PILAR RM

Risk Analysis and Management

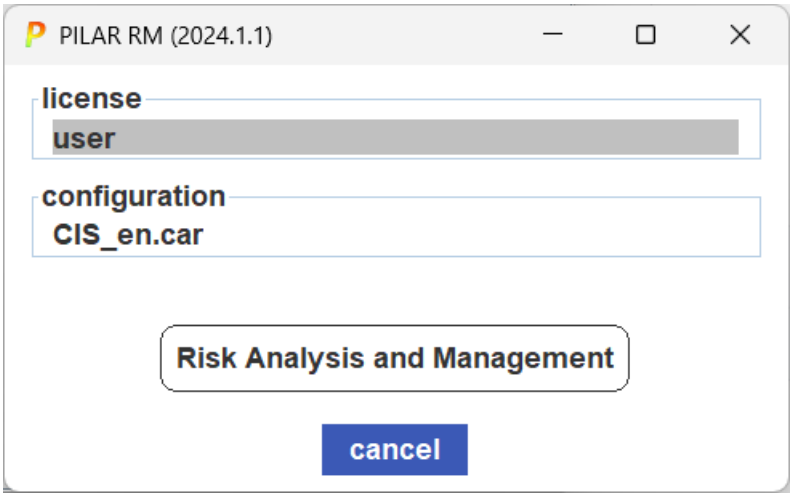
Help Files

version 2024.1

February, 2024

General

1 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.

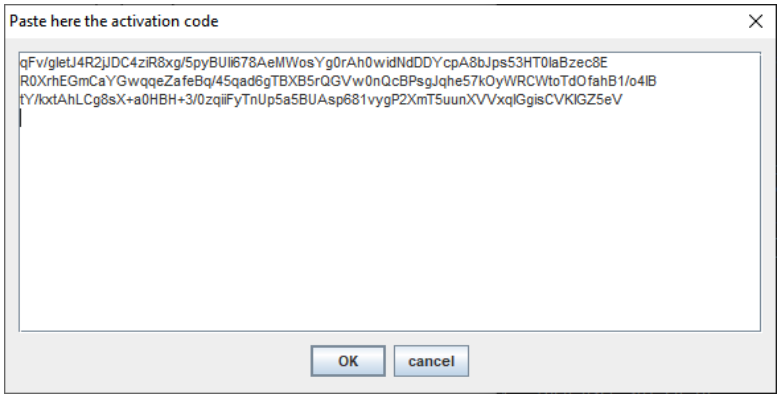
Select “Risk Analysis and Management” to start.

1.1 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.

2 Edit / Options

You may tune the behaviour of PILAR

Normal settings (for plain users):

- *Options / Valuation*
- *Options / Likelihood*
- *Options / Effects*
- *Options / Threats*
- *Options / Maturity*
- *Options / Special phases*

Advanced settings (for advanced users):

- *Options / CSV*
- *Options / Value Model*
- *Options / Project phases*
- *Options / Security domains and project phases*
- *Options / xor*
- *Options / Loops*
- *Options / Save*
- *Options / Export: safeguards*
- *Options / Cross dimension value transfer*
- *Options / Timing*
- *Options / PD risk*
- *Options / Residual risk*
- *Options / ROLL*

These options are specific for each project analysis, so you may edit only when a project is open, and the options will affect only the current project.

Some personalised versions of the tool may offer additional options.

2.1 Options – Valuation

The information system may be rated asset by asset (plus dependencies) or by security domains.

You are always requested to rate the essential assets.

valuation / assets + dependencies

the value of the essential assets is applied to all the assets in the domain.

valuation / assets + domains

the value is distributed according to dependencies between assets.

Domain valuation is faster, while dependencies are more precise.

valuation / mix: assets + dependencies + domains

if the asset has dependencies, use them to get value; otherwise, by domain.

2.2 Options – Likelihood

How to describe the likelihood of a threat.

potential	likelihood	level	ease	ARO
XL extra large	AC almost certain	VH very high	E easy	100
L large	VH very high	H high	M medium	10
M medium	P possible	M medium	D difficult	1
S small	U unlikely	L low	VD very difficult	0.1
XS extra small	VR very rare	VL very low	ED extremely difficult	0.01

ARO – Annual Rate of Occurrence

2.3 Options – Effects

How to describe the consequences of a threat.

level	percentage
T - total	100%
VH - very high	90%
H - high	50%
M - medium	10%
L - low	1%

2.4 Options – Threats

threats / manual

the user explicitly selects threats, and sets the valuation when needed (this is the default behaviour in PILAR before version 4.4)

threats / automatic

the system selects and applies the standard valuation

threats / mix

Something between manual and automatic. By default, threats are identified and valued automatically using the TSV file. However, some assets or threats may be marked as manual. PILAR recalculates automatic values as needed but respects manual ones.

Analysis >> Threats >> valuation

2.5 Options – Maturity

PILAR may use either the maturity levels or administrative statements about the status of the implementation of the safeguard. That is, PILAR changes the text associated to levels L0 to L5.

level	maturity	status
L0	non-existent	does not exist
L1	initial / ad hoc	started
L2	repeatable but intuitive	partly done
L3	defined process	working
L4	managed and measurable	monitored
L5	optimised	continuous improvement

PILAR may translate maturity levels into an index between 0.0 and 1.0; this index is frequently named as percentage (of compliance):

level	index	percentage
L0	0.0	0%
L1	0.1	10%
L2	0.5	50%
L3	0.8	80%
L4	0.9	90%
L5	1.0	100%

2.6 Options – Special phases

Determines whether PILAR presents a project phase with recommendations for safeguards.

Select the ones you with to be shown.

Based on the configuration, PILAR evaluates a number of maturity recommendations that are shown as special phases; e.g. PILAR. You cannot edit the values in these phases; you can only see the recommendation and use it as a reference.

2.7 Options – CSV

You may select the column separator that will be used in CSV exports.

2.8 Options – Value model

You may select between qualitative and quantitative analysis.

Qualitative analysis uses levels (low to high), and when adding levels, the highest level is used.

- See *Assets / Valuation / qualitative*

Quantitative analysis uses numeric quantities, and when adding quantities, traditional addition is used.

- See *Assets / Valuation / quantitative*

2.9 Options – Project phases

Establishes the relationship between phases to re-use maturity values.

project phases / linked

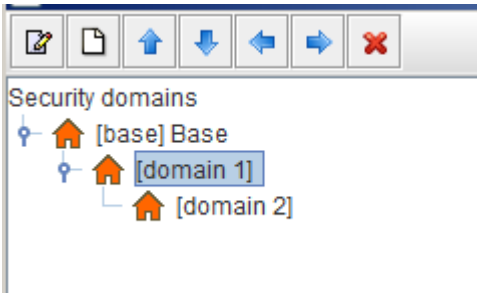
if a safeguard is not evaluated in a phase, the value of the previous phase is inherited

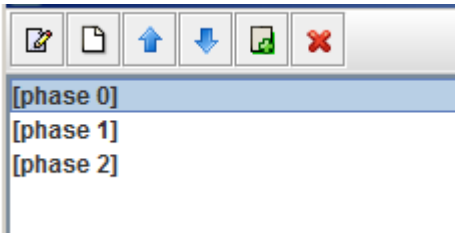
project phases / independent

no value is inherited from any previous phase

2.10 Security domains and project phases

When assigning values to safeguards and controls, if a cell in the table is left empty, PILAR tries to use the value from another cell.





security domains & project phases / phases first

when a safeguard is not evaluated in phase in a domain, PILAR tries to use the value from the previous phase; if none, it tries to use the value from the next security domain

security domains & project phases / domains first

when a safeguard is not evaluated in phase in a domain, PILAR tries to use the value from the next security domain; if none, it tries to use the value from the previous phase
(this is the default behaviour before version 4.4)

	domains first			phases first		
	phase 0	phase 1	phase 2	phase 0	phase 1	phase 2
domain 2	7th	4th	**1st**	**3rd**	**2nd**	**1st**
domain 1	8th	5th	**2nd**	6th	5th	4th
base	9th	6th	**3rd**	9th	8th	7th

When an asset is subject to individual evaluation, it behaves as if in its own (unnamed) security domain. That is:

	domains first			phases first		
	phase 0	phase 1	phase 2	phase 0	phase 1	phase 2
ASSET	7th	4th	**1st**	**3rd**	**2nd**	**1st**
domain 1	8th	5th	**2nd**	6th	5th	4th
base	9th	6th	**3rd**	9th	8th	7th

2.11 Options – Xor

In early versions of PILAR, under XOR marks, several safeguards could be evaluated for maturity. PILAR used the highest valued out of the applicable ones. In order to select one of them for risk mitigation, you may mark other as n.a., or just leave them evaluated with a low value, even no valuation.

Currently, PILAR forces users to select one, and only one, safeguard to apply. The others are marked as n.s. (not selected).

When there is no risk in a security domain, selection makes no sense, and the user can not choose. This feature is used to establish a baseline or general maturity evaluation in a base domain. Later, on subdomains, one of the options may be selected.

2.12 Options – Loops

PILAR supports loops in dependencies. It is a powerful feature but may be disconcerting if it goes out of control. The aim of this option is to make loops optional. But already existing loops are not optional, so PILAR can just call your attention.

allow

loops are allowed; this is the traditional setting

warn

loops are allowed, but the user is informed

no

loops are not allowed; if there are loops, PILAR breaks the loop

This option is to be completed on start-up, when a project is been loaded, but there is still no change to set options. To control project loading, you may use annotations in the CAR file; namely:

load.loops= allow

loops are allowed; this is the traditional setting

load.loops= warn

loops are allowed, but the user is informed

load.loops= no

loops are not allowed; if there are loops, PILAR breaks the loop

Options set from CAR file are valid only for the current session.

2.13 Options – Save

In manual mode, threat valuation is always saved. In automatic mode, threat saving may be skipped; PILAR will recalculate when restarted.

2.14 Options – Export: safeguards

It controls whether safeguard valuation is printed for every phase, or only when there are changes. In the graphical user interface, PILAR only draws explicit values. In textual reports, CSV, and XML, you may choose.

export: safeguards / all: every maturity value

prints every maturity, even if inherited from another phase or domain

export: safeguards / minimal (skip duplicates)

prints only explicit maturity values

2.15 Options – Cross dimension value transfer

Determines whether PILAR propagates value from one security dimension onto another security dimension. For instance, an accountability requirement on essential services is translated onto an integrity requirement on logs.

The mechanism is fully described in https://www.ar-tools.com/doc/

cross dimension value transfer / on

values are transferred from one dimension to another

cross dimension value transfer / off

values are constraint into its original dimension

2.16 Options – Timing

In physical protections, you may estimate the detection, reaction, and response times to remove some attacks that are not feasible because the attacker needs more time than the reactive capabilities of the system under attack.

See “Zones” at https://www.ar-tools.com/doc/

2.17 Options – Privacy risk

When profiles are applied to mitigate risk, you may decide whether only likelihood is mitigated (preventive) or both impact and likelihood are mitigated (mixed, preventive and mitigating).

Default was only likelihood up to 6.2.4.

2.18 Options – Residual risk

PILAR tries to do its best to evaluate the residual risk after applying safeguards; but there is no unique international agreement on the formulae to use.

Up to version 4.2, it was using an algorithm.

After 4.3, it is using a new algorithm that is less aggressive (the effectiveness of safeguards is less aggressive when reducing impact and risk).

2.19 Options – ROLL

Versions of MGR files.

PILAR keeps a copy of the N last versions of MGR files. Namely

name.mgr	last (current) version
name_1.mgr	previous version
name_2.mgr	second previous version
… … …	
name_N.mgr	Nth previous version (oldest version retained)

When xxx.mgr file is saved, for roll versions set to 3, the following sequence is followed:

drop ← xxx_3.mgr ← xxx_2.mgr ← xxx_1.mgr ← xxx.mgr

2.20 Discontinued

From previous versions, no longer available.

2.20.1 Options - Authenticity

This option is not available any longer. Do it manually.

2.20.2 Options - Accountability

This option is not available any longer. Do it manually.

2.20.3 Options – LOG (experimental)

Discontinued.

3 Reports

3.1 From template

PILAR can generate a report following a given pattern. The pattern is a document in RTF format. There are many word processors able to save files in RTF format. Use any of those for preparing a corporate presentation of results.

The format of templates is described at

https://www.ar-tools.com/doc/

3.2 Textual reports

PILAR may generate RTF or HTML texts to be used directly as bulk reports, or to be integrated into your own reports.

The documentation collects the information introduced to PILAR and summarises it in different presentations.

Reports are useful during risk analysis to check that the elements of the system are well recorded, and every stakeholder agrees with the model.

Reports are useful during risk treatment to follow the impact and risk indicators as safeguards are deployed and improved.

Risk summary

A standard all-included report.

Value model (short)

Value model (long)

The report goes through the assets, their dependencies, and their own and accumulated values, dimension by dimension.

- The short version only presents the list of assets, and the value of the assets with own value.
- The long version adds full detail, asset by asset.

Zones

This report lists zones and border elements connecting zones.

Threat report

The report goes through assets and threats, showing the threats on each asset, and the assets exposed to each threat.

Evaluation of safeguards

The report goes safeguard by safeguard, presenting its effectiveness on each phase.

Defects report (report of vulnerabilities)

Similar to the “evaluation of safeguard” report above, but it filters out those safeguards that are good enough. In other words: you select a threshold level, and the safeguards below are reported.

Impact analysis

Presents the impact, accumulated and deflected, on each asset on each phase.

Risk analysis

Presents the risk, accumulated and deflected, on each asset on each phase.

Security profiles (EVL)

Presents the evaluation of the controls of specific security profiles.

3.3 Graphical reports

Value / security domain

Valuation of security domains.

- select one or more domains on the left
  click on tree root to select / deselect all
- select one or more dimensions on the right
  click on tree root to select / deselect all
- click DRAW

Value / asset

Valuation of individual assets.

- select one or more assets on the left
  click on tree root to select / deselect all
- select one or more dimensions on the right
  click on tree root to select / deselect all
- click DRAW

Safeguards / aspect

Overall valuation of safeguards by aspect of security.

- select one or more security domains on the left
  click on tree root to select / deselect all
- select one or more phases on the right
  click on tree root to select / deselect all
- click DRAW

Safeguards / strategy

Overall valuation of safeguards by strategy.

- select one or more security domains on the left
  click on tree root to select / deselect all

- select one or more phases on the right
  click on tree root to select / deselect all
- click DRAW

Safeguards / type of protection

Overall valuation of safeguards by type of operation.

- select one or more security domains on the left
  click on tree root to select / deselect all
- select one or more phases on the right
  click on tree root to select / deselect all
- click DRAW

Accumulated impact / asset

Shows the evolution of impact along phases, asset by asset.

- select one or more assets on the left
  - click on tree root to select / deselect all
  - click on headings of asset groups to select / deselect all the assets in the group
  - click on top-button DOMAINS to add all assets in a given domain
- select one or more phases on the right
  - click on tree root to select / deselect all
  - click on top-button CLEAR to clear the selection
  - click on top-button ALL to select all the phases
- click DRAW to show on screen
- click CSV to export to csv file

To collapse the tree. Only first level of branching.

To adjust the number of levels of branches that are expanded.

Accumulated impact / dimension

Shows the evolution of impact along phases, asset by asset.

- select one or more dimensions on the left
  click on tree root to select / deselect all
- select one or more phases on the right
  click on tree root to select / deselect all
- click DRAW to show on screen

- click CSV to export to csv file

Accumulated risk / asset

Shows the evolution of risk along phases, asset by asset.

- select one or more assets on the left
  - click on tree root to select / deselect all
  - click on headings of asset groups to select / deselect all the assets in the group
  - click on top-button DOMAINS to add assets in a given domain
- select one or more phases on the right
  - click on tree root to select / deselect all
  - click on top-button CLEAR to clear the selection
  - click on top-button ALL to select all the phases
- click DRAW to show on screen
- click CSV to export to csv file

To collapse the tree. Only first level of branching.

To adjust the number of levels of branches that are expanded.

Accumulated risk / dimension

Shows the evolution of risk along phases, asset by asset. The tree-map displays an area that is proportional to the risk on the asset shown on the label.

- select one or more dimensions on the left
  click on tree root to select / deselect all
- select one or more phases on the right
  click on tree root to select / deselect all
- click DRAW to show on screen
- click CSV to export to csv file

Accumulated risk / dimension / phase

Shows the distribution of risk in one dimension in one phase, asset by asset.

- select one dimension on the left
- select one phase on the right
- click DRAW to show on screen

Deflected impact

Shows the evolution of impact along phases, asset by asset.

- select one or more assets on the left
    - click on tree root to select / deselect all
    - click on headings of asset groups to select / deselect all the assets in the group
    - click on top-button DOMAINS to add assets in a given domain
- select one or more phases on the right
    - click on tree root to select / deselect all
    - click on top-button CLEAR to clear the selection
    - click on top-button ALL to select all the phases
- click DRAW to show on screen
- click CSV to export to csv file

To collapse the tree. Only first level of branching.

To adjust the number of levels of branches that are expanded.

Deflected risk

Shows the evolution of risk along phases, asset by asset.

- select one or more assets on the left
    - click on tree root to select / deselect all
    - click on headings of asset groups to select / deselect all the assets in the group
    - click on top-button DOMAINS to add assets in a given domain
- select one or more phases on the right
    - click on tree root to select / deselect all
    - click on top-button CLEAR to clear the selection
    - click on top-button ALL to select all the phases
- click DRAW to show on screen
- click CSV to export to csv file

To collapse the tree. Only first level of branching.

To adjust the number of levels of branches that are expanded.

Pareto

This graph is only available in quantitative analysis.

It is a vertical histogram after sorting the assets on the X axis from higher to lower contribution to the total value; the graph also shows the total value, and the incremental contribution of each value to the final total.

3.4 Databases

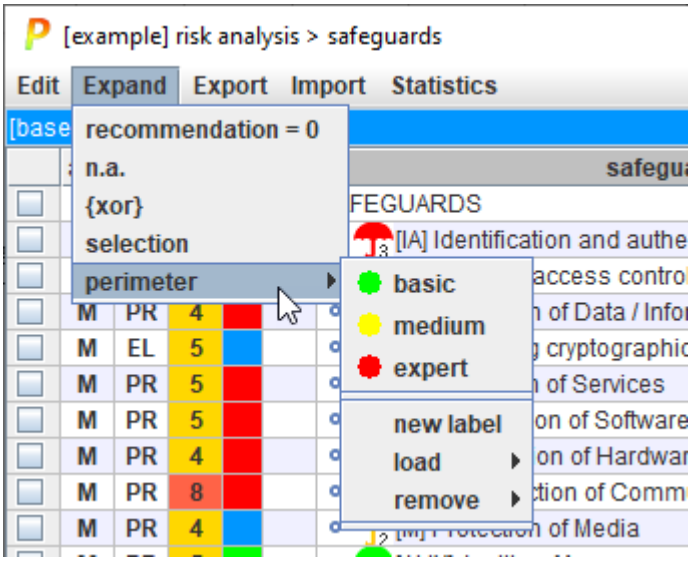
You can find instructions on using PILAR with an external database at

https://www.ar-tools.com/doc/

4 Perimeters

Perimeters are expansion patterns for trees of safeguards and security profiles (evl).

