- tempest zones, separating device and cable emissions from outside listeners (e.g. grids)

With respect to the border, border assets are of one of these types




Please, note that a border asset may be a single asset (such as a firewall) or a collection of elements (several firewalls, one proxy, servers in a DMZ, etc.). In this last scenario it is recommended to define one asset for the border functionality as a whole. For logical borders, this asset may be [arch.ip], and shall be located between protected zones




## VI.2. Vulnerabilities

PILAR may deal with CVE's: Common Vulnerabilities and Exposures, as described at https://cve.mitre.org/

An information security "vulnerability" is a mistake in system elements that can be directly used by a hacker to gain access to a system or network.

CVE considers a mistake a vulnerability if it allows an attacker to use it to violate a reasonable security policy for that system (this excludes excluding entirely "open" security policies in which all users are trusted, or where there is no consideration of risk to the system).

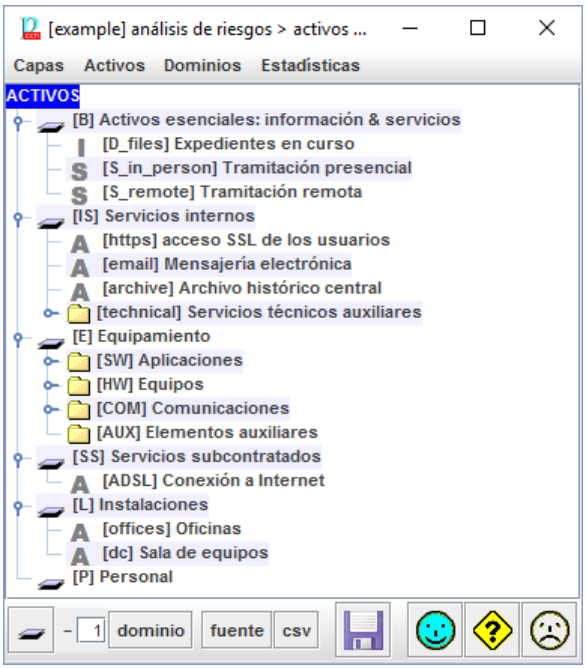
For CVE, a vulnerability is a state in a computing system (or set of systems) that either:

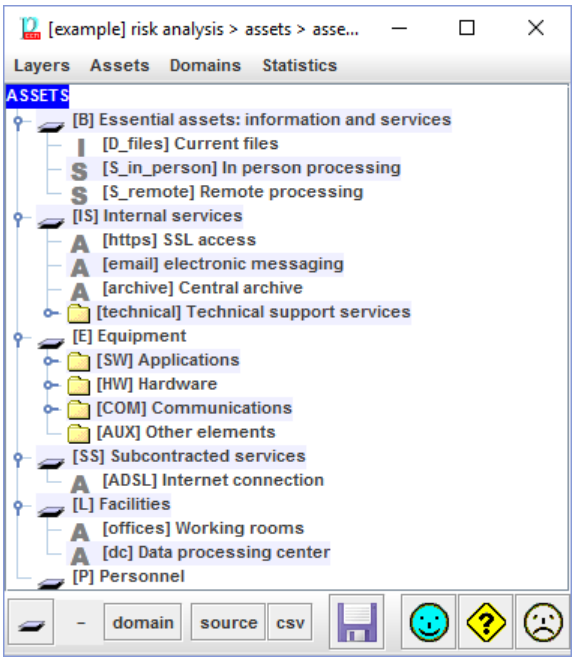
- allows an attacker to execute commands as another user
- allows an attacker to access data that is contrary to the specified access restrictions for that data
- allows an attacker to pose as another entity
- allows an attacker to conduct a denial of service

See "Vulnerabilities" at https://www.pilar-tools.com/doc/

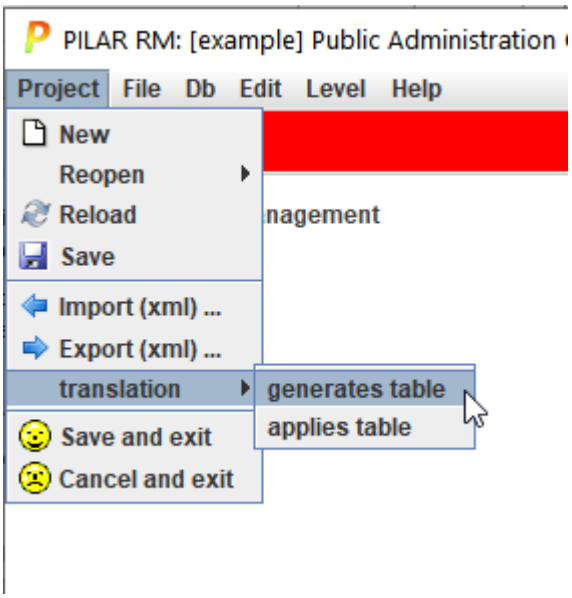
## VI.3. Multi language

PILAR is able to take a project written in one source language SL, and translate it into another target language TL. PILAR used elements' codes as keys, and changes elements' names.