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
```

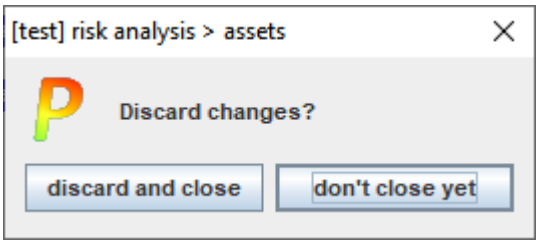
Screens

5 OK, Cancel, Help

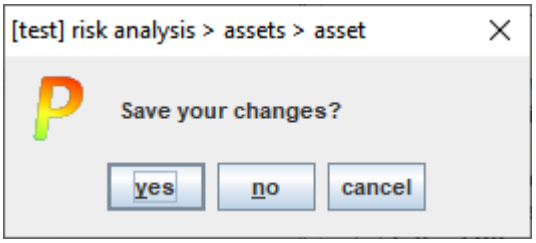
Most screens include buttons for:

	OK. The changes are saved, and the screen is closed.
	CANCEL. The changes are undone, and the screen is closed.
	HELP. Jumps into this help files.

If there are changes, and you click CANCEL, PILAR will ask for confirmation:



If there are changes, and you try to close the window, PILAR will ask for instructions on how to proceed:

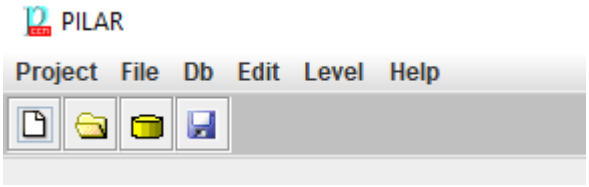


where you can

CANCEL	Do not exit.
NO	Discard changes and exit.
YES	Save changes and exit.

6 Main control panel

6.1 Basic controls



Top menu PROJECT

New	Starts a new project from scratch
Reopen	Returns to recent projects
Reload	Reloads project from external source
Save	Saves current project either in a file, or in database (according to its source).
Import (xml)	Imports data in XML format. See https://www.ar-tools.com/doc/
Export (xml)	Exports project data onto XML format. See https://www.ar-tools.com/doc/
Translation	You may generate a translation table or apply a translation table. See users' manual
Save and exit	Saves project, and terminates
Cancel and exit	Terminates without saving data

Top menu FILE

Open	Starts an existing project from a file
Import	Imports data from another project on top of this one.
Save as ...	Saves a copy, where the user may select the file, and establish a password
save subsets	An XML file is generated. It collects the dimensions, classes, threats, and valuation criteria that have been marked as OFF. Later on, this XML file may be referenced from a configuration file (.car) and PILAR will start excluding those elements. subsets = subsets.xml

Top menu DB

Only if the license enables SQL support.

Database tables are described in a separate document.

See https://www.ar-tools.com/doc/

Open	Starts an existing project from a database
Import	Imports data from another project on top of this one, reading from a database
Save as ...	Saves a copy, where the user may select the database

Top menu EDIT

Preferences	sets font size and family.
Options	see *Edit_options*

Top menu LEVEL

Basic	Only basic options, with the aim of simplifying life to early users.
Medium	Somewhere in between basic and expert
Expert	All the options are shown

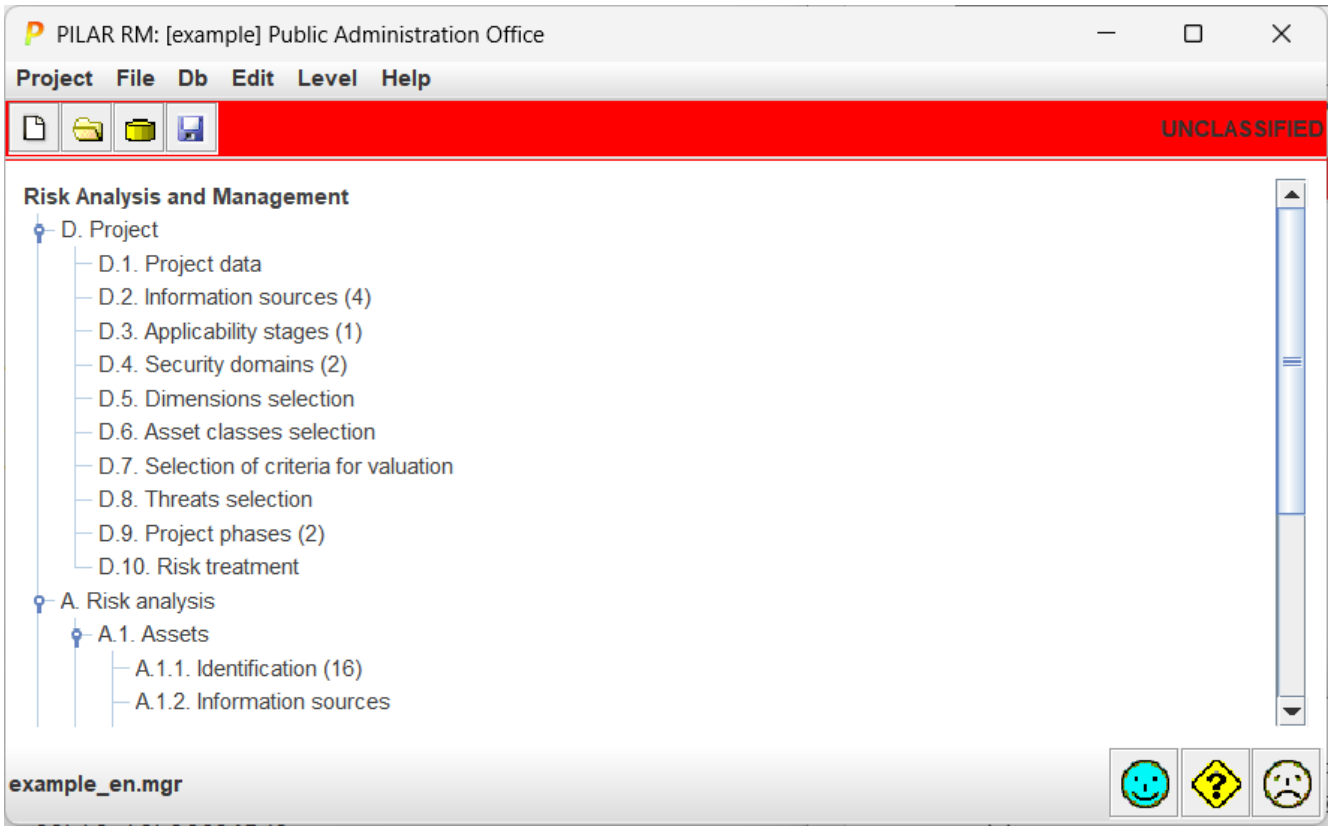
Top menu HELP

help	starts the in-line help pages
about PILAR	shows version information
last version?	connects to PILAR web site to check for updates
system status	presents current usage of system resources

Top toolbar

	Starts a new project from scratch
	Starts an existing project from a file
	Starts an existing project from a database
	Saves current project either in a file, or in database (according to its source).

6.2 Project controls

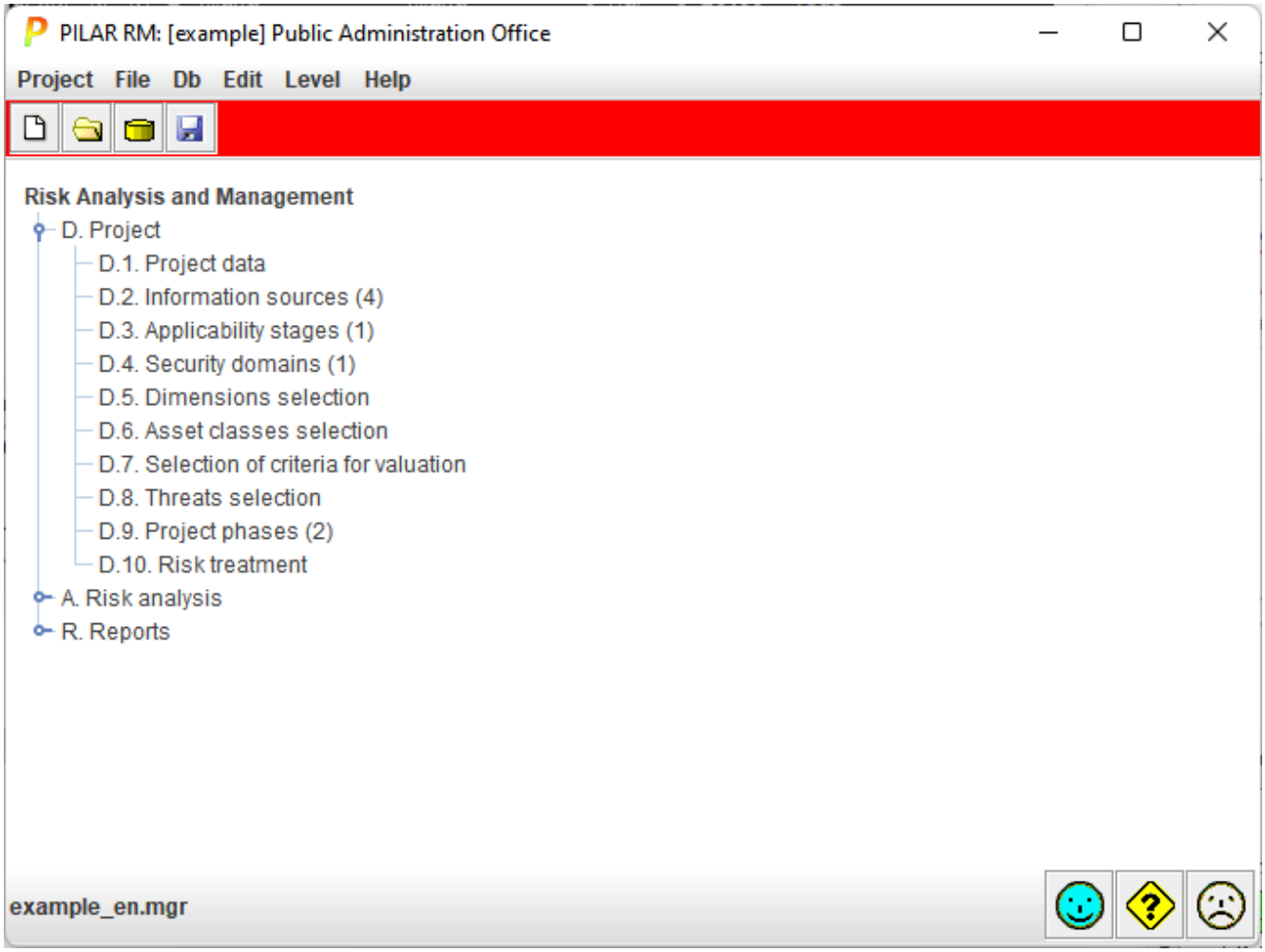


The bottom row presents the name of the file, or of the database.

The inner tree presents the activities. Expand as needed and click to jump to the corresponding activity.

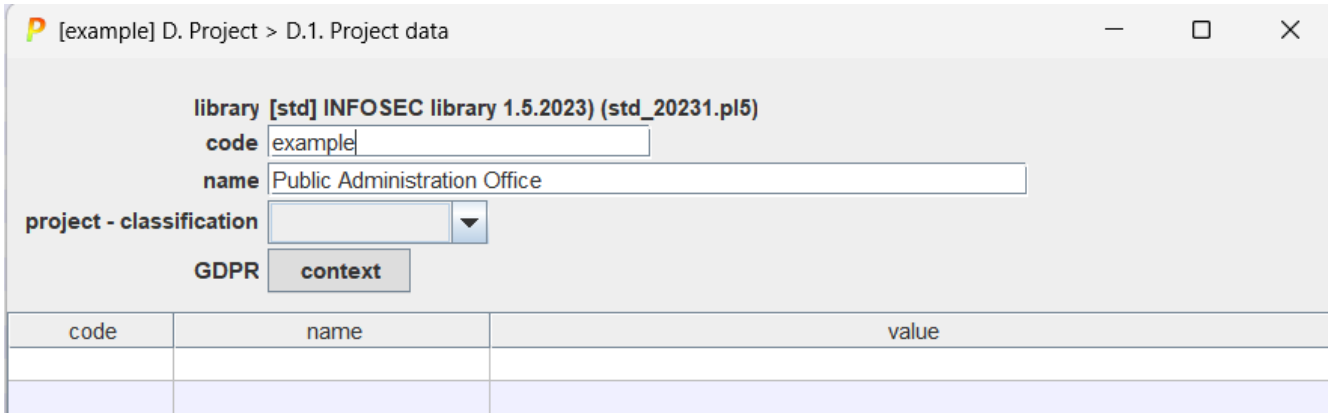
Numbers count elements defined by the user; in the above example, 4 information sources, 1 stage, 2 security domains, 16 assets, etc.

7 Project



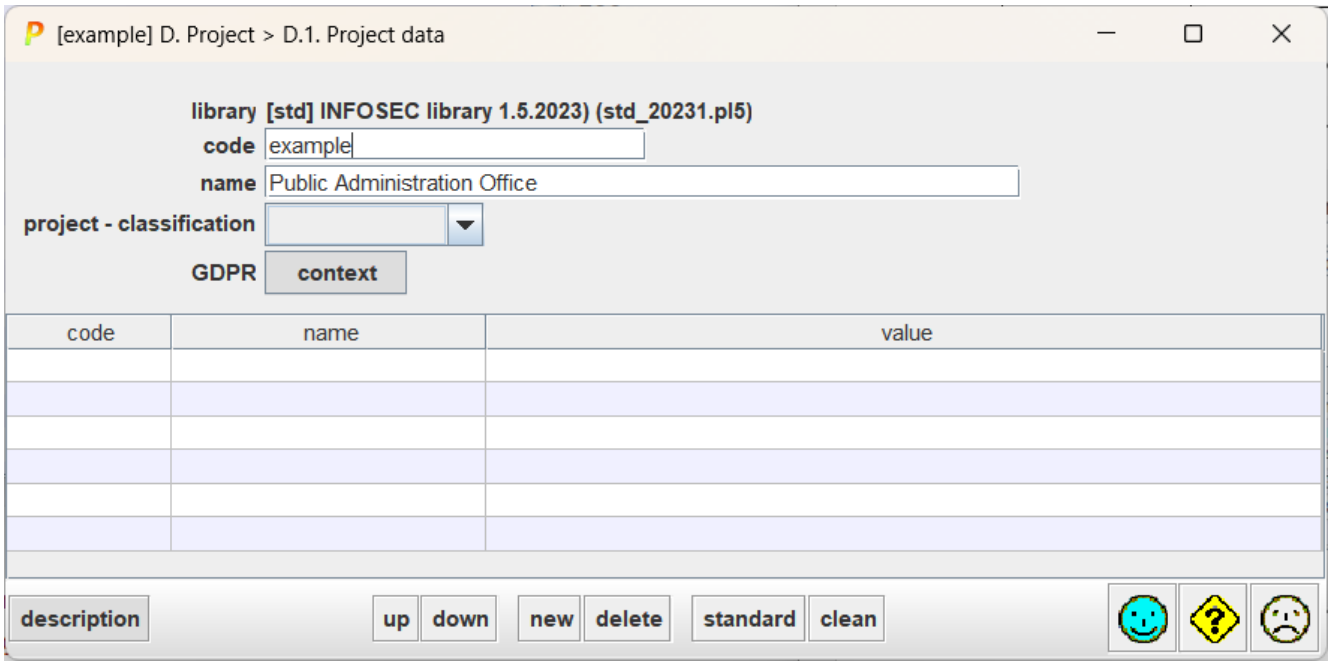
7.1 Project data

Quick start
Select a code and a descriptive name. Click **OK** to continue.



library	The library (selected on start-up). See configuration in users' manual
code	The project code: it should be unique
name	The name: a short description
classification	The default marking for the reports
GDPR context	You may load administrative information to meet the requirements of the GDPR. This information may be system-wide, here, or for specific assets. See *gdpr_data*

You may add administrative information: key-value pairs.

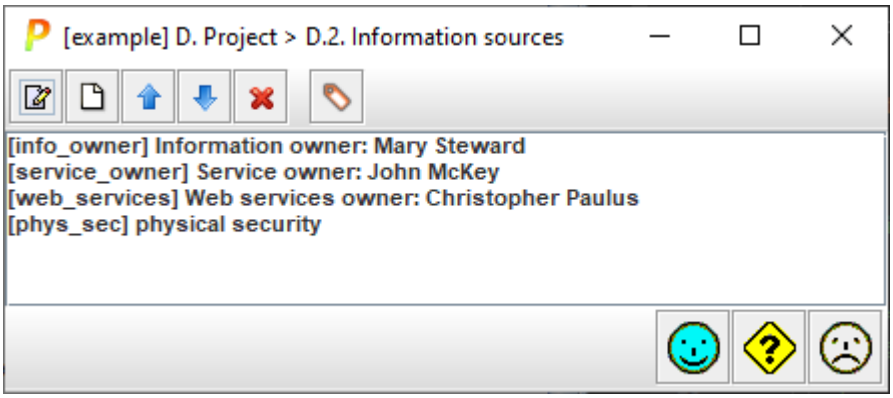


code	Key codes for key-value pairs. Useful for translations. Click to edit.
name	Key names for key-value pairs. Click to edit.
value	Values for key-value pairs. Click to edit.
up	Select a key-value pair and move it up in the list.
down	Select a key-value pair and move it down in the list.
new	Create a new row.
delete	Remove a row.
standard	Add standard keys.

clean	Remove empty rows.
description	A longer description. The description may include hyperlinks (URLs). To go to the linked page RIGHT-CLICK, then

7.2 Information sources

This screen is used to identify and manage information sources.

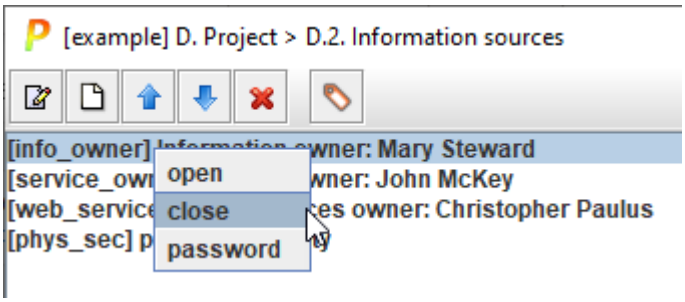


	select a source and click to edit
	select a source and click to add another source
	select a source and click to move it up also: SHIFT + UP_ARROW
	select a source and click to move it down also: SHIFT + DOWN_ARROW
	select a source and click to delete it also: DELETE

	adds standard labels. Standard labels are user defined in INFO configuration file.
	Default values are as follows:
	`<sources>`
	`  <source c="lr">legal restrictions</source>`
	`  <source c="nj">not justified</source>`
	`  <source c="nj.1">not worth the money</source>`
	`  <source c="nj.2">more discomfort than benfit</source>`
	`  <source c="nj.3">impractical (unrealistic)</source>`
	`</sources>`

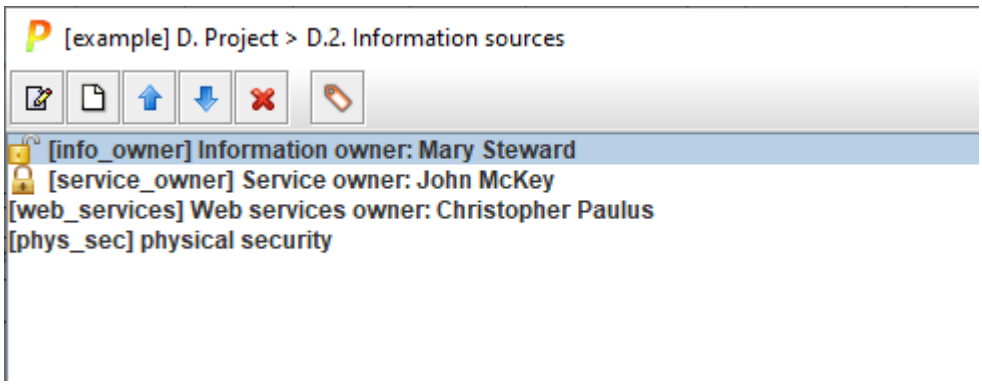
panel	list of sources select and double click to edit

You may right-click on an information source to manage an associated password:



password	to set (or remove) a password
login	to provide the password to open the source
logout	to close the source

When a source has an associated password, it may be open or closed.



Closed sources block write/modify operations on elements associated to the source. You need either a password-free or an open source to have write access to elements associated to them.

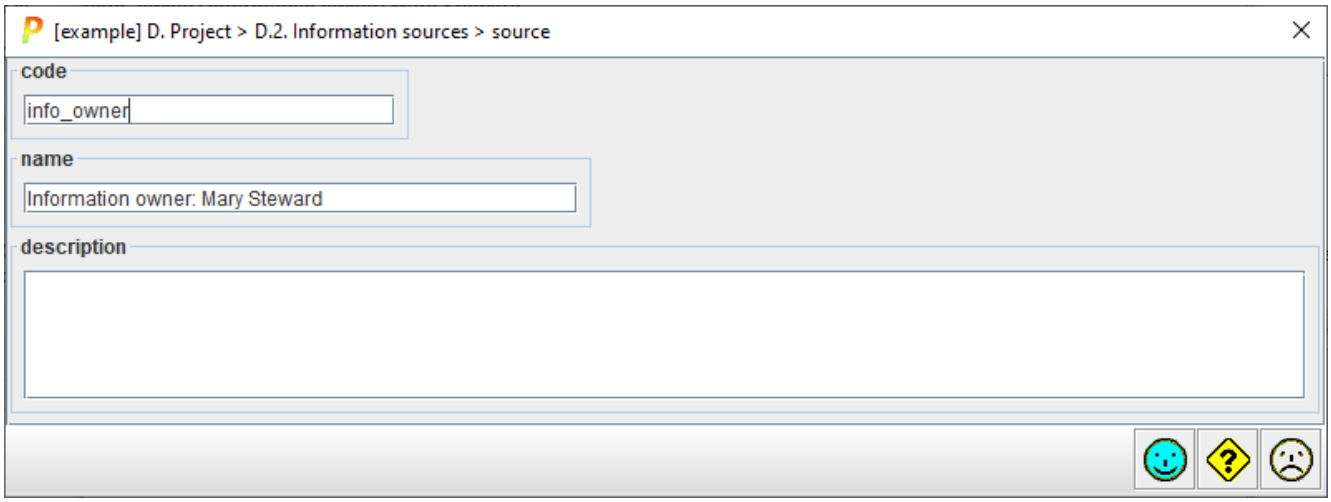
See “access control” on users’ manual.

7.2.1 Edition

When editing an information source, you may specify:

- the code: it must be unique
- the name: a short description
- a longer description

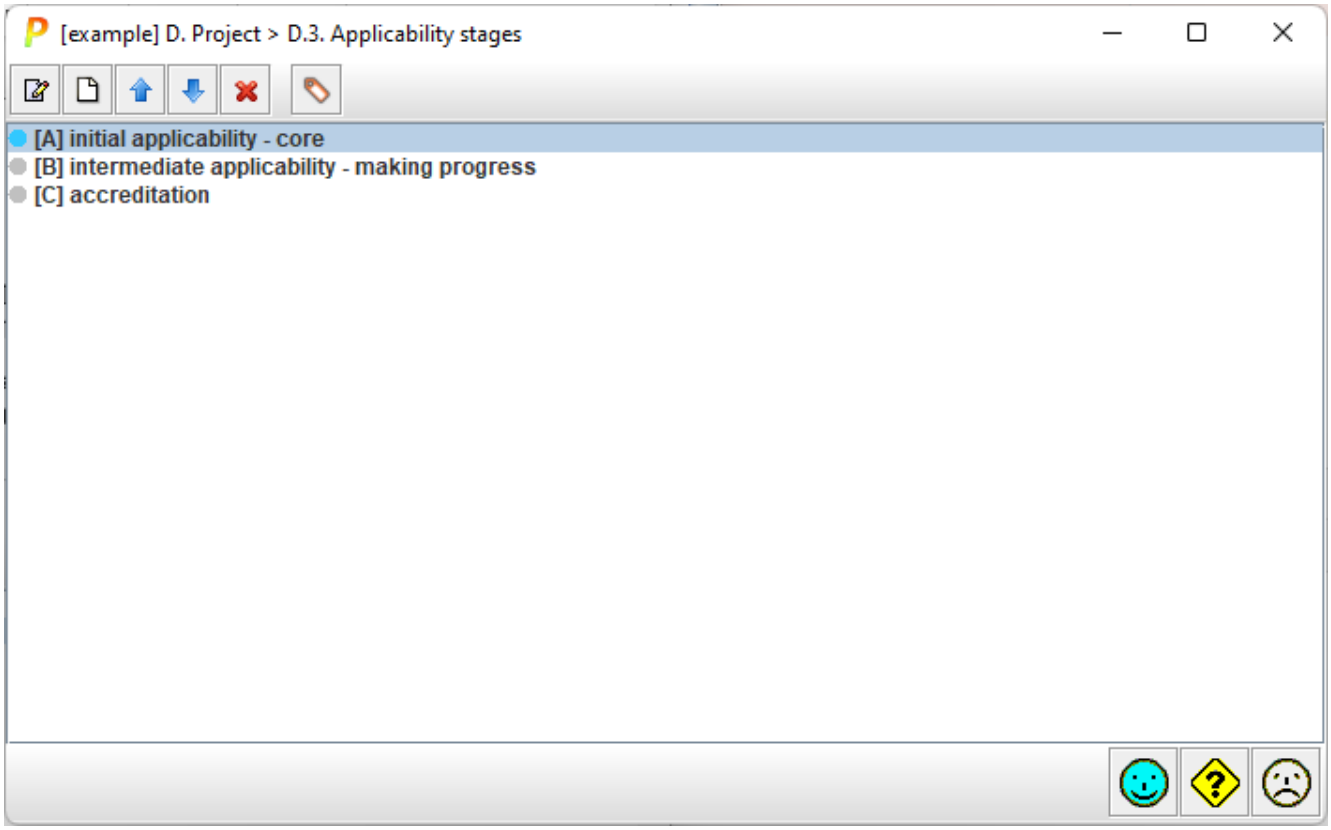
The description may include hyperlinks (URLs). To go to the linked page RIGHT-CLICK, then 


[example] D. Project > D.2. Information sources > source
code
info_owner
name
Information owner: Mary Steward
description

7.3 Applicability stages

You may define several applicability stages. That means that in different project stages, different safeguards and controls are selected as applicable.

This functionality is useful when you want to stablish an implementation roadmap and incorporate security measures gradually. Or when different accreditation bodies approve different applicability statements.



The small bullet on the left shows which one is the current applicability (the applicability values that are applied currently). Grey bullet for every stage, and blue bullet for current one.

	select a stage and click to edit
	select a stage and click to add another stage below it
	select a stage and click to move it up also: SHIFT + UP_ARROW
	select a stage and click to move it down also: SHIFT + DOWN_ARROW
	select a stage and click to delete it also: DELETE
	adds standard stages; standard stages are user defined in INFO configuration file.

On the panel

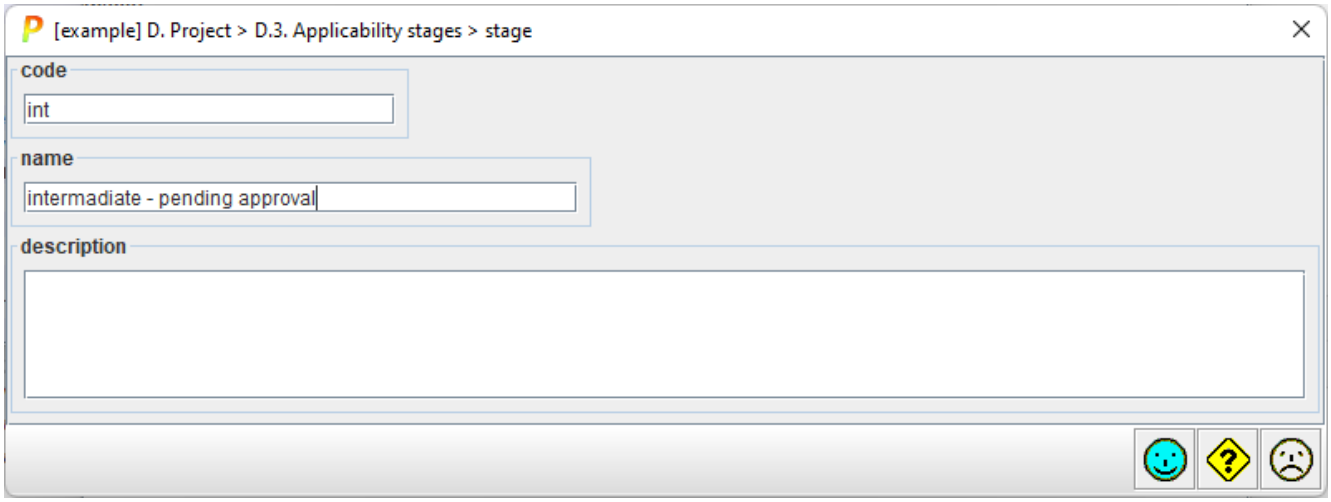
- select and double click to edit
- right-click to select a stage as current

7.3.1 Edition

When editing a stage, you may specify

— the code: it must be unique
— the name of the stage
— a longer description

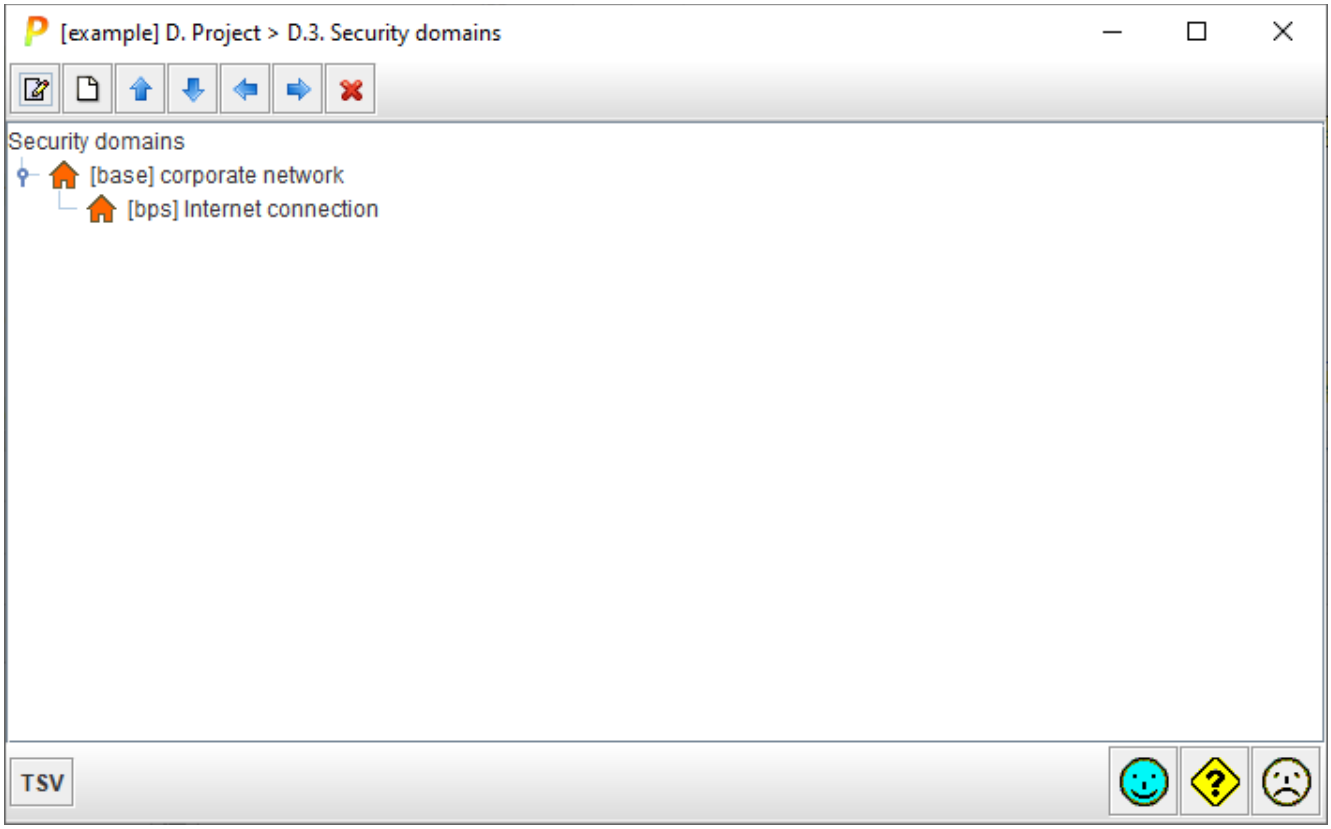
The description may include hyperlinks (URLs). To go to the linked page RIGHT-CLICK, then



7.4 Security domains

You may classify assets into security domains. Each domain has a separate evaluation of safeguards. When different assets are subject to different safeguards, or safeguard maturities, domains permit to organise the assets into groups.

This screen establishes and manages a hierarchy of domains. There is always a BASE domain you may not remove. Assets that are not assigned to any domain remain in the BASE domain.



Top toolbar:

	select a domain and click to edit
	select a domain and click to add another domain within it
	select a domain and click to move it up also: SHIFT + UP_ARROW
	select a domain and click to move it down also: SHIFT + DOWN_ARROW
	select a domain and click to move it left also: SHIFT + LEFT_ARROW
	select a domain and click to move it right also: SHIFT + RIGHT_ARROW
	select a domain and click to delete it

	also: DELETE

On the panel with the hierarchy of domains

- select and double click to edit
- click on the handle to expand / collapse the tree

Click bottom TSV to assign a threats profile to each security domain.

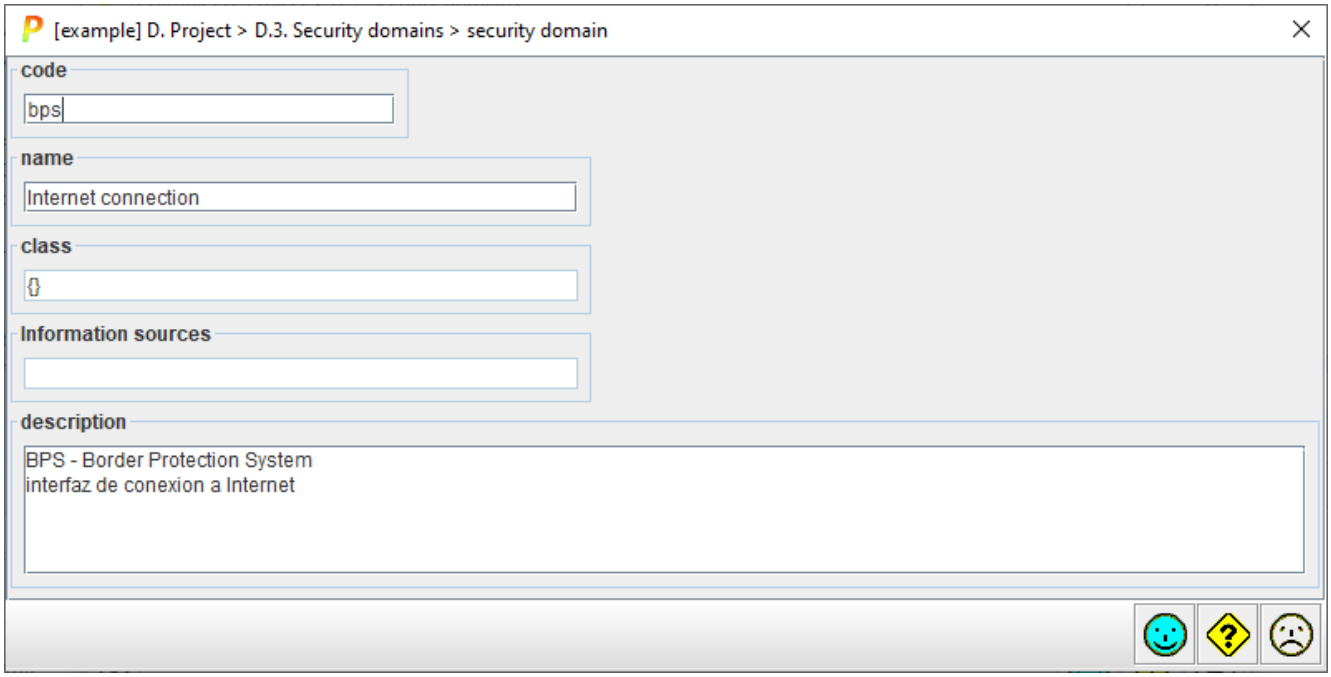
- See "*Threat Standard Values*".

7.4.1 Edition

When editing a security domain, you may specify

— the code: it must be unique
— the name of the security domain
— the domain class; this is used to mark the domain to be evaluated under specific security profiles; the classes depend on the configuration
— one or more sources of information
— a longer description

The description may include hyperlinks (URLs). To go to the linked page RIGHT-CLICK, then 

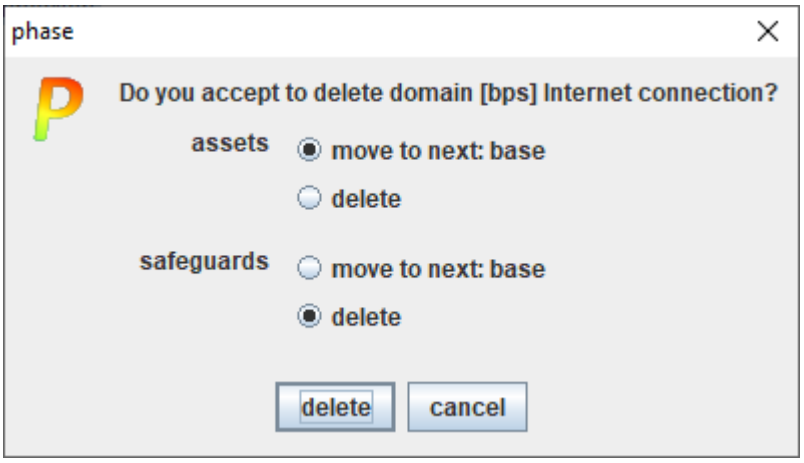


Sources control the write access to elements in the domain: assets, safeguards and controls.

A domain may be labelled with one or more classes. The set of available classes is determined by configuration. Most classes lack any semantics; it is just a mark to filter domains.

7.4.2 Removal

When you try to delete a domain, PILAR asks what to do with the data in that domain; to be precise, what to do with the assets in the domain, and what to do with the safeguards evaluated in that domain. If the domain does not have another one above, there is little to do: delete the data. But if the domain is nested, you may choose to send assets and safeguards to the nesting domain:

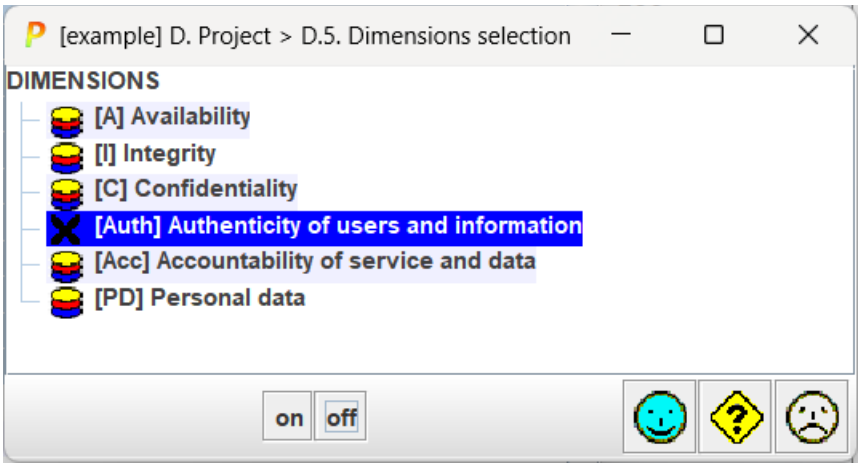


7.5 Dimensions selection

The standard library establishes the available dimensions.

However, you may switch off some dimensions. Click on the check box to select.

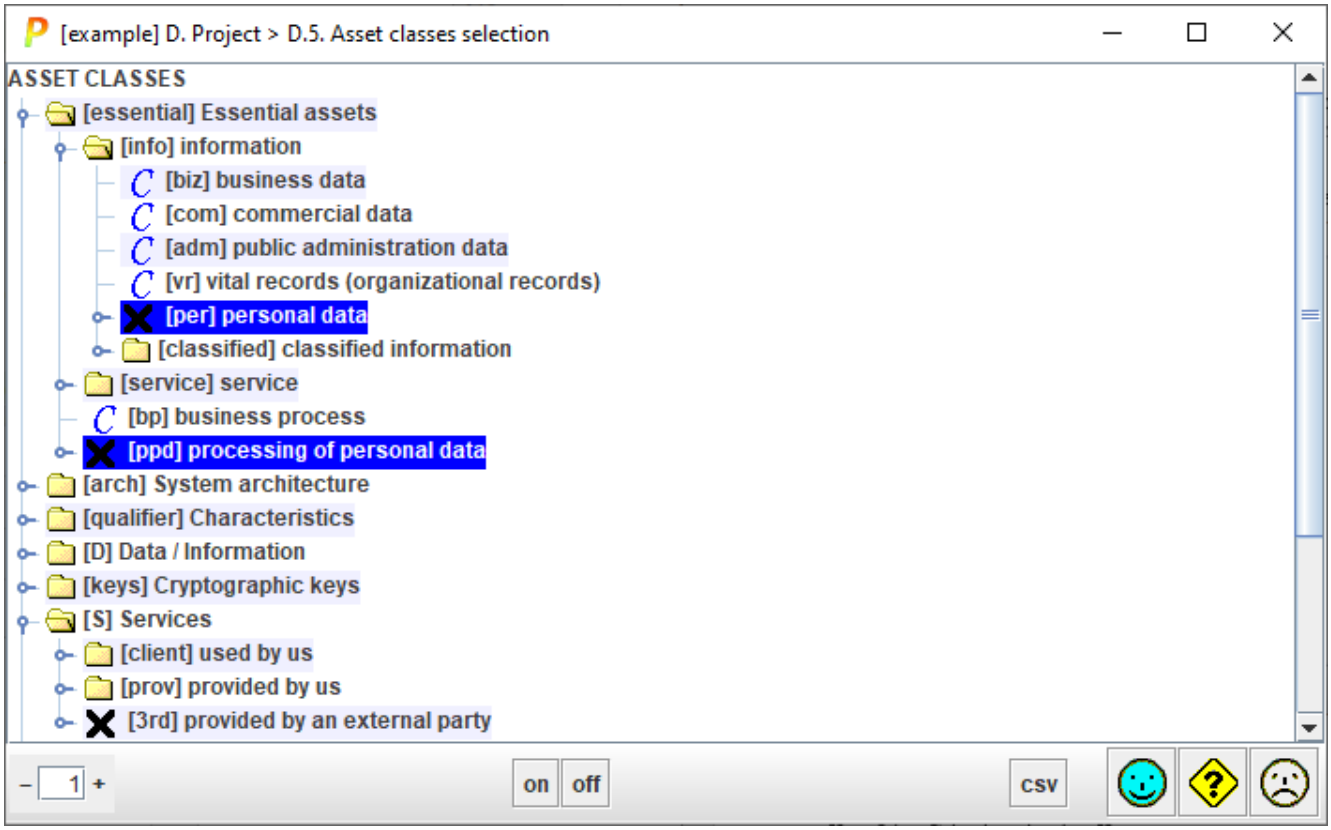
Deselected dimensions are not removed from the model. The only effect is to remove from the presentations, so you may focus on the "topic of the day" removing unnecessary information from the screens.



7.6 Asset classes selection

Assets classes qualify assets. Available classes are provided by the standard library and can be extended by the user via personalization files. You may, project by project, hide out some classes to focus on the relevant ones.

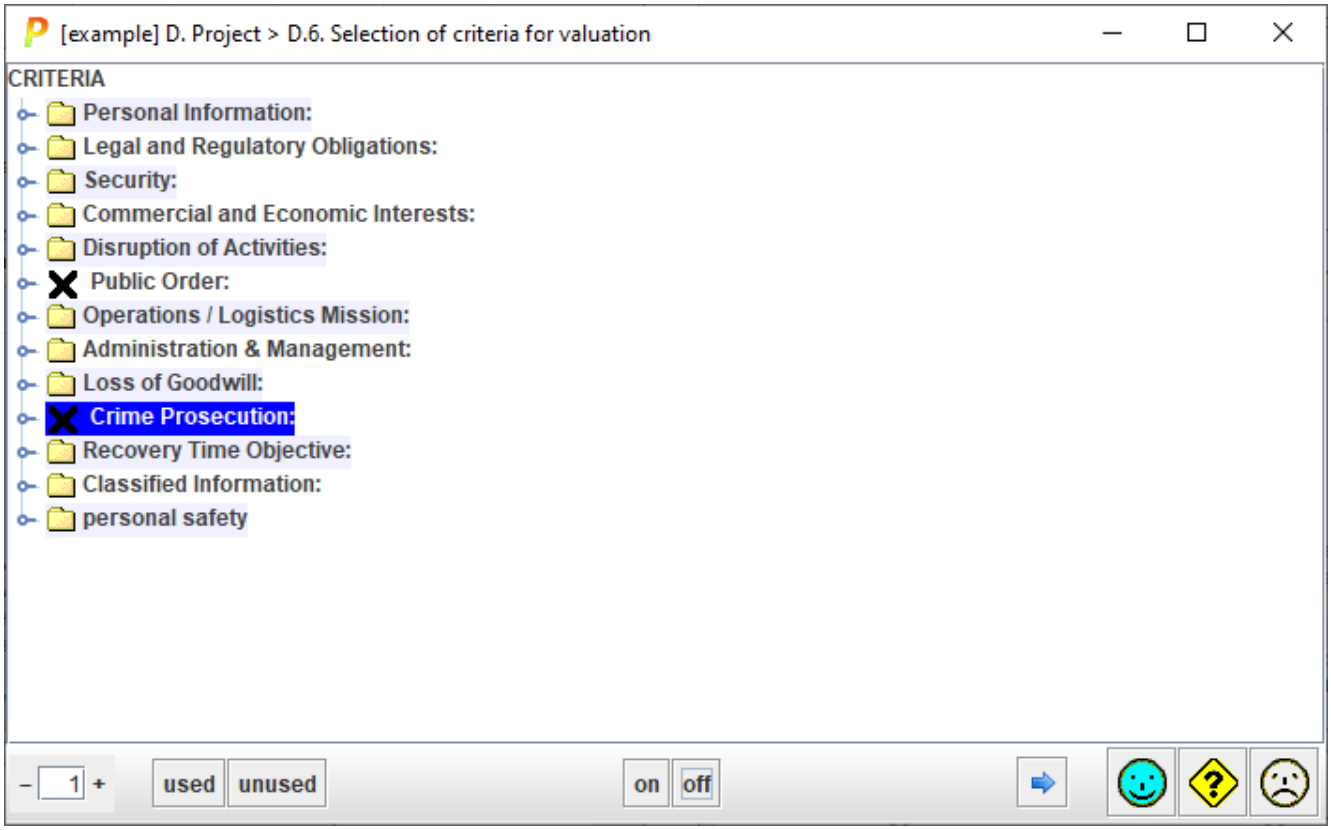
Select the classes you want to hide / unhide and use ON / OFF buttons.



7.7 Selection of criteria for valuation

The standard library provides a collection of standard criteria to assign value levels to assets. However, you may switch off some criteria.

Off criteria are not removed from the model. The only effect is to remove them from the presentations, removing unnecessary information from the screens.



Basic use: select one or more criteria on central panel and click bottom ON / OFF buttons to select / unselect the criteria.

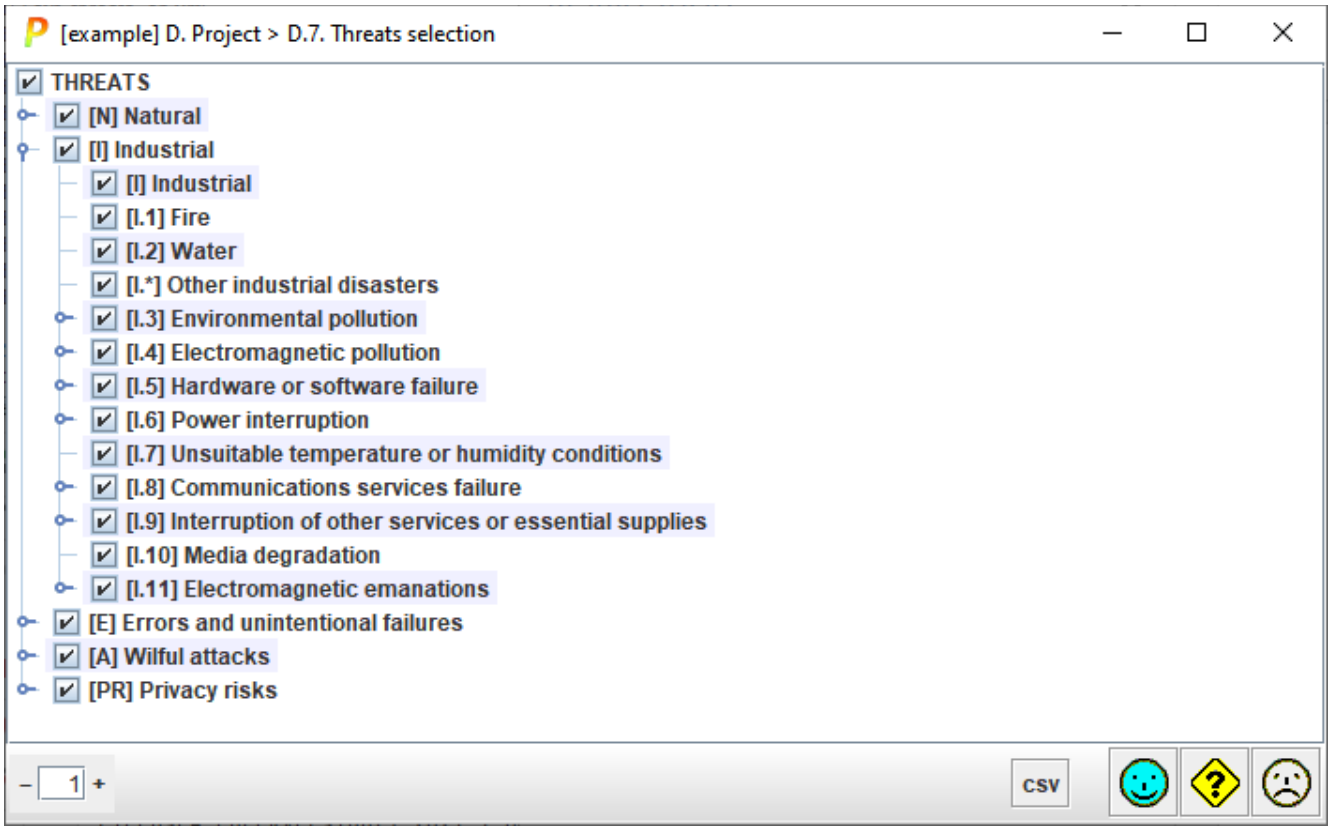
- 1 +	Select the level of expansion of the tree.
used	Selects those criteria currently used in the risk analysis project.
unused	Select those criteria that are not currently used in the risk analysis project.