### VI.3.1. Create a dictionary




In main window

Project > translation > generates table

select a file

example.rw

PILAR writes a text file with translation rules. One rule per line, that the user may edit, and that will be applied sequentially.

You may also use ".csv" as the extension of the rules file, either generating or applying. Then you can use excel to edit the translation rules.

Example,

```
asset: [mission] System mission -> [] Misión del sistema
```

PILAR looks for an asset with code 'mission'. The code is not changed, but the name is translated into Spanish. You may algo provide a new code in the right side:

```
asset: [mission] System mission -> [misión] Misión del
sistema
```

## VI.4. Access control

PILAR provides means to protect project modification. It is based on sources of information.

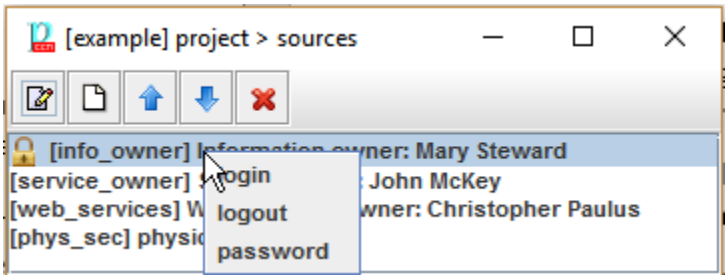
Basic concepts:

- an information source may be protected by a password; you may login into the source if you know the password
- any element may be associated to one or more source(s); for the elements associated to sources, you need to log into one or more of the sources to get write access; otherwise, the element is read-only for you

Elements with controlled access

- security domains
- zones (logical, physical, and tempest)
- project phases

### VI.4.1. Passwords




**Project > Information sources > [right click] > password**

To set a password (or change, or remove password control).

**Project > Information sources > [right click] > login**

To provide a password to unlock the source.

**Project > Information sources > [right click] > logout**

To lock the source.

### VI.4.2. Access restrictions: Security domains

When a security domain has information sources, you need to log into at least one of the sources in order to

- modify sources
- modify code, name, and description
- modify assets (in the security domain)
    - create, change of domain, removal
    - modify sources
    - modify code, name, description, administrative attributes

    - modify classes
- modify safeguards for the security domain
    - modify sources
    - applicability, comments, rating
- modify controls for the security domain
    - modify sources
    - applicability, comments, rating

### VI.4.3. Access restrictions: Project phases

When a project phase has information sources, you need to log into at least one of the sources in order to

- modify sources
- modify code, name, and description
- modify safeguards for the phase
    - modify sources
    - applicability, comments, rating
- modify controls for the phase
    - modify sources
    - applicability, comments, rating

### VI.4.4. Access restrictions: Zones

When a zone has information sources, you need to log into at least one of the sources in order to

- modify sources
- modify code, name, and description

## VI.5. Databases

You may use an external data base. Any SQL compliant engine with a JDBC interface.

An external database may be used to store projects, and risk analysis results. A database may be useful for sharing the risk analysis with other people, and for reporting using database querying tools.

See “SQL tables” at https://www.pilar-tools.com/doc/

## VI.6. Batch mode

PILAR may be run in batch mode, that is without graphical interface. This mode is useful for:

- unattended evaluation of risks (e.g. overnight)
- reactive risk analysis (e.g. upon reporting of vulnerabilities)

See “Batch mode” at https://www.pilar-tools.com/doc/

# Annex A – Maturity levels

PILAR uses maturity levels to evaluate safeguards and controls according to the Capability Maturity Model (CMM) used to qualify the maturity of processes.

**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. 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.

**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.

# Annex B – Glossary

**accountability**

The ability to map a given activity or event back to the responsible party.
[ISACA, Cybersecurity Fundamentals Glossary, 2014]

**applicability**

Formal statement on a safeguard or control about its adequacy to protect the information system. A safeguard does not apply when it would have no effect on system risks. A control does not apply when it would have no effect on system compliance.

**statement of applicability (SoA)**

Formal declaration that establishes which safeguards (or controls) are appropriate for an information system.

**asset**

Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances, and reputation.
[ISACA, Cybersecurity Fundamentals Glossary, 2014]

**essential assets**

Essential assets are those assets that model the requirements that the organization imposes on the information system.