on	enable selected criteria
off	disable (hide) selected criteria
csv	export selected criteria to csv file

7.8 Threats selection

The standard library establishes the available threats.

However, you may switch off some threats. Select the threat or threat group and click ON / OFF buttons on the bottom.

Off threats are not removed from the model. The only effect is to remove from the presentations, so you may focus on the "topic of the day" removing unnecessary information from the screens.



☑ ☐	Click to turn on/off one threat or a group of threats.
– 1 +	Select the level of expansion of the tree.
csv	export to csv file

7.9 Project phases

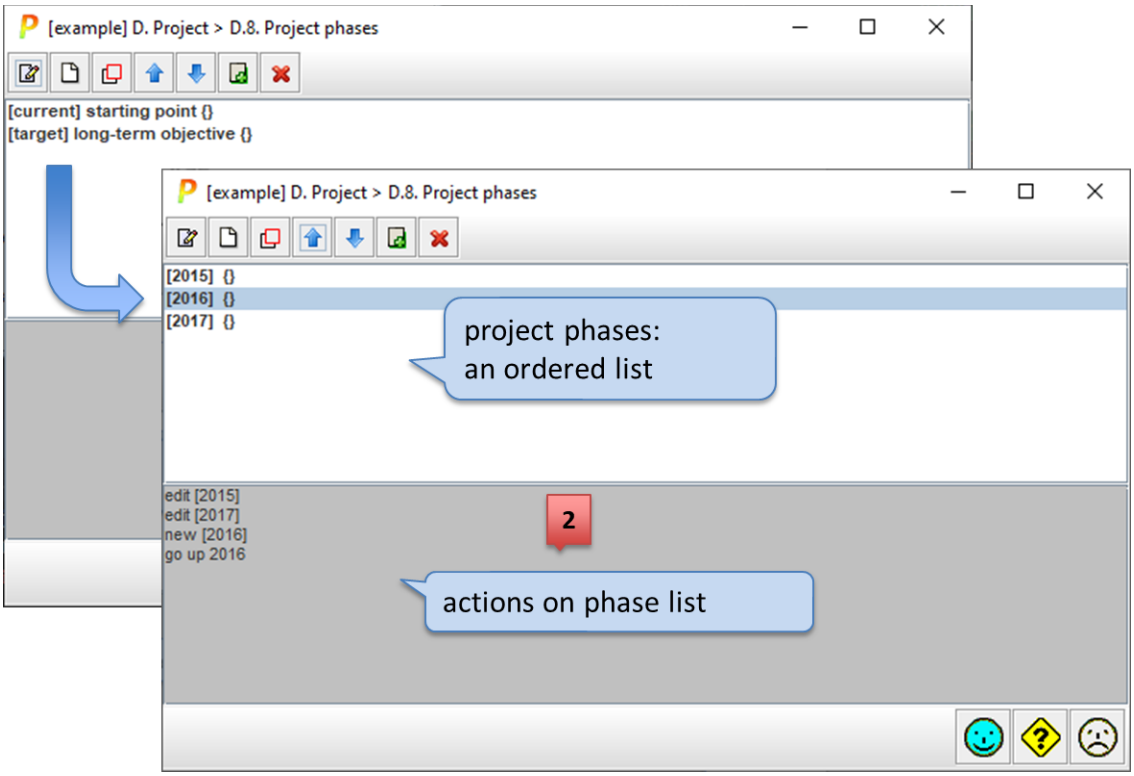
Quick start
Do nothing! The standard should be enough: • [current] the system as it is today • [target] the system you would love to have Click **OK** to continue.

Let us identify the phases of the project, to show risk evolution. At least, there is always a base phase, which shows the current situation. Then several phases mark the future evolution.

You may identify and assign values to backup equipment and safeguards in each phase.

There are several ways to use the phases:

- as different stages of a project to improve security; that is, to review the progress of risk as security improvement programs are executed
- as historical, for example for years, to present the progress of system security



	Click to edit the selected phase. See "*Edit one phase*".
	Click to create a new phase. See "*Edit one phase*".
	Click to clone the selected phase. A new phase is created that inherits all the values associated to the original one. Then you may edit to adjust.

	to move a phase up (before the previous one) also SHIFT + UP_ARROW (one or more phases)
	to move a phase down (after the next one) also SHIFT + DOWN_ARROW (one or more phases)
	Click to merge two phases into one. It merges the selected phase with the following one. This action is typically used before a phase is removed in order to use the values of the disappearing phase into the next phase(s). See "*Combination and removal of phases*
	Remove the selected phase.

7.9.1 Combination and removal of phases

Let us have 4 phases: F1, F2, F3 y F4

and the following valuation of a group of safeguards

	F1	F2	F3	F4
group	L1	L1-L2	L1-L3	L1-L3
S1	L1			
S2	L1	L2		
S3	L1	L2	L3	

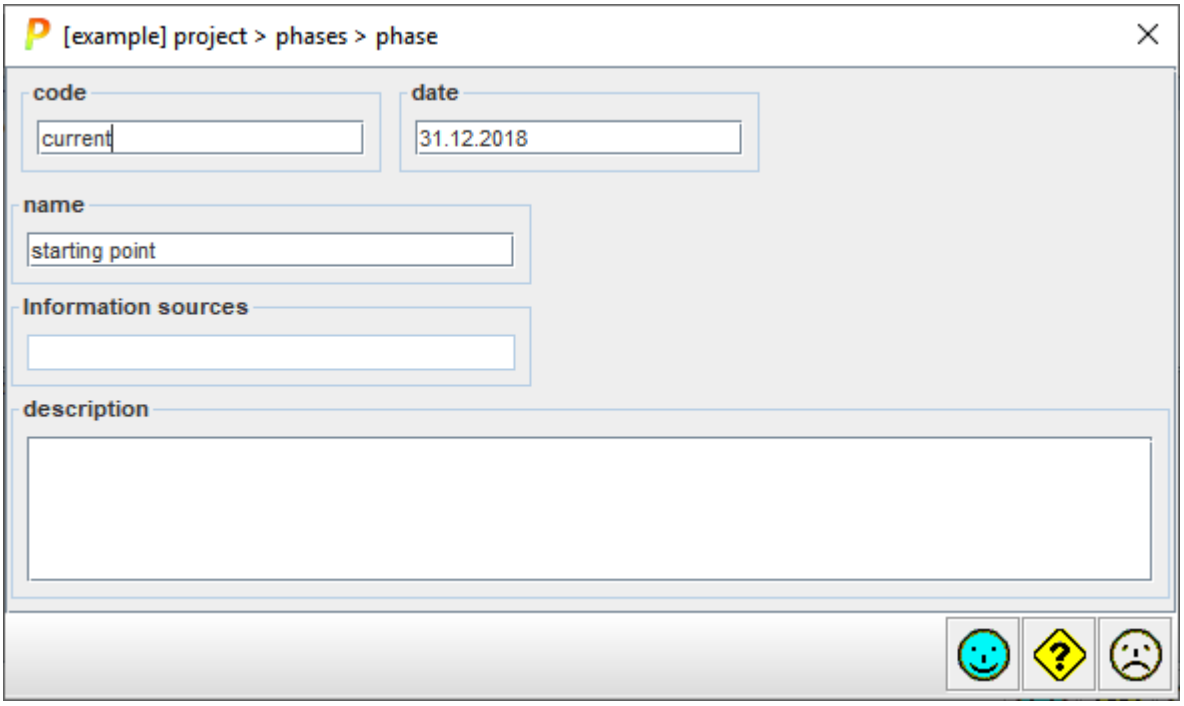
If we combine F2 + F3, the values in phase F2 that are not modified in phase F3, are copied in phase F3:

	F1	F2	F3	F4
group	L1	L1-L2	L1-L3	L1-L3
S1	L1			
S2	L1	L2	L2	
S3	L1	L2	L3	

So, we may now remove phase F2 without losing information:

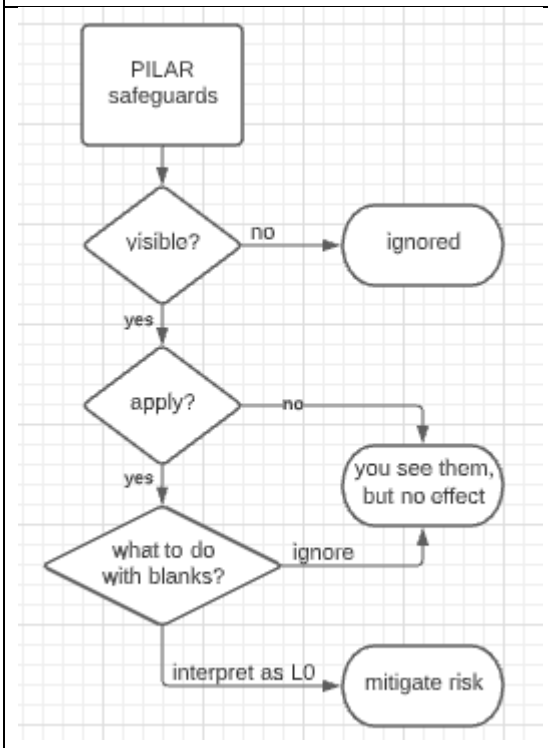
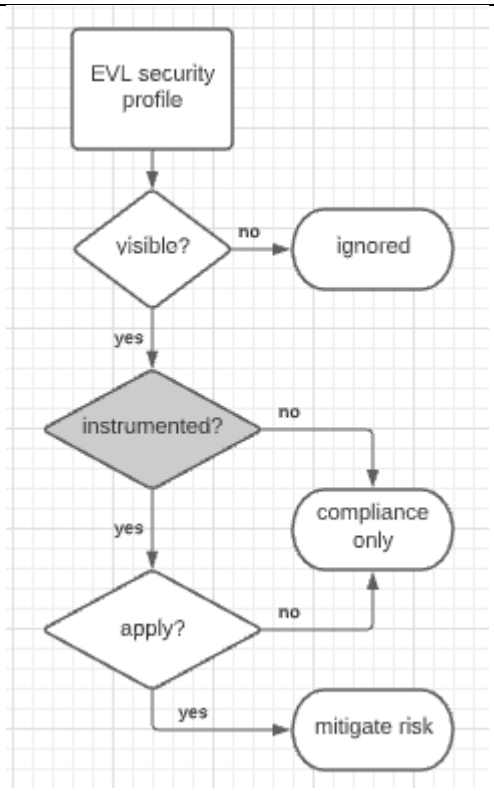
	F1	F3	F4
group	L1	L1-L3	L1-L3
S1	L1		
S2	L1	L2	
S3	L1	L3	

7.9.2 Edit one phase



code	it must be unique
date	(optional) a point in time to associate PILAR phases to actual time. Format is: day . month . year
name	a short description
sources	Sources of information associated to the phase. Sources control write access to safeguard and control rating for the phase.
description	A longer description The description may include hyperlinks (URLs). To go to the linked page RIGHT-CLICK, then

7.10 Risk Treatment

SUMMARY	
safeguards (PILAR and NIST)	security profiles (EVL)
	

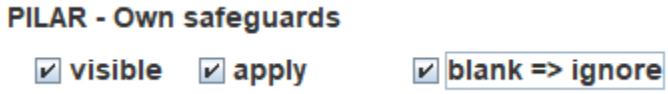
You may control how different security measures (safeguards and profile controls) are used.

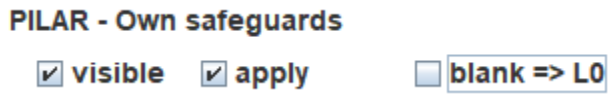
For the collection of safeguards in PILAR, you may see them (visible) or not.

- If not visible, they are completely ignored in interface and in risk mitigation.

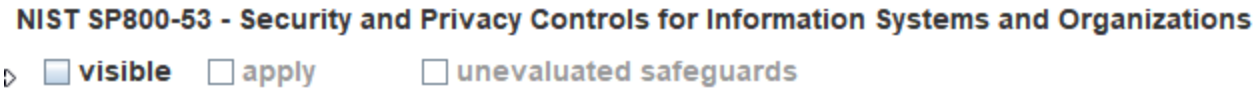
- If visible, you may choose whether they are applied to mitigate risk, or not.

- If visible and applicable, you may choose how to deal with safeguards that are not evaluated (blank). You may ignore them or use them as if a L0 maturity value were assigned to them.



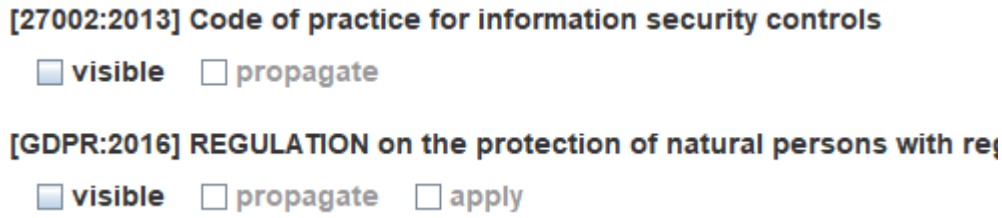


For NIST 800-53 rev.5 collection of safeguards, you have the same options:

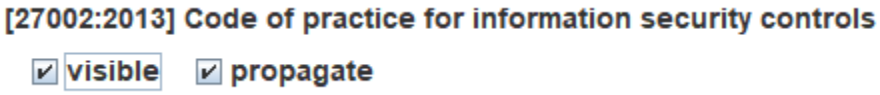


For security profiles, EVL, you may select whether they are visible o invisible.

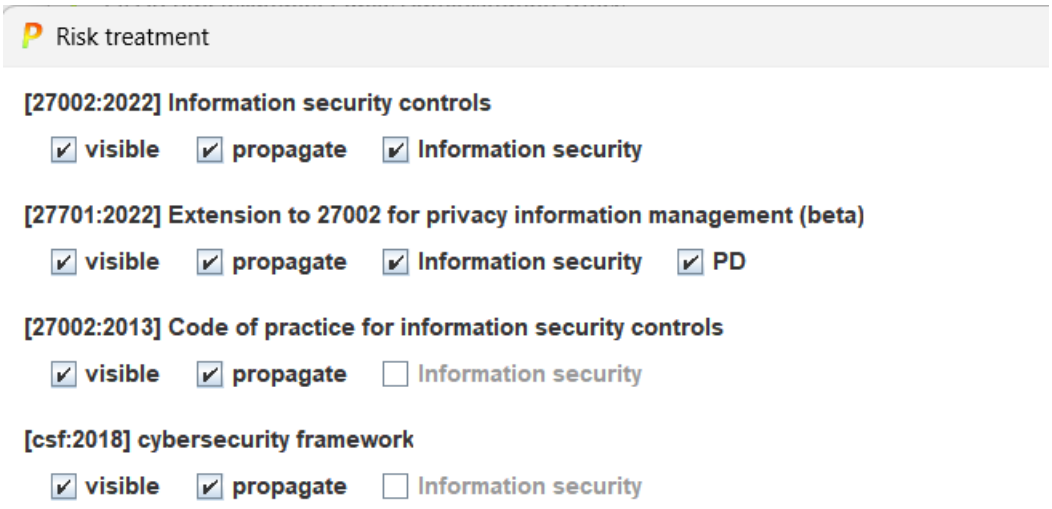
- If invisible, they are ignored.



- If visible, you may choose whether maturity values set for controls are automatically propagated (pushed down) to the mapped safeguards.



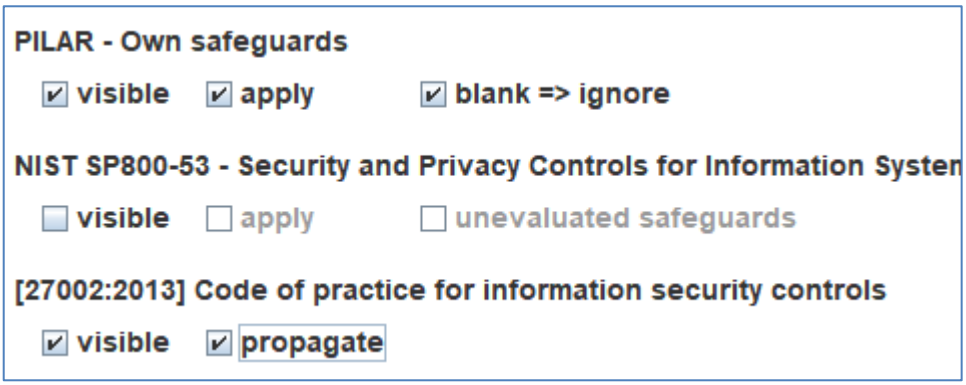
- For some security profiles, if visible, you may choose to apply their controls to mitigate risk. only some EVL are instrumented with the mitigation knowledge. Some security profiles may be used to mitigate information security risks, other to mitigate privacy risks, and some may be used for both areas. You choose …



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

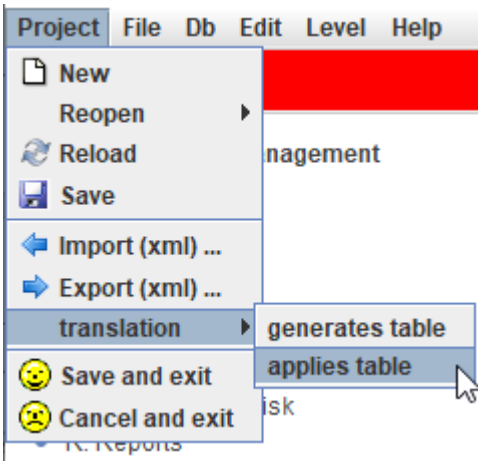
Previous version of PILAR used ONLY PILAR collection of safeguards to treat risk and used EVL profiles for compliance. You may fall back to that working mode selecting options like this

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



7.11 Project translation

You may translate the language used for project elements. PILAR may translate element code and element name.



During generation, a translation table is generated with the rules to translate project, information sources, security domains, layers, assets, and phases.

During application, the rules are applied sequentially.

A translation table is a text file. Each line in the file is a translation rule.

Character '#' is used to mark comments, that are not interpreted.

Rewrite rules are lines with the following format

```
element : [src_code] src_name -> [target_code] target_name
```

element is one of: 'project', 'source', 'domain', 'layer', 'asset', or 'phase'.

The source code is used to select the element. The source name is ignored. The code of the selected element is replaced by the target code, if it is provided; otherwise, the source code is not modified. The name of the selected element is replaced by the target code, if it is provided; otherwise, the source name is not modified.

Example

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

PILAR looks for an asset with code ‘mission’. The code does not change, but the name is translated into Spanish.

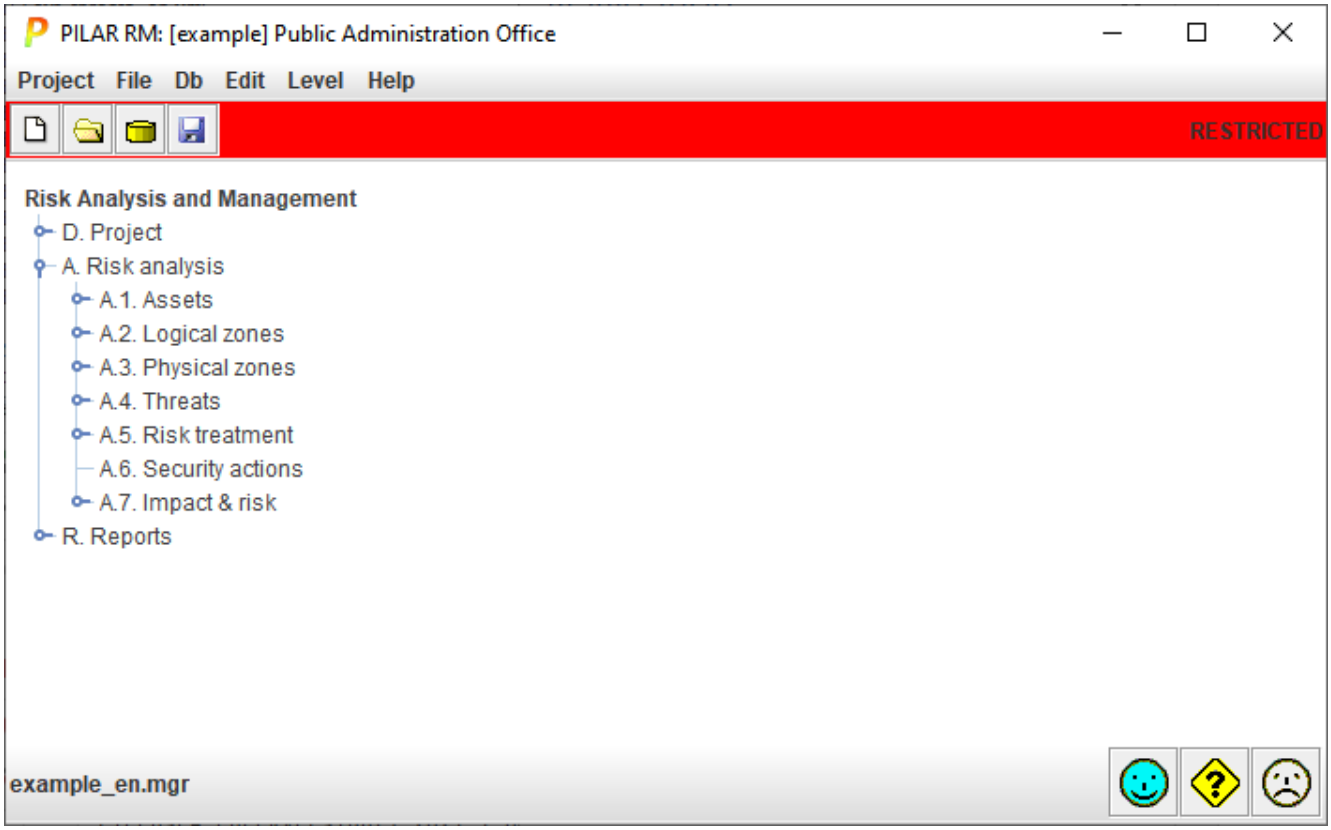
7.11.1 Alternative format: CSV

As an alternative option to text rules, you may use CSV (excel) format. You must specify “.csv” as the extension of the rules file.

The translation rules are organized in rows and columns:

A	B	C	D	E
element	src_code	src_name	trgt_code	trgt_name
asset	mission	System mission		Misión del sistema

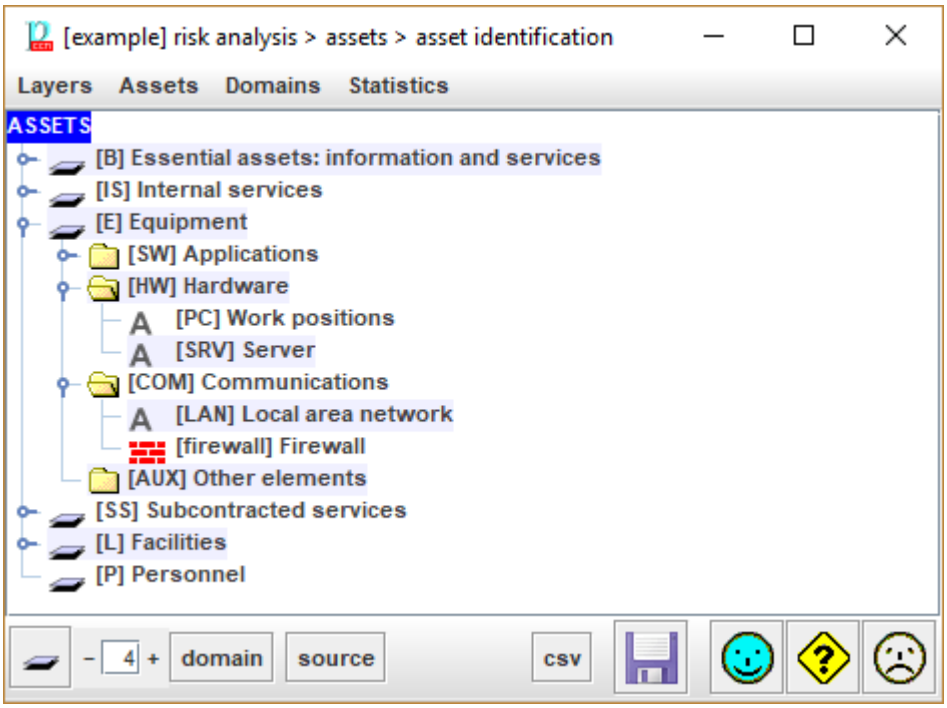
8 Risk analysis



8.1 Assets / Identification

Quick start
Go to **layers'** menu (above) and click **STANDARD LAYERS**. Select a layer or a group and right click on **NEW ASSET**. Click **OK** to finish asset identification.

This screen is used to capture the assets and their unique characteristics.



There are several kinds of information to input:

layers

Assets are organized in layers.

Layers have no impact on risk analysis: it is just a way of organizing assets for a better understanding and communication.

groups of assets

It is a convenient way or organising assets within a layer.

You may think of it as the organization of assets (files) into groups (directories).

Groups have no impact on risk analysis.

assets

At last, these are essential for risk analysis.

To move one layer, group or asset

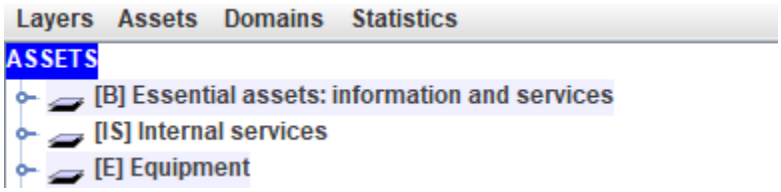
select with the mouse, then drag and drop onto the desired position

To move one or more assets, you may drag & drop, or select and then use arrows:

- SHIFT + UP_ARROW: to move up, before the previous one
- SHIFT + DOWN_ARROW: to move down, after the next one
- SHIFT + LEFT_ARROW: to move left, brother(s) of the current father
- SHIFT + RIGHT_ARROW: to move right, son(s) of the current elder brother

Double click to edit. See "*Edit one asset*".
Right click to operate on assets. See "*Asset operations*".

Top menus



- *Layers menu*
- *Assets menu*
- To edit security domains. See "*Security domains*".
- *Statistics menu*

Bottom toolbar

	Click to collapse assets tree.
	To select the level of expansion (tree depth).
domain	Click and select a security domain. PILAR will select the assets in that domain.
source	Click and select a source of information. PILAR will select the assets associated to that source.
csv	Export to a file using format CSV (comma-separated values).
	Saves current project either in a file, or in database (according to its source).

8.1.1 Layers menu

standard layers	Incorporate layers defined in the INFO file.
new layer	Creates a new layer.
edit layer	Edits an existing layer.
delete layer	Removes a layer.

To insert the standard layers (see info file)

- layers / standard layers

To insert a new layer

- menu layers / new layer

or

- select a layer
- right click + new layer

To edit a layer

- menu layers / edit layer

or

- select a layer
- right click + edit layer

To remove a layer

- menu layers / delete layer

or

- select a layer
- right click + delete layer

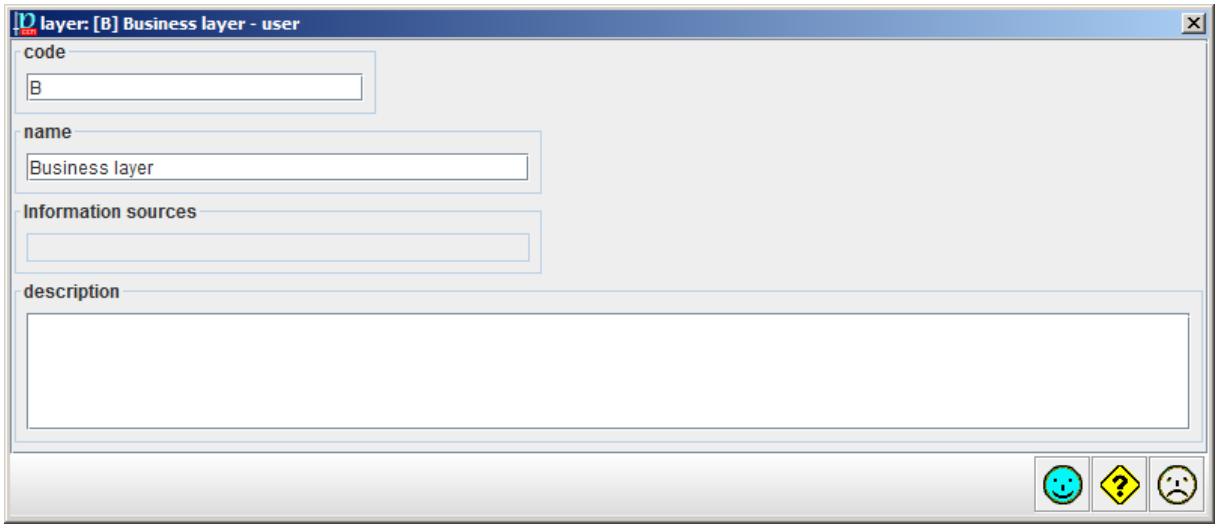
or

- select a layer
- click DEL

To move a layer to another position

- drag & drop with the mouse

You may edit layer data:



- The code must be unique.
- The name is a short, one-line, description.
- You may associate one or more information sources to the layer.

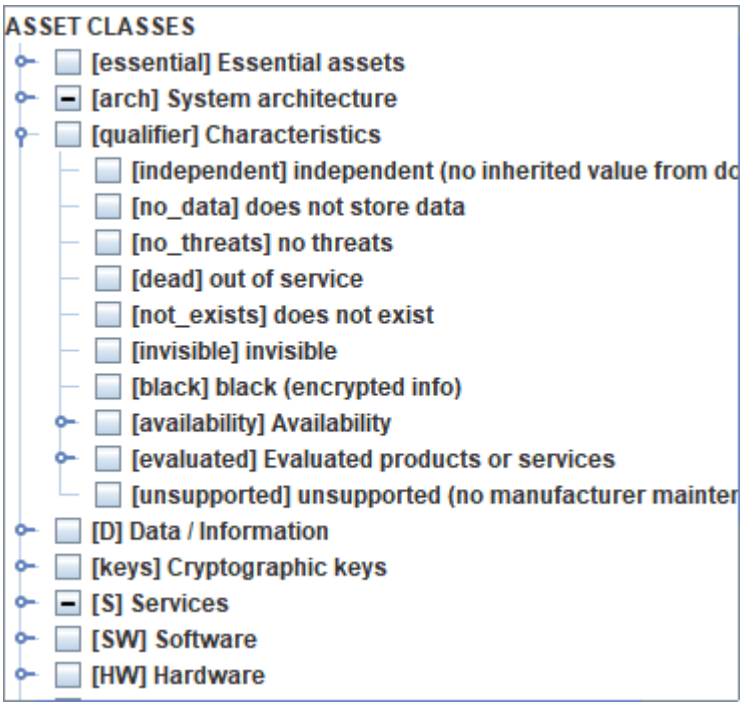
- The description may be larger and include external hyperlinks. To go to the linked page RIGHT-CLICK, then  .

8.1.2 Assets menu

new asset / new asset	Creates a new asset. See "*Edit one asset*".
new asset / new asset group	Creates a new asset group (a directory). See "*Edit one asset*".
new asset / duplicate asset	A new asset is created, using as initial contents that of another asset. You have to edit the new asset and, at least, change the code that must be unique. See "*Edit one asset*".
copy	Takes one or more assets to be duplicated later on.
cut	Extracts one or more assets from the tree, to be pasted later on.
paste	Pastes the assets that were cut into a new place in the tree.
edit	See "*Edit one asset*".
merge assets	Select two or more assets and merges them by adding asset classes. You have to edit the new asset and, at least, change the code that must be unique. See "*Edit one asset*".
description	Jumps directly to the long description for the selected asset.
security domain	Changes the selected assets into a security domain.
information sources	Assigns one or more information sources to the selected assets.
sort / [a..z] …	The selected assets are sorted alphabetically, by code.
sort / … [A..Z]	The selected assets are sorted alphabetically, by name.
sort / undo	Undoes the last sorting operation; that is, return to the original order.
asset / group / be group!	Changes the selected assets from plain assets into asset groups.
asset / group / don't be group!	Changes the selected assets from asset groups into plain assets.
delete / delete children	Removes the children of the selected assets.

delete **/ delete asset**	Removes the selected assets, and their children.

Previous versions included some asset qualifiers. These qualifiers are moved onto asset classes



independent	the asset does not inherit values from the essential assets in the domain
no_data	the asset does not store data (some threats are not applicable)
no_threats	You may mark an asset as threat-free, or subject to threats.
dead	the asset is out of service. You may stop / restart an asset. It only affects availability.
not_exists	You may enable / disable an asset. If it does not exist, it is ignored for the risk analysis.
invisible	You may hide an asset from presentation screens.
black	data in this asset is encrypted (some threats do not apply)
availability	tunes the impact on availability
evaluated	the product or services is evaluated or has a security accreditation
unsupported	the manufacturer no longer provides security patches

To insert a new asset

- select one layer | one asset
- menu assets / new asset / new asset

or

- select one layer

- right click / new asset

or

- select one asset
- right click / new asset / new asset

To insert a new group of assets

- select one layer | one asset
- menu assets / new asset / new asset group

or

- select one layer
- right click / new asset group

or

- select one asset
- right click / new asset / new asset group

To insert an asset that duplicates another one

- select one asset
- menu assets / new asset / duplicate asset

or

- select one asset
- right click / new asset / duplicate asset

To edit an asset

- select one asset
- menu assets / edit

or

- select one asset
- right click / edit

To add a long description to an asset

- select one asset
- menu assets / description

or

- select one asset
- right click / description

or while editing the asset

To place an asset into a security domain

- select one asset
- menu assets / domain / select / OK

or

- select one asset
- right click / domain / select / OK

or while editing the asset

To associate one asset to sources of information

- select one asset
- menu assets / information sources / select / OK

or

- select one asset
- right click / information sources / select / OK

or while editing the asset

To transform a plain asset into a group

- select one asset
- menu assets / asset-group / be group

or

- select one asset
- right click / asset-group / be group

To transform a group of assets into a plain asset

- select one asset
- menu assets / asset-group / do not be group

or

- select one asset
- right click / asset-group / do not be group

To remove one asset (and the member of the group if any)

- select one asset
- menu assets / delete / delete asset

or

- select one asset
- right click / delete / delete asset

or

- select one asset
- click DEL

To remove the members of a group

- select one asset
- menu assets / delete / delete children

or

- select one asset
- right click / delete / delete children

To move one asset to another place in the tree

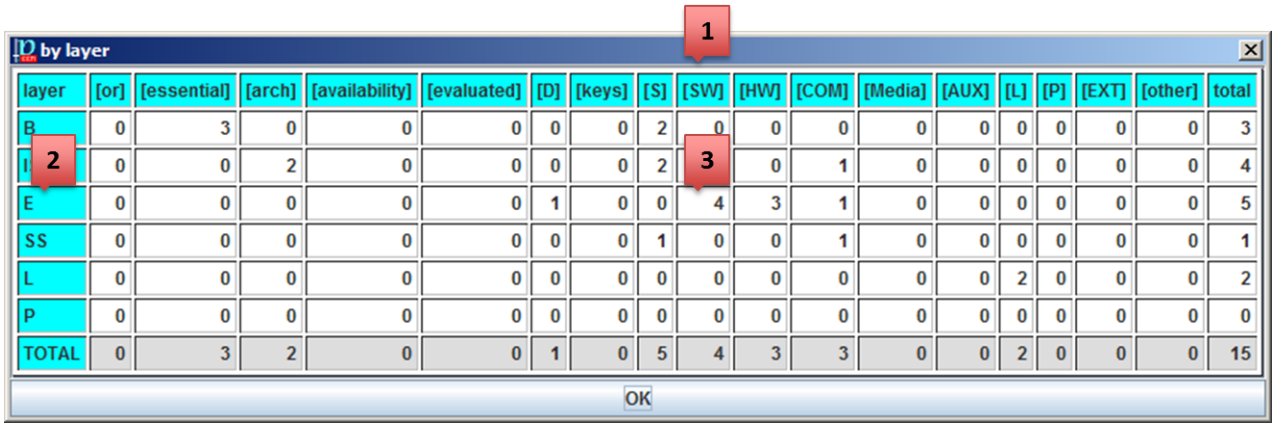
- drag & drop
- cut & paste

or

- SHIFT + UP_ARROW: to move up, before the previous one
- SHIFT + DOWN_ARROW: to move down, after the next one
- SHIFT + LEFT_ARROW: to move left, brother(s) of the current father
- SHIFT + RIGHT_ARROW: to move right, son(s) of the current elder brother

8.1.3 Statistics menu

PILAR presents a summary of assets, counting asset classes (the number of assets with a mark in each class). The counts may be aggregated by layers, by security domains, or by information sources. The outcome is like the following one:



layer	[or]	[essential]	[arch]	[availability]	[evaluated]	[D]	[keys]	[S]	[SW]	[HW]	[COM]	[Media]	[AUX]	[L]	[P]	[EXT]	[other]	total
B	0	3	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	3
I	0	0	2	0	0	0	0	2	0	0	1	0	0	0	0	0	0	4
E	0	0	0	0	0	1	0	0	4	3	1	0	0	0	0	0	0	5
SS	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1