Typically, an information system has essential information to protect, and essential services to provide. These essential assets determine the system needs on security.

**supporting assets**

Assets that are not essential. These assets are not organizational needs, but elements that implement the required functionality. Supporting assets inherit value to protect from essential assets.

**authenticity**

Undisputed authorship.
[ISACA, Cybersecurity Fundamentals Glossary, 2014]

**availability**

Ensuring timely and reliable access to and use of information.
[ISACA, Cybersecurity Fundamentals Glossary, 2014]

**compliance**

Adherence to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations, as well as voluntary requirements resulting from

contractual obligations and internal policie.
[ISACA, Cybersecurity Fundamentals Glossary, 2014]

**confidentiality**

Preserving authorized restrictions on access and disclosure, including means for protecting privacy and proprietary information.
[ISACA, Cybersecurity Fundamentals Glossary, 2014]

**impact**

Security indicator. It measures what may happen when a threat occurs.

**information**

An instance of an information type.

A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor-sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
[https://csrc.nist.gov/glossary/term/information-type]

**information System**

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
[https://csrc.nist.gov/glossary/term/System]

**integrity**

The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

**phases**

PILAR treats risks by stages or phases.

Phases are snapshots of system evolution, showing safeguard deployment or improvement.

**risk**

effect of uncertainty on objectives [ISO Guide 73:2009]

NOTE 1: An effect is a deviation from the expected — positive or negative.

NOTE 2: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

NOTE 3: Risk is often characterized by reference to potential events and consequences, or a combination of these.

NOTE 4: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence.

NOTE 5: In the context of information security management systems, information security risks can be expressed as effect of uncertainty on information security objectives.

NOTE 6: Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.

**direct risk – accumulated risk**

The risk evaluated on supporting assets. That is, where the incident occurs.

**indirect risk – deflected risk**

The risk evaluated as indirect consequences on essential assets. That is, on business value.

**inherent risk – potential risk**

The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls).
[ISACA, Cybersecurity Fundamentals Glossary, 2014]

**residual risk**

The remaining risk after management has implemented a risk response.
[ISACA, Cybersecurity Fundamentals Glossary, 2014]

**risk owner**

person or entity with the accountability and authority to manage a risk.
[ISO Guide 73:2009]

**security domains**

PILAR groups assets into security domains. Each asset belongs to one single domain.

A security domain is a collection of assets under a uniform protection, typically under a single authority.

Security domains are used to make a difference between some assets and other ones. For instance:

- central facilities, remote sites, tele-workers, …
- central host, unix frontend, PC's, …
- physical protection, logical protection, …
- …

**security measures**

The means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, technical, management, or legal nature.
[ISACA, Cybersecurity Fundamentals Glossary, 2014]

Synonyms: controls, countermeasures, safeguards

**security profile**

Security profiles are mappings of the system safeguards onto some profile that the user needs to know to which extend is satisfied. [PILAR]

**service**

A capability or function provided by an entity.
[https://csrc.nist.gov/glossary/term/service]

**threat**

potential cause of an unwanted incident, which may result in harm to a system or organization.
[ISO/IEC 27000:2014]

**valuation - rating**

Assets are valued to establish the security requirements on the asset; that is, the value measures the direct or indirect consequences of threat that occurs.

**zones**

Zones are used to determine the position of the attack. An attack originates in a zone and can progress to other zones through the border elements.

An asset belongs to one or more zones, being the direct object of the attacks from the zone to which it belongs, and the indirect object of attacks originated in another zone, through the border assets.

PILAR has logical zones (separated, for example, by firewalls), physical zones (separated by physical perimeter defenses) and TEMPEST zones (separated by anti-emission protections).

.

# Annex C - References


- Magerit: version 3,
  "Methodology for Information Systems Risk Analysis and Management".
  http://administracionelectronica.gob.es/
- ISO 31000:2009
  Risk management -- Principles and guidelines.
- ISO/IEC Guide 73:2009
  Risk management – Vocabulary.
- ISO/IEC 31010:2009
  Risk management -- Risk assessment techniques.
- ISO/IEC 27005:2011
  Information technology - Security techniques - Information security risk management.
- NIST SP 800-39, 2011
  Managing Information Security Risk: Organization, Mission, and Information System View
  http://csrc.nist.gov/publications/PubsSPs.html
- NIST SP 800-37 Rev. 1, 2010
  Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
  http://csrc.nist.gov/publications/PubsSPs.html
- NIST SP 800-30 Rev. 1, 2012
  Risk Management Guide for Information Technology Systems.
  http://csrc.nist.gov/publications/PubsSPs.html
- ISACA:2013
  COBIT 5 for Risk
  http://www.isaca.org/
- AS/NZS 4360:2004
  Risk management