L	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	2
P	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TOTAL	0	3	2	0	0	1	0	5	4	3	3	0	0	2	0	0	0	15

Each column refers to a major class of assets. For instance, [1] marks [SW]. In column [1] there are 3 assets with classes of this column, all of them in layer [E].

Each row refers to a layer (or domain, or source). For instance, [2] marks [E]. In row [2], 1 asset has a mark in class [availability], 2 assets in [D], 3 assets in [D], and so on. Altogether, there are 5 assets in this layer.

The totals may not match the addition of the cells since one asset may mark several classes.

Table may be printed: right click.

8.1.4 Asset operations

On the tree

— double click opens an asset to edit. See "*Edit one asset*".
— right click opens a menu. The options are similar to those in the top toolbar but notice that now actions affect to only one element.

To move one asset to another place in the tree

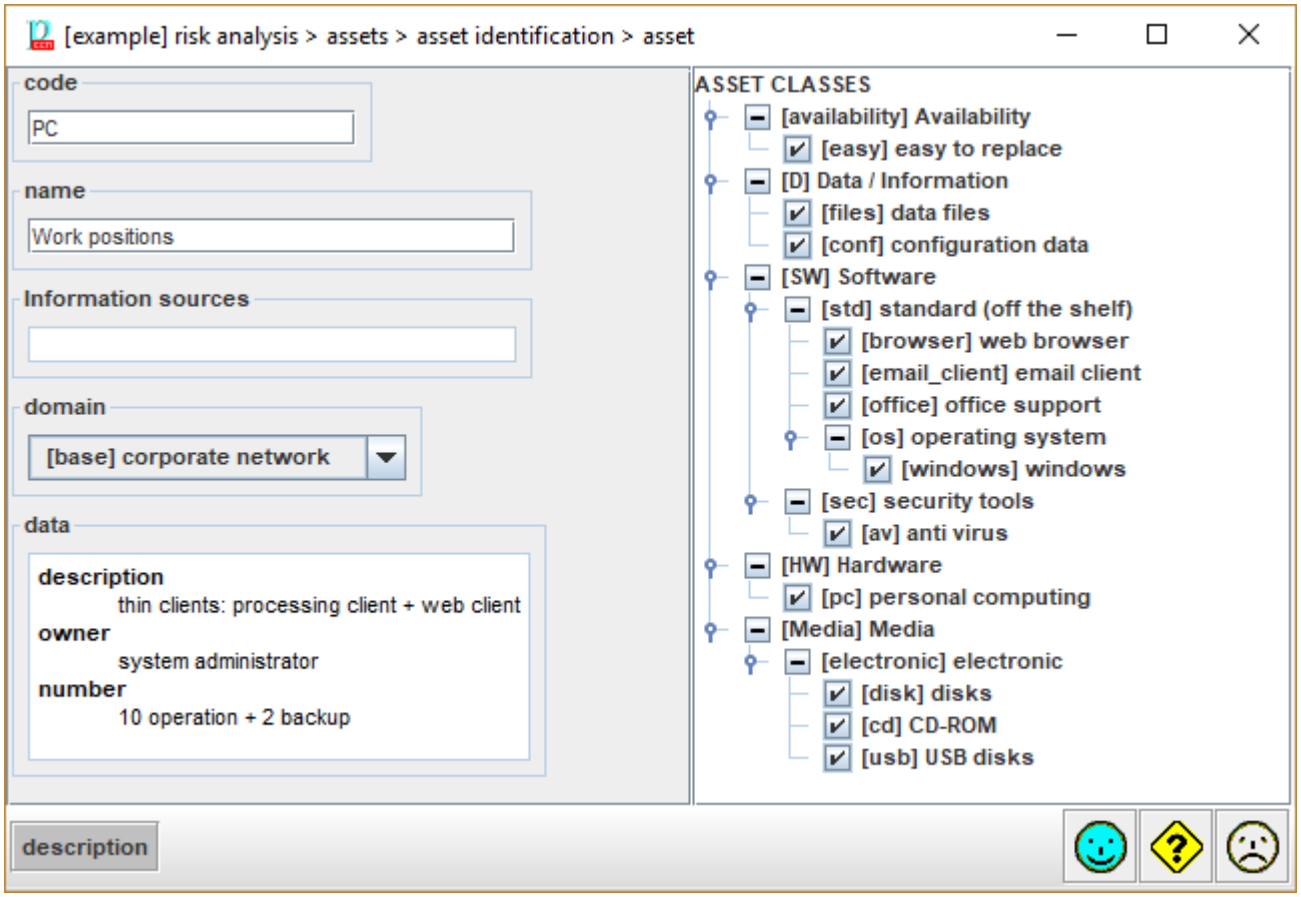
- drag & drop
- cut & paste

or use arrows to move the selected assets

- SHIFT + UP_ARROW: to move up, before the previous one
- SHIFT + DOWN_ARROW: to move down, after the next one
- SHIFT + LEFT_ARROW: to move left, brother(s) of the current father
- SHIFT + RIGHT_ARROW: to move right, son(s) of the current elder brother

8.2 Assets / Edit one asset

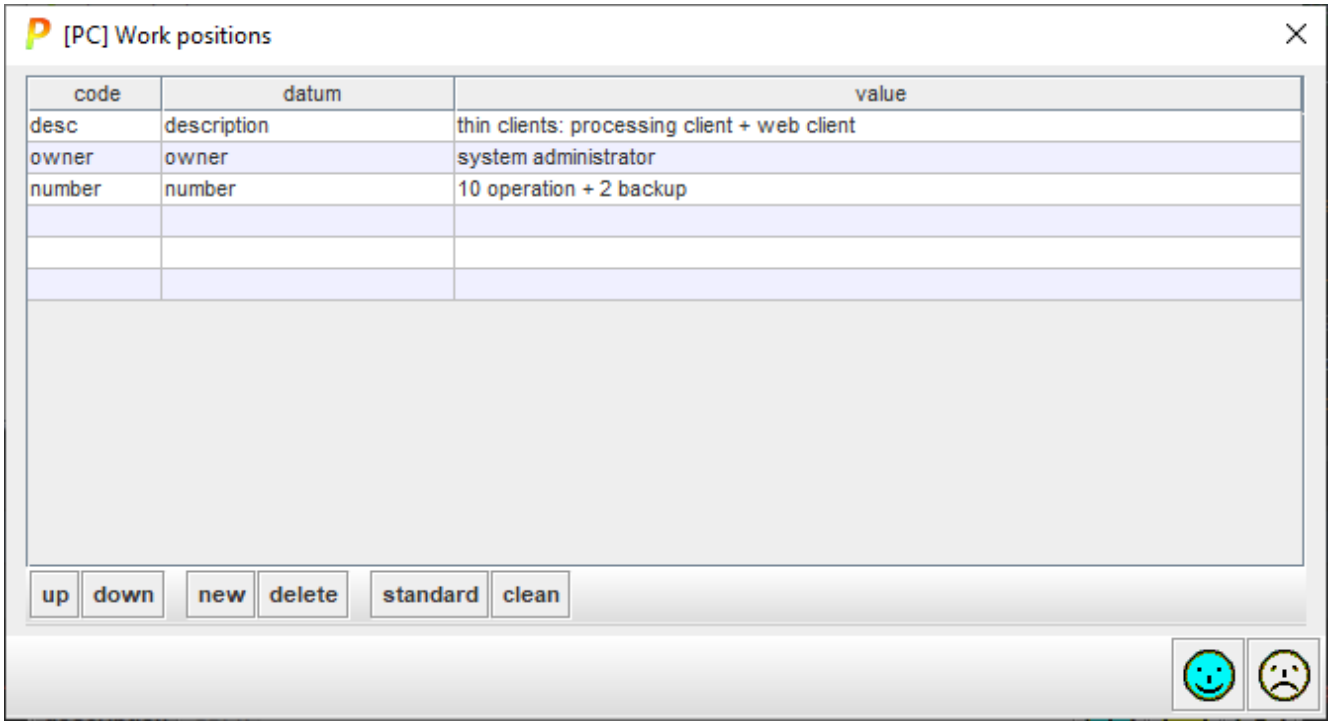
Quick start
Select a **unique code** and a descriptive name. Check on one or more classes on the right panel. Click **STANDARD** and add some descriptive information. Click **OK** to continue.



code	which shall be unique.
name	A short description: one line.
sources	Click to associate the asset to zero or more information sources.
domain	Select the security domain to which the asset belongs.
description	A longer description. The description may include hyperlinks (URLs). To go to the linked page RIGHT-CLICK, then

Data: Key-value pairs

Key-value pairs to describe the asset. It is just for administrative purposes.
On double click, an editing window opens



- Click on the code column to edit a code. The code is useful for translations.
- Click on the datum column to edit a name
- Click on the value column to edit a value.

Operations on the key-value pairs:

- up – moves the selected row upwards
- down – moves the selected row downwards
- new – adds one more row
- delete – removes the selected row
- standard – adds standard keys, considering the classes marked
  See info file.
- clean – removes the rows that have no contents in the value field

8.2.1 Asset classes

You may qualify the asset with zero or more classes. Classes are used to select threats and safeguards.

- ☐ means that the class is not selected for this asset
- ☑ means that the class is selected for this asset
- ▪ means that a subclass is selected for this asset

Since there are many classes, you may double-click on tree entries to collapse the subtree. Collapsing means that only selected classes are displayed.

Class clean / delete

You may right-click on the asset classes' tree to clean or to delete marks. Cleaning means removing redundant marks; while deleting means removing marks.

Example

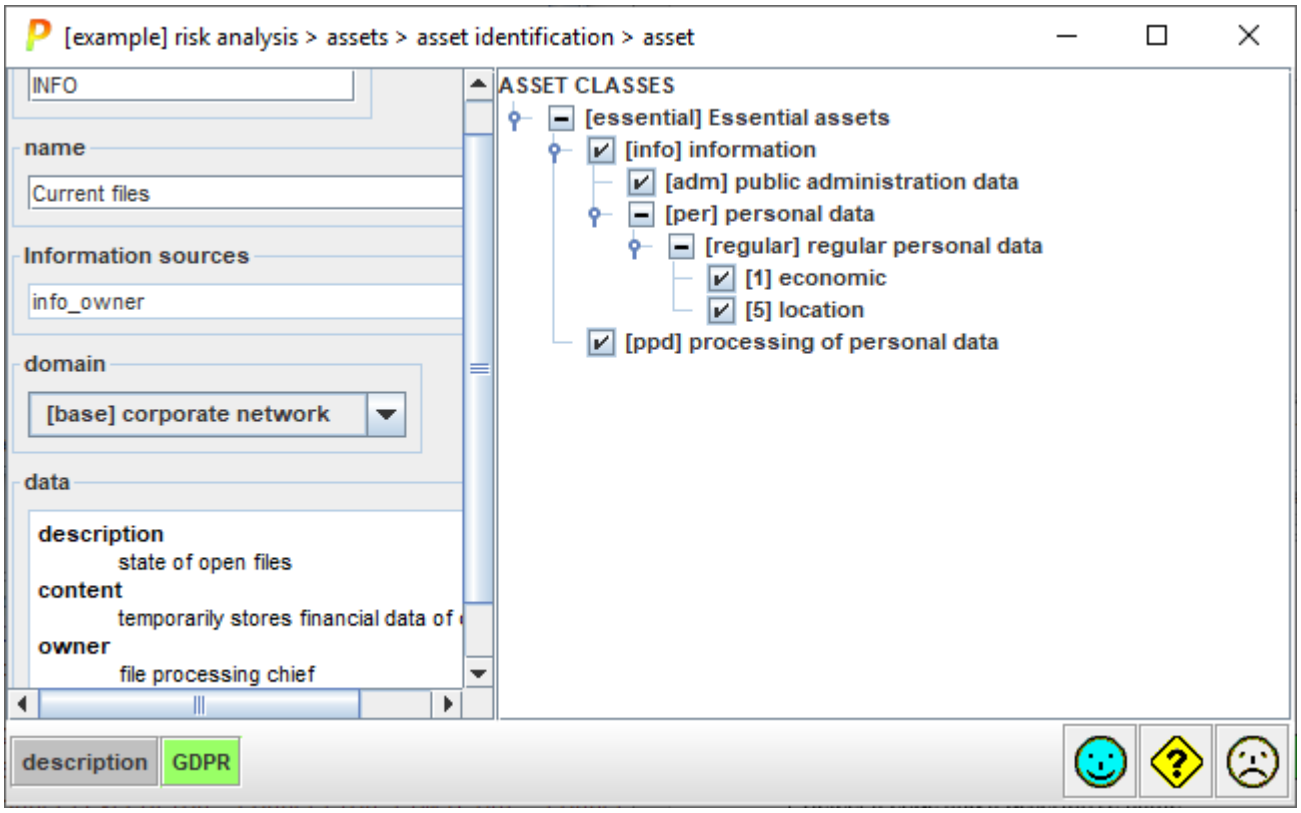
right click + CLEAN	**right click + DELETE**
[keys] Cryptographic keys [info] protecting information [encrypt] encrypting & decrypting keys [shared_secret] shared secret (symmetric key) [public_encryption] public encrypting keys [public_decryption] private decrypting keys [sign] digital signature keys [public_signature] private signing keys [public_verification] public signature verification keys [shared_secret] shared secret (symmetric key) [com] protecting communications [disk] media encryption [encrypt] encrypting & decrypting keys [x509] public key certificates	[keys] Cryptographic keys [info] protecting information [encrypt] encrypting & decrypting keys [shared_secret] shared secret (symmetric key) [public_encryption] public encrypting keys [public_decryption] private decrypting keys [sign] digital signature keys [public_signature] private signing keys [public_verification] public signature verification keys [shared_secret] shared secret (symmetric key) [com] protecting communications [disk] media encryption [encrypt] encrypting & decrypting keys [x509] public key certificates

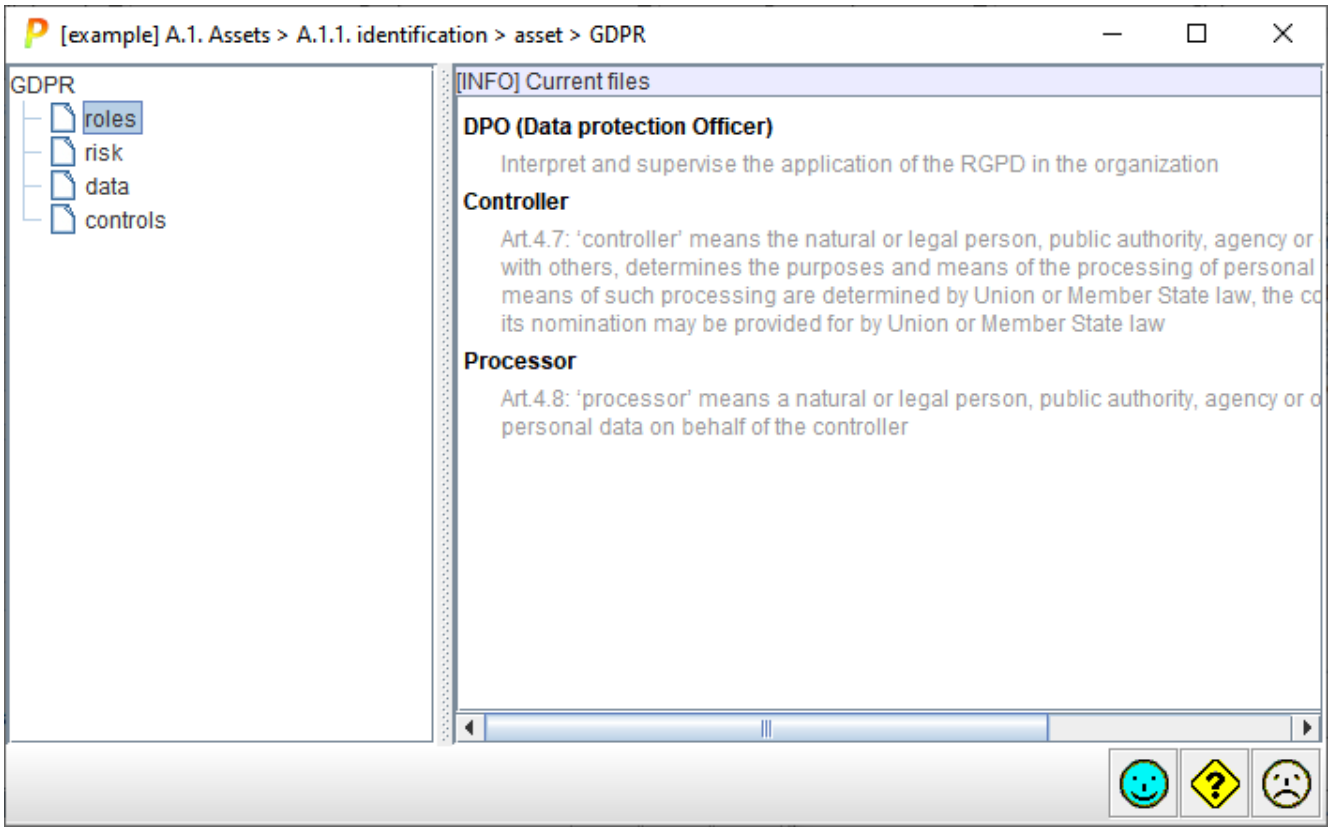
8.2.2 GDPR: privacy

For assets that encompass personal data, you may specify more administrative information.

This information may be provided system-wide (see *Project data*) or per asset.

It is self-explanatory:





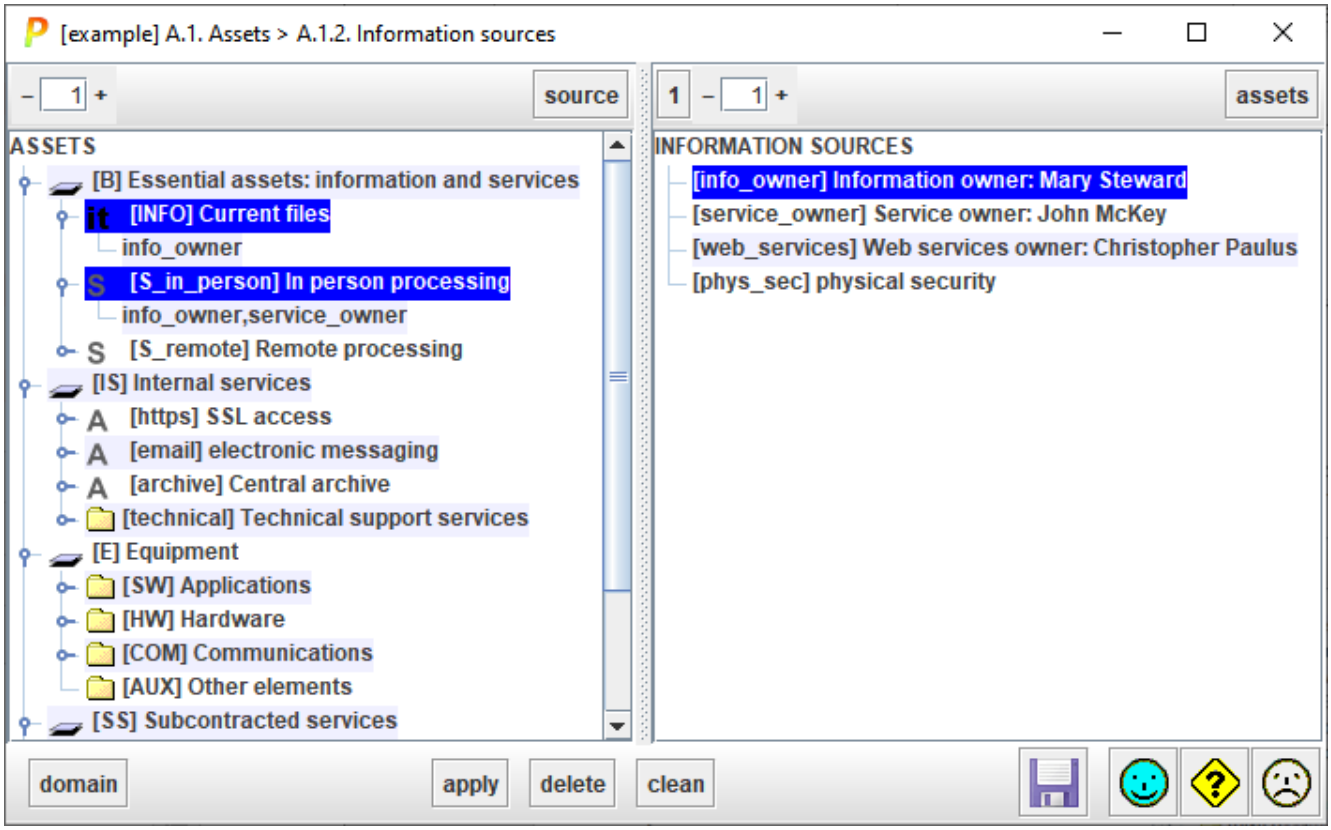
This information goes directly onto reports.

8.3 Assets / Sources

To manage the association of assets to information sources.

The left panel show the asset tree. The right panel, the information sources.

TBD



Top left

– 3 +	Controls the level of expansion of the left tree (assets).
SOURCE	Select one or more assets on the left. Click SOURCE, and PILAR will select the associated information sources on the right.

Top right

– 3 +	Controls the level of expansion of the right tree (information sources).
ASSETS	Select one or more information sources on the right. Click ASSETS, and PILAR will select the associated assets on the left tree.

Bottom

DOMAIN	Select assets in left panel that belong to the given domain
APPLY	Select one or more assets on the left. Select one or more sources on the right. Click APPLY to associate.
DELETE	Select one or more assets on the left. Select one or more sources on the right. Click DELETE to dissociate.
CLEAN	Select one or more assets on the left. Click CLEAN to dissociate from sources.

To associate a source to an asset

- select one or more assets (left panel)
- select one or more information sources (right panel)
- click APPLY

To remove an association

- select one or more assets (left panel)
- select one or more sources (right panel)
- click DELETE

or click DELETE key

To discover the sources associated to an asset

- select the asset (left panel)
- click SOURCE (left panel, top)

To discover the assets associated to a source

- select the source (right panel)
- click ASSETS (right panel, top)

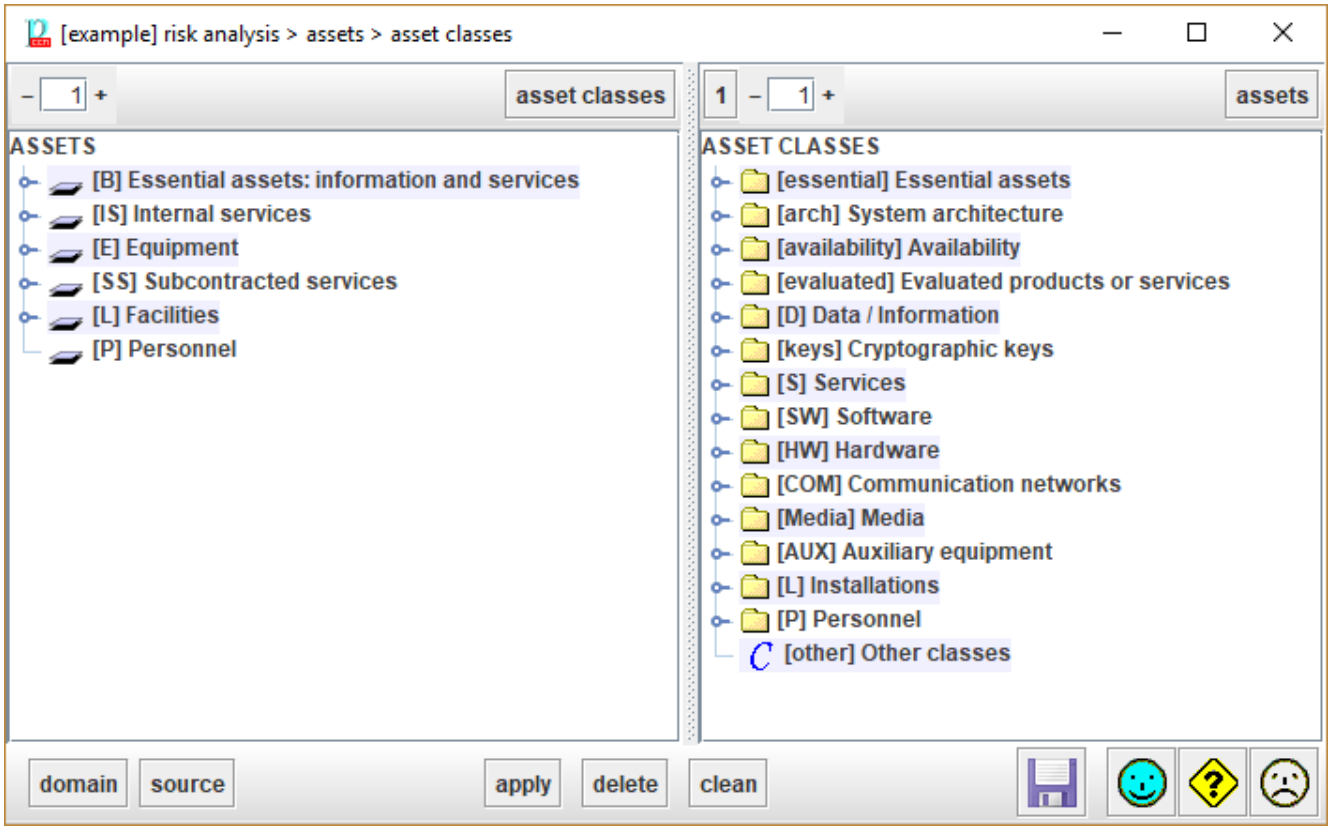
To copy the associations of one asset to another

- select the source asset (left panel)
- click SOURCES (left panel, top)
- select the target asset (left panel)
- click APPLY

8.4 Assets / Classes

To associate classes to assets.

The left tree, organised by asset, shows the codes of the asset classes that are associated to each asset.



Top left

– 3 +	Controls the level of expansion of the left tree (assets).
ASSET CLASSES	Select one or more assets on the left. Click ASSET CLASSES, and PILAR will select the associated classes on the right tree.

Top right

– 3 +	Controls the level of expansion of the right tree (asset classes).
ASSETS	Select one or more asset classes on the right. Click ASSETS, and PILAR will select the associated assets on the left tree.

Bottom

domain	Select assets in left panel that belong to the given domain
source	Select assets in left panel associated to the selected source
apply	Select one or more assets on the left. Select one or more classes on the right. Click APPLY to associate.
delete	Select one or more assets on the left. Select one or more classes on the right. Click DELETE to dissociate.
clean	Select one or more assets on the left. Click CLEAN to dissociate from classes.

To associate a class to an asset

- select one or more assets (left panel)
- select one or more classes (right panel)
- click APPLY

To remove a class association

- select one or more assets (left panel)
- select one or more classes (right panel)
- click DELETE

or click DELETE key

To discover the classes associated to an asset

- select the asset (left panel)
- click ASSET CLASSES (left panel, top)

To discover the assets associated to a class

- select the class (right panel)
- click ASSETS (right panel, top)

To copy the associations of one asset to another

- select the source asset (left panel)
- click ASSET CLASSES (left panel, top)
- select the target asset (left panel)
- click APPLY

8.5 Assets / CPE names

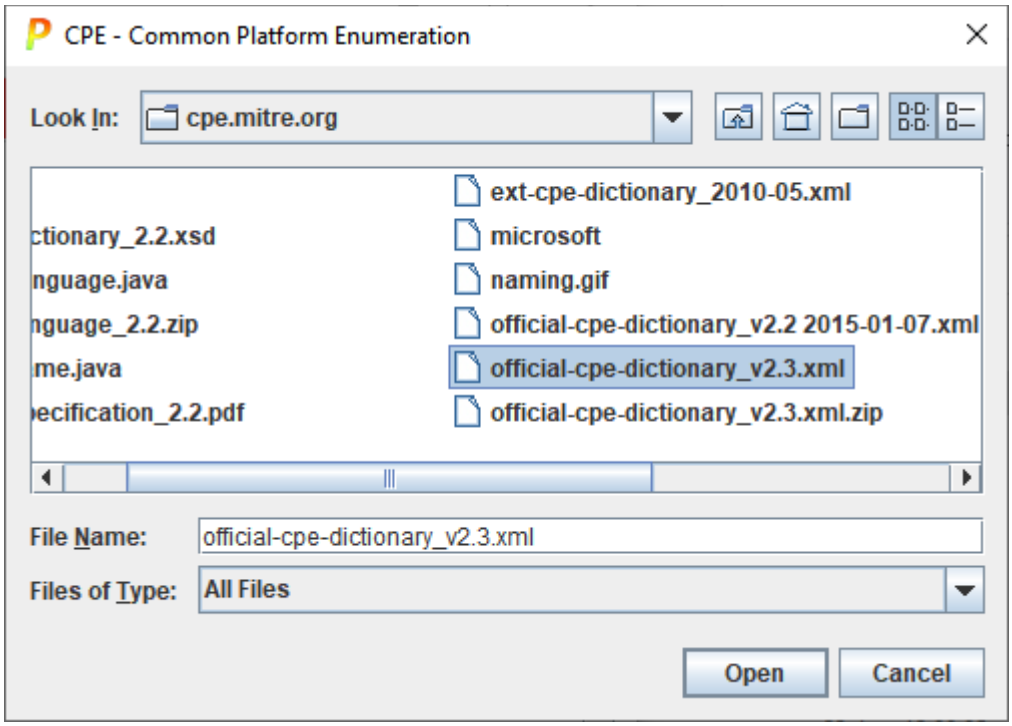
Assets may be associated to one or more CPE names. This information may be used to find reported vulnerabilities.

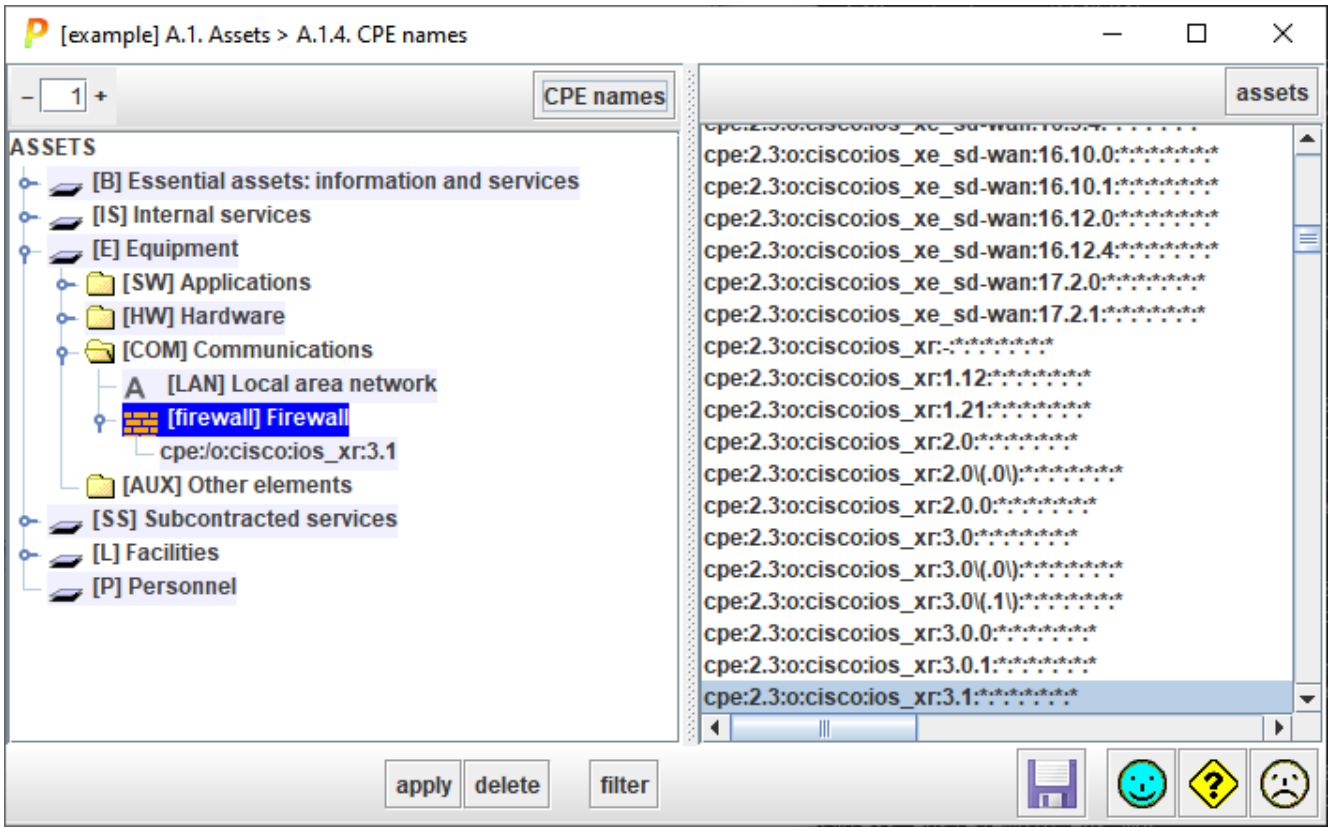
See https://www.ar-tools.com/doc/

The CPE dictionary of names is constantly evolving. Download an updated version from here:

https://nvd.nist.gov/download.cfm

NIST distributes the dictionary in version 2.2 and 2.3. PILAR reads both but prefers 2.3 if available.





Top left

3	Controls the level of expansion of the left tree (assets).
CPE NAMES	Select one or more assets on the left. Click CPE NAMES, and PILAR will select the associated CPE names on the right tree.

Top right

3	Controls the level of expansion of the right tree (CPE names).
ASSETS	Select one or more CPE names on the right. Click ASSETS, and PILAR will select the associated assets on the left tree.

Bottom

APPLY	Select one or more assets on the left. Select one or more CPE names on the right. Click APPLY to associate.
DELETE	Select one or more assets on the left. Select one or more CPE names on the right. Click DELETE to dissociate.
FILTER	Reduces right panel list filtering by manufacturer.

To associate a name to an asset

- select one or more assets on the left panel
- select one or more names on the right panel
- click APPLY

To dissociate a name from an asset

- select the name to remove
- click DELETE

To select the names associated to an asset

- select one or more assets on the left panel
- click CPE names

To select the assets associated to a name

- select one or more names on the right panel
- click ASSETS

To search for an asset or a CPE name

- ctrl-F on the appropriate panel

8.6 Assets / Dependencies

Dependencies may be established between assets. Dependencies are used to propagate value (that is, security requirements) from valuable assets ‘above’ onto equipment assets ‘below’.

You may rate the system by domains or asset by asset. You select in *Options / Valuation*

If you are valuating by domains, you may skip dependencies, and jump directly into *Valuation by domains*

If you are valuating asset by asset, you have to establish the dependencies, and then jump into *Valuation by assets*

Quick start

If you have identified facilities (installations) …

- associate each equipment to the facility where it is located

If you have identified services and equipment …

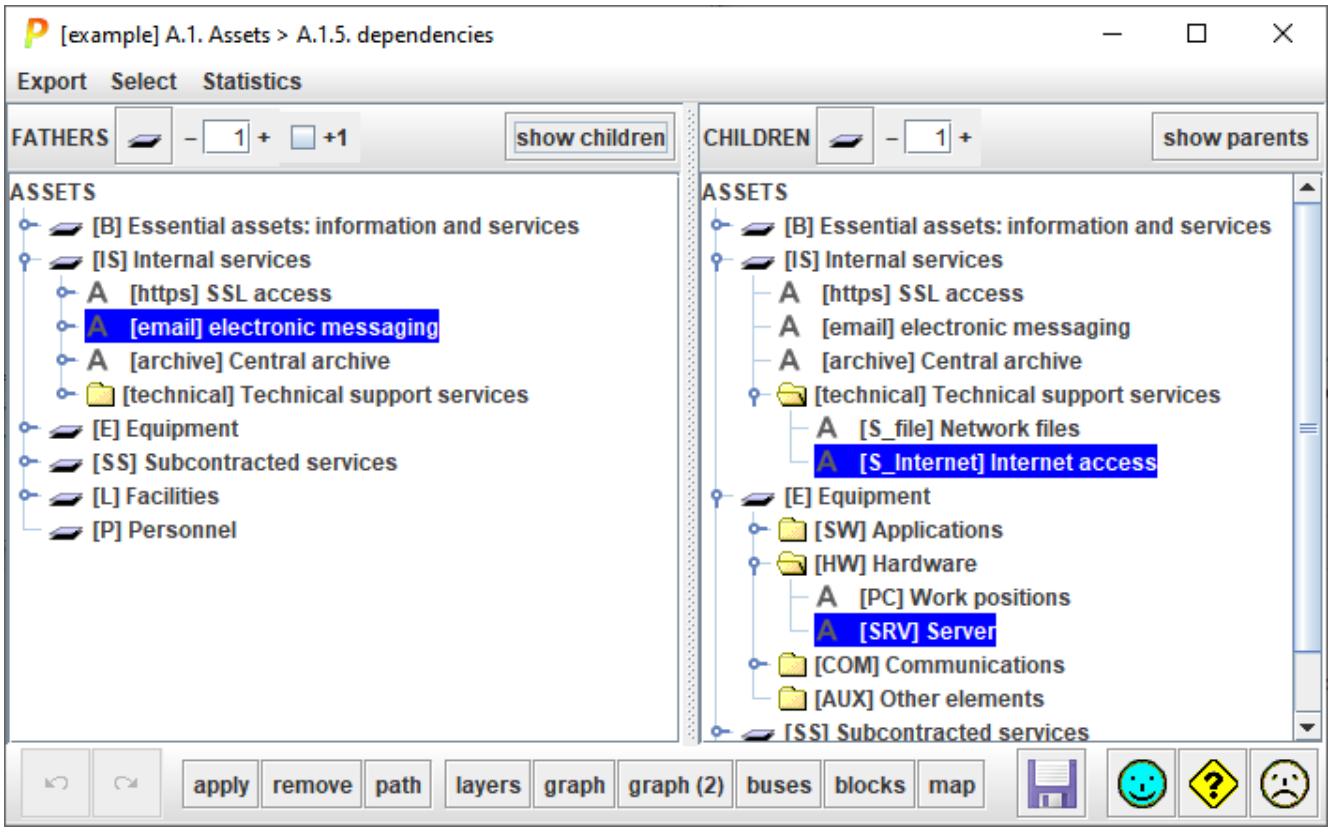
- associate each service to the equipment it uses: software, hardware, communications, media, …

If you have identified people …

- associate each person to the services or equipment they may cause harm (either accidentally or deliberately)

Repeat until every asset under the business layer is used for something.

This screen is used to establish the dependencies between assets. The left panel shows the "father" assets (the asset above in the dependency graph), while the right panel shows the "children" assets (the assets below in the dependency graph).



Top menu EXPORT

… to XML	eXtensible Markup Language
… to GraphML	export data to GraphML format
… to CSV	Comma Separated Values; export for excel

Top menu SELECT

no father	selects assets without dependencies above
no son	selects assets without dependencies below
dependency loops	selects assets trapped in a loop (I depend on you, you depend on … me)

Top menu STATISTICS

dependencies	summary table

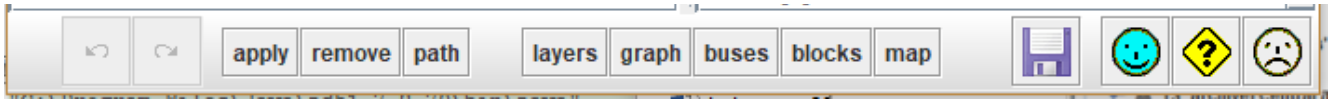
Top left toolbar FATHERS

	Click to collapse left assets tree.
	Control the level of expansion of the left tree. If [+1] is selected, the descendent asset is shown as well.
[+1]	Controls whether assets (left) tree includes descendants or only assets
SHOW CHILDREN	Select an asset on the left panel. Click SHOW CHILDREN for PILAR to select the direct descendants, and mark the indirect descendants, on the right tree.

Top right toolbar CHILDREN

	Click to collapse right assets tree.
	Control the level of expansion of the right tree.
SHOW PARENTS	Select an asset on the right panel. Click SHOW PARENTS for PILAR to select the direct ascendants, and mark the indirect ascendants, on the left tree.

Bottom toolbar



	undo. The last APPLY or REMOVE done
	redo. The last APPLY or REMOVE undone.
APPLY	Select one or more assets on the left. Select one or more assets on the right. Click APPLY to make each asset on the left depend on every asset on the right.
REMOVE	Select one or more assets on the left. Select one or more assets on the right. Click REMOVE to make each asset on the left independent from every asset on the right. Or select a dependency on the left and click REMOVE to remove it.
PATH	Select one asset on the left, and one asset on the right. Click PATH to open a window with the route(s) from the left asset (green) down to the right asset (red).
LAYERS	Opens a new window with as many boxes as layers, showing dependencies. See "*Assets / Dependencies / Layers*".
GRAPH (1)	Opens a new window with as many boxes as assets, showing dependencies. See "*Assets / Dependencies / Graph*".
GRAPH (2)	As GRAPH, but uses an alternative algorithm for default placing of boxes. See "*Assets / Dependencies / Graph*".
BUSES	Opens a new window with as many boxes as assets, showing dependencies. See "*Assets / Dependencies / Buses*".
BLOCKS	Opens a new window with as many boxes as assets, showing dependencies. See "*Assets / Dependencies / Blocks*".
MAP	Opens a new window with as many boxes as assets, showing dependencies. See "*Assets / Dependencies / Map*".

Several screens present a LIVE checkbox on top. If selected, the diagram follows the assets selected on the main screen. Otherwise, the diagram has to be updated manually.

To establish a dependency

- select F in the left panel (one or more assets)
- select S in the right panel (one or more assets)
- click on APPLY

If F or S, or both of then, are groups, the dependency will be established between the corresponding sons. So, when a group depends on another group, every asset from the father group depends on each asset of the son group.

To remove a dependency

- select F in the left panel (one or more assets)
- select S in the right panel (one or more assets)
- click on REMOVE

or

- select S in the left panel (one or more assets)
- click on REMOVE

To find out the sons of F

- select F in the left panel (one or more assets)
- click on SONS

To find out the fathers of S

- select S in the right panel (one or more assets)
- click on FATHERS

To set a degree of dependency

By default, dependencies are 100% on every dimension.

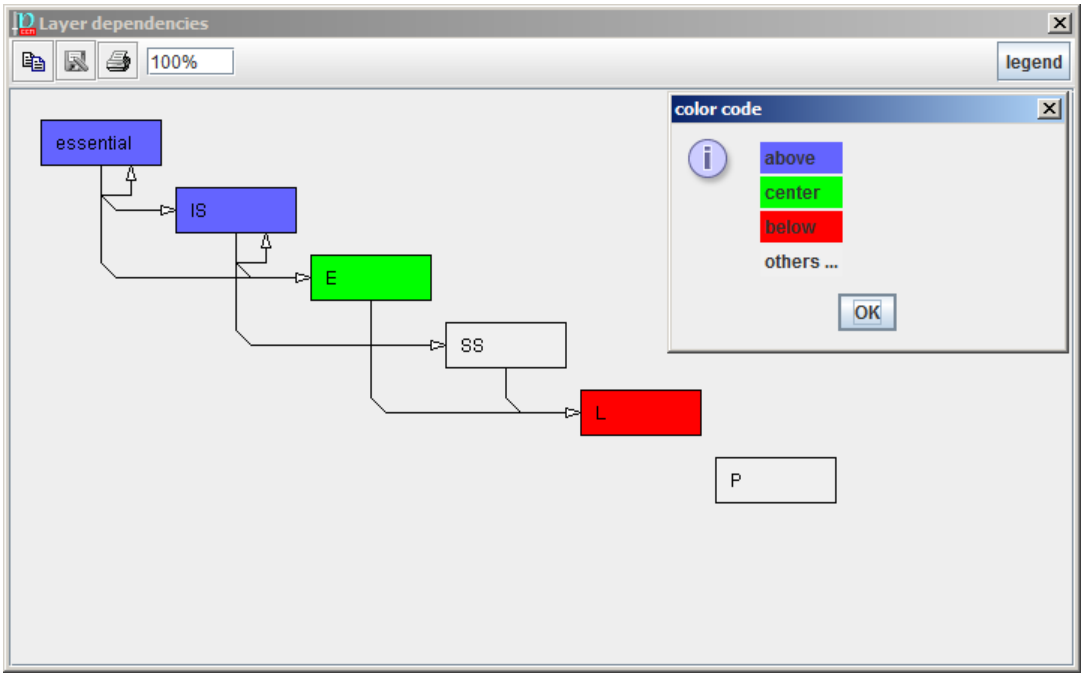
To set a degree between 0% and 100%:

- expand dependencies under an asset
- select the son asset
- click on the right button of the mouse *Dependencies per dimension of security*

To discover the dependency route from one asset to another

- select the father on the left panel
- select the son on the right panel
- click on PATH

8.6.1 Dependencies – Layers



The graph shows the relationships between layers. A layer L1 depends on a layer L2 if there is at least one asset in L1 that depends on at least one asset in L2.

If the model is "clean"

- layers above only depend on layers below
- layers below only depend on layer above
- there may be internal dependencies within layers

That is not mandatory; but projects that do not adhere to the rule are harder to understand and to explain.

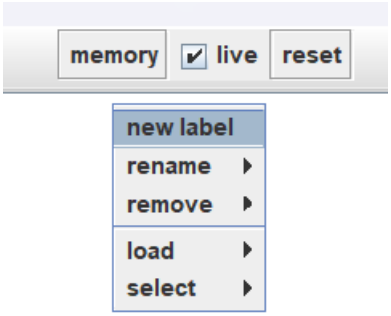
When you click on one layer, the graph gets colour:

deep blue	directly related layers above
green	the reference layer
bright red	directly related layers below
grey	unrelated

	**copy**	Copies the image to the note pad to paste it somewhere else.
	**save**	to store the picture as an image file. The available image formats depend on the hosting machine; some formats are quite widespread: jpg, jpeg, png
	**print**	to send the picture to a printer

100%	**scale**	to enlarge / decrease the image
	legend	show the colour codes

Estas gráficas presentan un botón MEMORIA que permite memorizar diagramas bajo un nombre



new label	Defines a new label with a name
rename	Renames the label
remove	Removel the label
load	The current diagram is recorded for the label
select	Recovers the diagram loaded onto the label

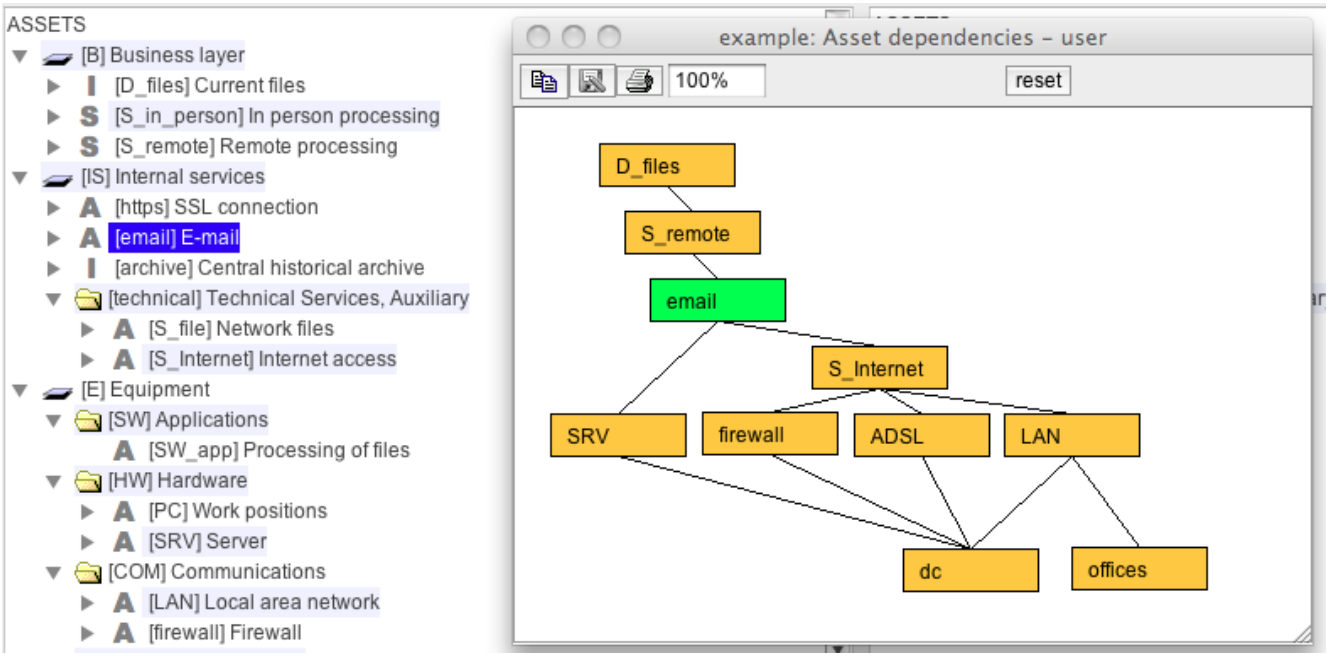
8.6.2 Dependencies – Graph

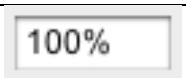
The graph shows the relationships between assets. It only presents the assets related to those selected on the main screen, or all the assets if nothing is selected.

Assets are heuristically positioned so that there is no relation going upwards: all dependencies go from top to bottom. However, if the picture is unpleasant, the user may reposition assets as desired (drag and drop on boxes).

Currently PILAR includes two automatic positioning algorithms (cleverly named (1) and (2)). The only difference is in the automatic positioning of the assets.

The graph tracks the selection on the main dependencies screen. So, if you select an asset, a group or a layer, only the assets in the group and those direct or indirectly linked will appear in the picture.



	**copy**	Copies the image to the note pad to paste it somewhere else.
	**save**	to store the picture as an image file. The available image formats depend on the hosting machine; some formats are quite widespread: jpg, jpeg, png
	**print**	to send the picture to a printer
	**scale**	to enlarge / decrease the image
	reset	repositions boxes to initial places (heuristic)

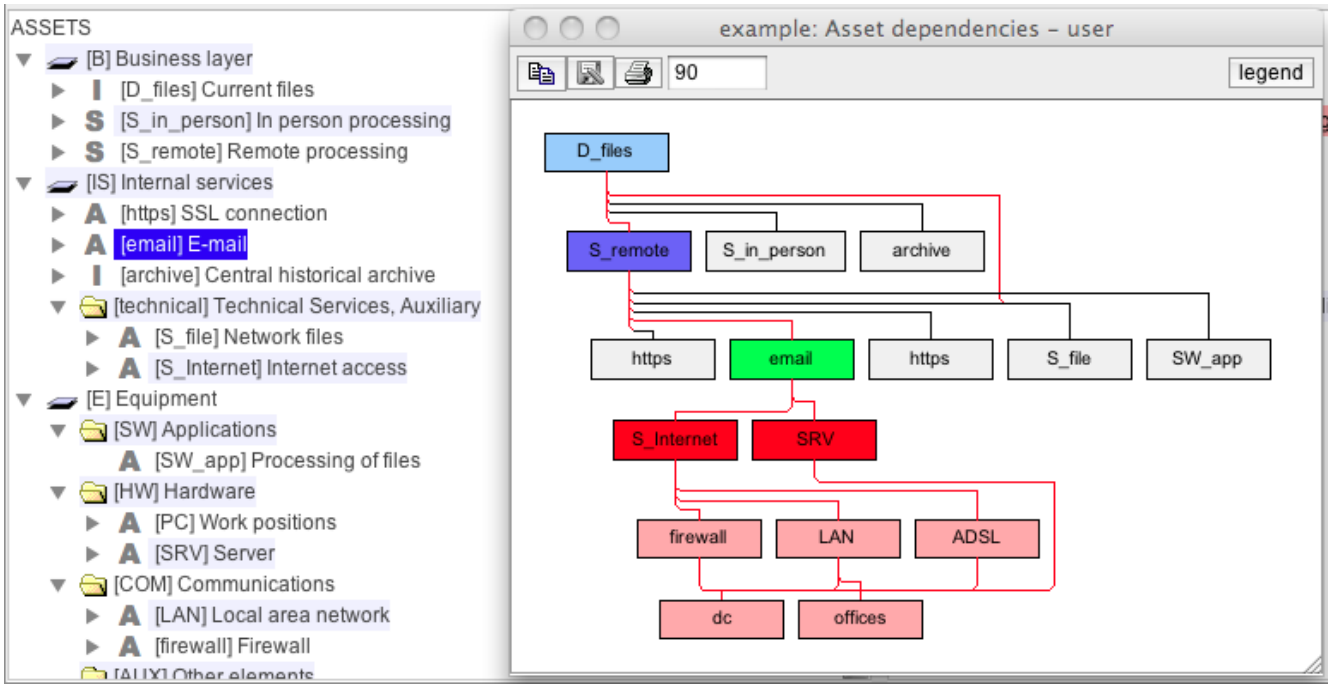
8.6.3 Dependencies – Buses

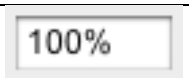
The graph shows the relationships between assets. It only presents the assets related to those selected on the main screen, or all the assets if nothing is selected.

Assets are heuristically positioned so that there is no relation going upwards: all dependencies go from top to bottom. PILAR create connection buses to connect one row to the next, and jump over rows.

The graph tracks the selection on the main dependencies screen. So, if you select an asset, a group or a layer, only the assets in the group and those direct or indirectly linked will appear in the picture.

Furthermore, within the assets shown, if you select one, it becomes green, those above turn red, and those below turn blue.



	**copy**	Copies the image to the note pad to paste it somewhere else.
	**save**	to store the picture as an image file. The available image formats depend on the hosting machine; some formats are quite widespread: jpg, jpeg, png
	**print**	to send the picture to a printer
	**scale**	to enlarge / decrease the image
	legend	show the colour codes

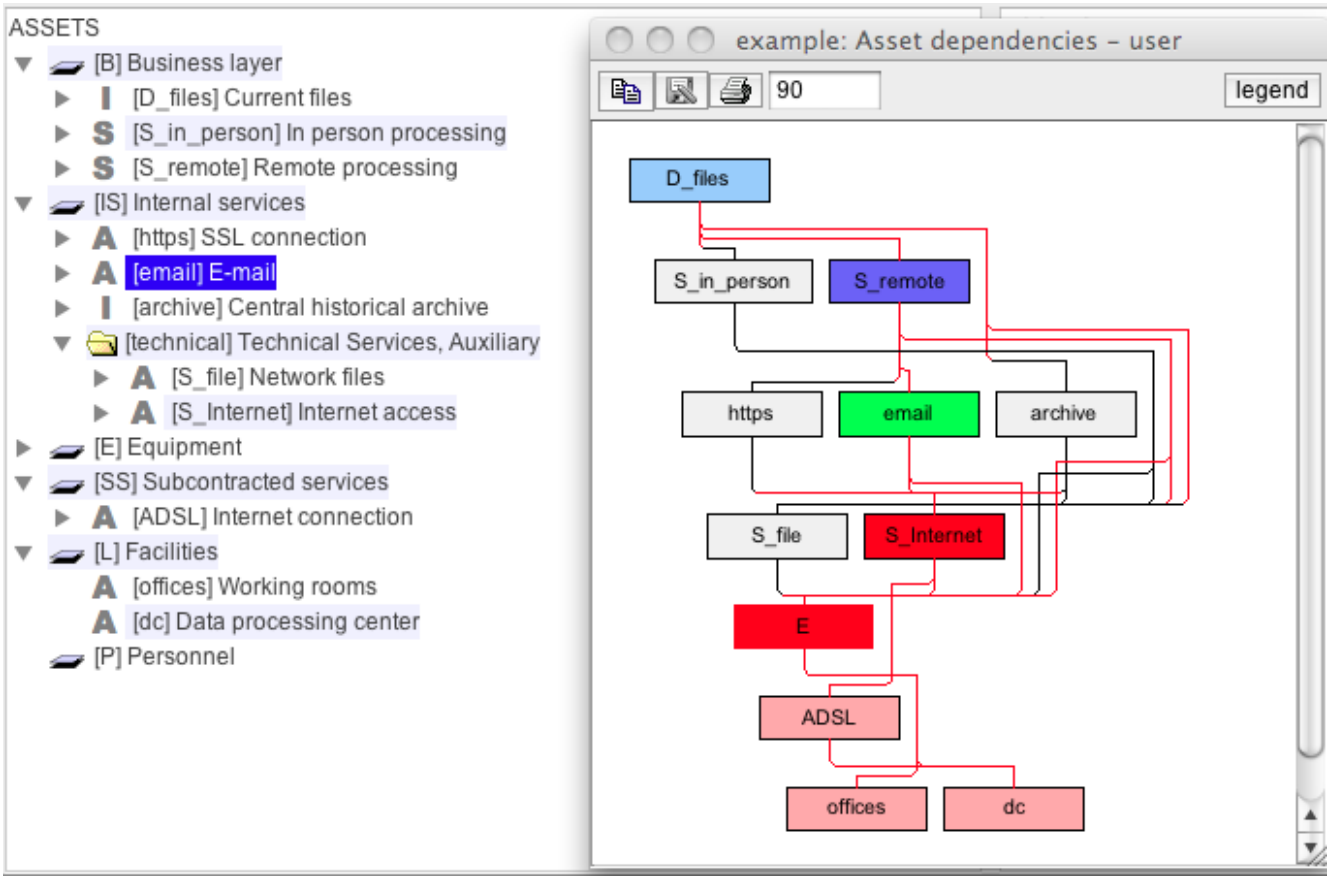
8.6.4 Dependencies – Blocks

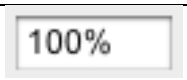
The graph shows the relationships between assets. It only presents the assets related to those selected on the main screen, or all the assets if nothing is selected.

Assets are heuristically positioned so that there is no relation going upwards: all dependencies go from top to bottom. PILAR create connection buses to connect one row to the next, and jump over rows.

The graph tracks the selection on the main dependencies screen. So, if you select an asset, a group or a layer, only the assets in the group and those direct or indirectly linked will appear in the picture.

Furthermore, within the assets shown, if you select one, it becomes green, those above turn red, and those below turn blue.



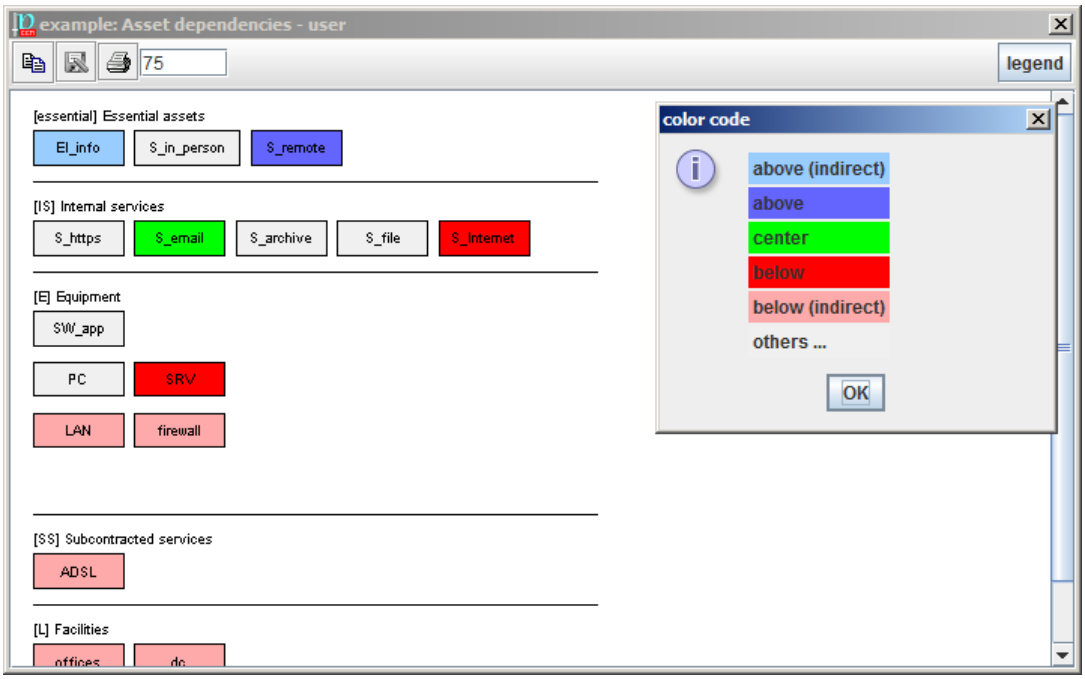
	**copy**	Copies the image to the note pad to paste it somewhere else.
	**save**	to store the picture as an image file. The available image formats depend on the hosting machine; some formats are quite widespread: jpg, jpeg, png
	**print**	to send the picture to a printer
	**scale**	to enlarge / decrease the image
	legend	show the colour codes

8.6.5 Dependencies – Map

Assets are presented in layers. Assets cannot be repositioned.

When an asset is selected, the map is coloured:

light blue	the assets indirectly above
strong blue	the assets directly above
green	the selected asset
strong red	the assets directly below
light red	the assets indirectly below
grey	unrelated



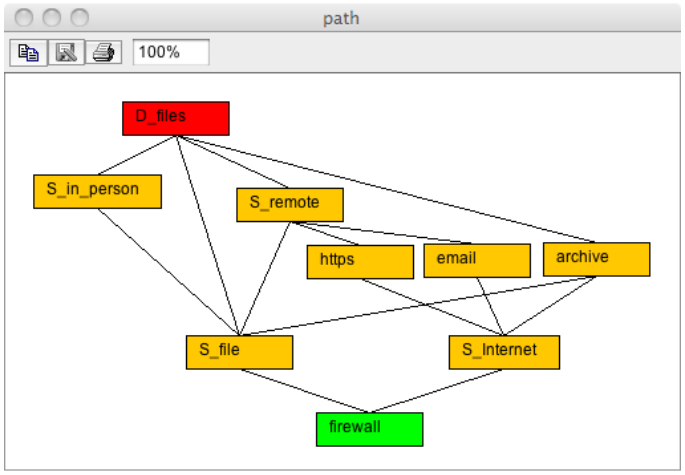
To modify the dependencies

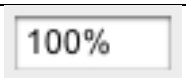
While an asset is selected (green) you may go to another asset and click on the right mouse button:

- to add this asset as above the selected one
- to add this asset as below the selected one
- to remove the dependency between this and the selected asset

To discover the dependency route from one asset to another

- select the father (green)
- select the son (right button)
- click on PATH
  the picture shows the routes (yellow) from the upper asset (red) to the lower asset (green):



	**copy**	Copies the image to the note pad to paste it somewhere else.
	**save**	to store the picture as an image file. The available image formats depend on the hosting machine; some formats are quite widespread: jpg, jpeg, png
	**print**	to send the picture to a printer
	**scale**	to enlarge / decrease the image
	legend	show the colour codes

8.6.6 Dependencies per dimension of security

You may specify a different dependency degree for each dimension of security. To do so, on the panel to edit asset dependencies, click the right button to jump into a new window where you may establish a precise dependency degree for each dimension.

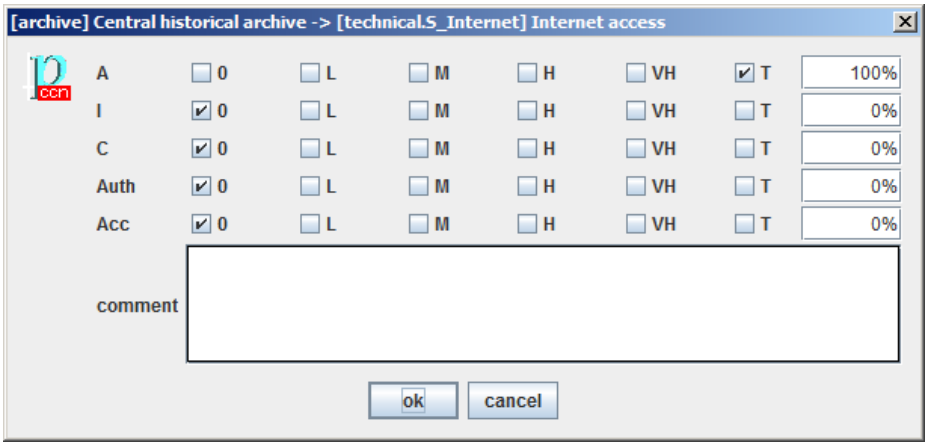
Typical values are as follow:

N	none	0%	no dependency
L	low	1%	academic – barely meaningful
M	medium	10%	meaningful, though not very much
H	high	50%	I do not know ...
VH	very high	90%	nearly complete
T	total	100%	full dependency

Click the right mouse button on the dependency you wish to modify:

- set all the same percentage is applied to every dimension
- set only 100% for the selected dimension, 0% for the others
- set 100% for the selected dimension, leave the other unmodified

— unset 0% for the selected dimension, leave the other unmodified
— details open the editing window



When you leave the editing window, the dependency degree appears on the dependencies tree using a compact notation. Let's show a few examples:

expression	**meaning**
A:100%	the dependency is only for the availability dimension; the other dimensions are not connected e.g. when a VPN stops the need to protect confidentiality any longer
I:100% / C:100%	the dependency is only for the integrity and confidentiality dimensions; the other dimensions are not connected e.g. when a redundant equipment guarantees availability

The format may be described as

expression ::= { one_dimension }0+

one_dimension ::= ACRONYM ':' percent '/'

When an expression is presented, all dimensions have a 0% dependency degree, except those explicitly stated.

8.7 Assets / Valuation

You may rate the system by domains or asset by asset. You select in *Options / Valuation*

If you are valuating by domains, you may skip dependencies, and jump directly into *Valuation by domains*

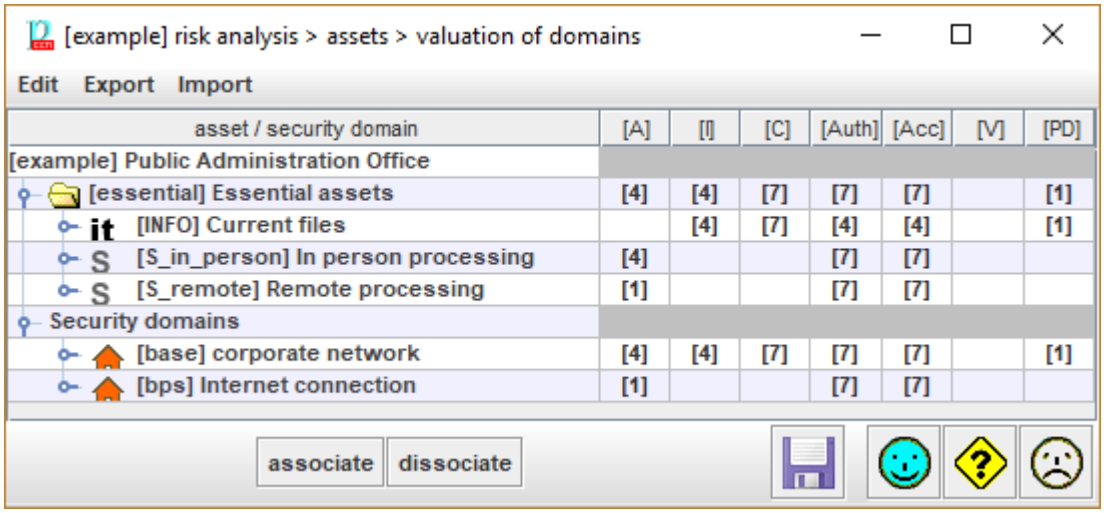
If you are valuating asset by asset, you have to establish the dependencies (see "*Dependencies between assets*), and then jump into *Valuation by assets*

8.7.1 Valuation by domains

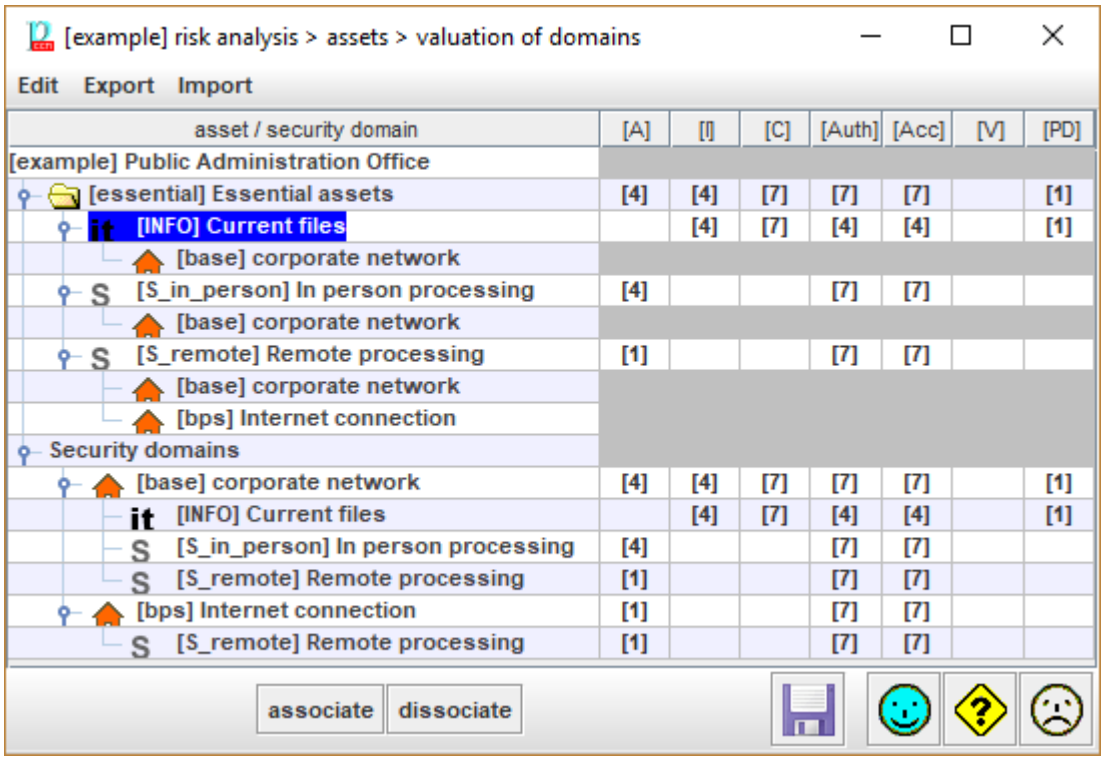
This approach provides a quick but imprecise assessment common for all the assets in each domain. It is faster than the evaluation by dependencies. Using this method, all assets in the domain receive the same values.

Nevertheless, some assets may be independent from the domain values. Use qualifier [independent] in asset classes.

The value of the information system is established for domains. The value is assigned to the essential assets (information and services) and transferred to the domain that hosts it, and to the domains that are associated to the essential asset.



You may better understand what is going on by displaying the association of assets to domains (and vice versa, of domains to assets):



Top menu EDIT

	Select one or more value cells. Copy values to be pasted.
	Select one or more destination cells. Paste the copied values. If the source range is 1 cell, and the destination covers several cells, the value is copied into all of them.

Top menu EXPORT

to CSV	CSV – comma separated values; for excel
to XML	XML – extensible markup language

Top menu IMPORT

from XML	XML – extensible markup language

Table - As many columns as security dimensions:

For each essential asset and each dimension, the value.

- See *Assets / Valuation / qualitative*
- See *Assets / Valuation / quantitative*

For each security domain, the value inherited from the essential assets associated to it.

Bottom toolbar

associate	Select one asset and one domain. Click to associate. Assets are always associated to their domain. You may associate to more domains.
dissociate	Select one asset and one domain. Click to dissociate. You may never dissociate an asset from its domain.

Typically, information assets require to protect confidentiality, integrity, authenticity and traceability, while services add requirements in terms of availability.

The value of the system is the largest value of those for any information or service.

Each domain inherits the valuation of the essential assets associated to it.

To associate an asset to a domain

- select the asset
- select the domain
- click ASSOCIATE

To disassociate an asset for a domain

- select the asset
- select the domain
- click DISSOCIATE

8.7.2 Valuation asset by asset

If you are valuating asset by asset, you have to establish the dependencies (see "*Dependencies between assets*).

Quick start

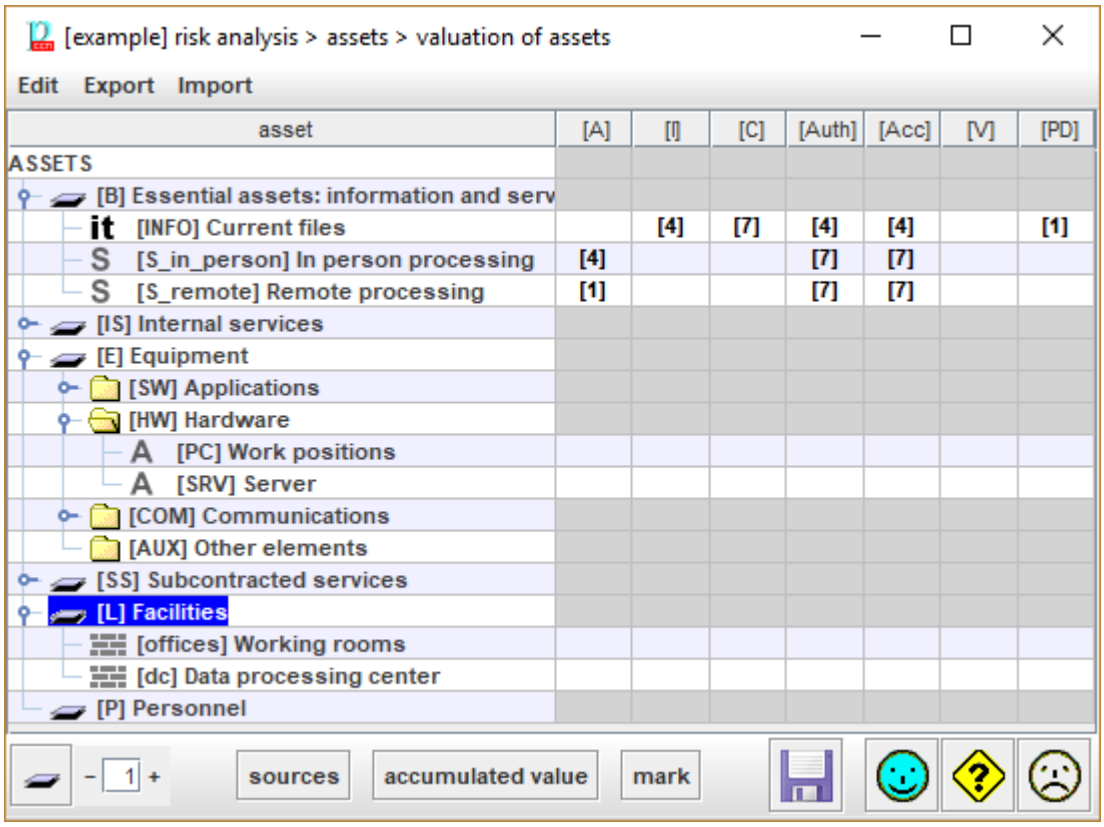
Which is your major concern with this information system?

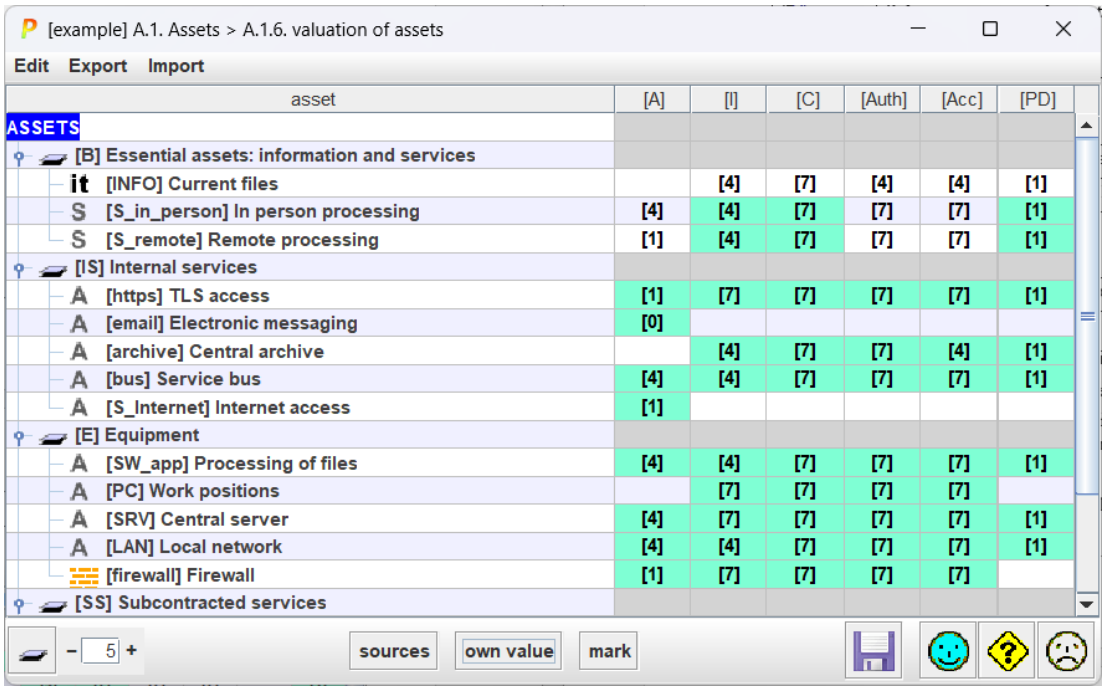
- Select and asset (row) in the business (up most) layer,
- select a security dimension (column); then
- double click to select a value from 0 (negligible) and 10 (absolutely critical)
  … or somewhere in between.

Repeat with other concerns until the rest is not so important.

Click **ACCUMULATED** and double check that every asset has a value that makes sense to you.

This screen is used to assign values to individual assets on each dimension.





Top menu EDIT

	Select one or more value cells. Copy values to be pasted.
	Select one or more destination cells. Paste the copied values. If the source range is 1 cell, and the destination covers several cells, the value is

	copied into all of them.

Top menu EXPORT

to CSV	CSV – comma separated values
to XML	XML – extensible markup language

Top menu IMPORT

from XML	XML – extensible markup language

Table - As many columns as security dimensions:

For each asset and each dimension, the value.

- See *Assets / Valuation / qualitative*
- See *Assets / Valuation / quantitative*

When presenting the own value of the asset, the value is shown on white background.

[A]	[I]	[C]	[Auth]	[Acc]
	[4]	[7]	[4]	[4]
[4]			[7]	[7]
[1]			[7]	[7]

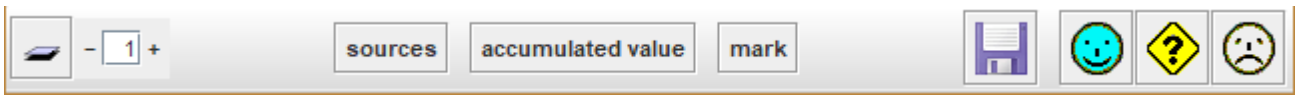
When presenting the accumulated value on the asset, the accumulated value is presented on green background.

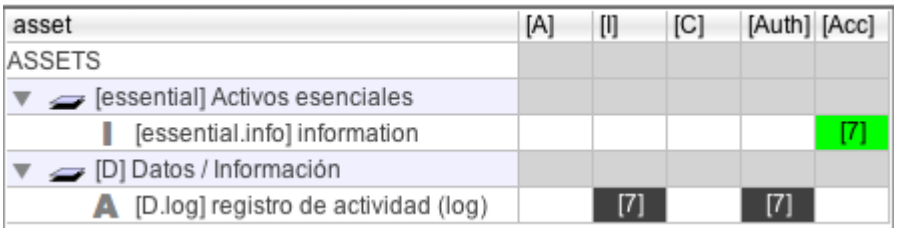
[A]	[I]	[C]	[Auth]	[Acc]
[4]	[4]	[7]	[7]	[7]
[4]	[4]	[7]	[7]	[7]
[4]	[4]	[7]	[7]	[7]

When the risk analysis is quantitative, the values are numbers.

	47K	100K	47K	47K
47K	47K	100K	260K	147K
10K	47K	100K	260K	147K

Bottom toolbar



	Click to collapse assets tree.
	Control the level of expansion of the assets tree.
sources	Select one source. PILAR will select the assets in the tree that associated with that source.
accumulated / own value	Switches from presenting only own value, or also accumulated values.
mark	Useful to see how value is propagated. Select one cell, click MARK. The value source is on green background. The destination of the value is on black background. For instance, to see how the needs on accountability are translated into integrity and authenticity of activity registers: 

The first column presents the assets, organised as a tree. The other columns cover security dimensions. Only assets may receive values; the other rows are dead.

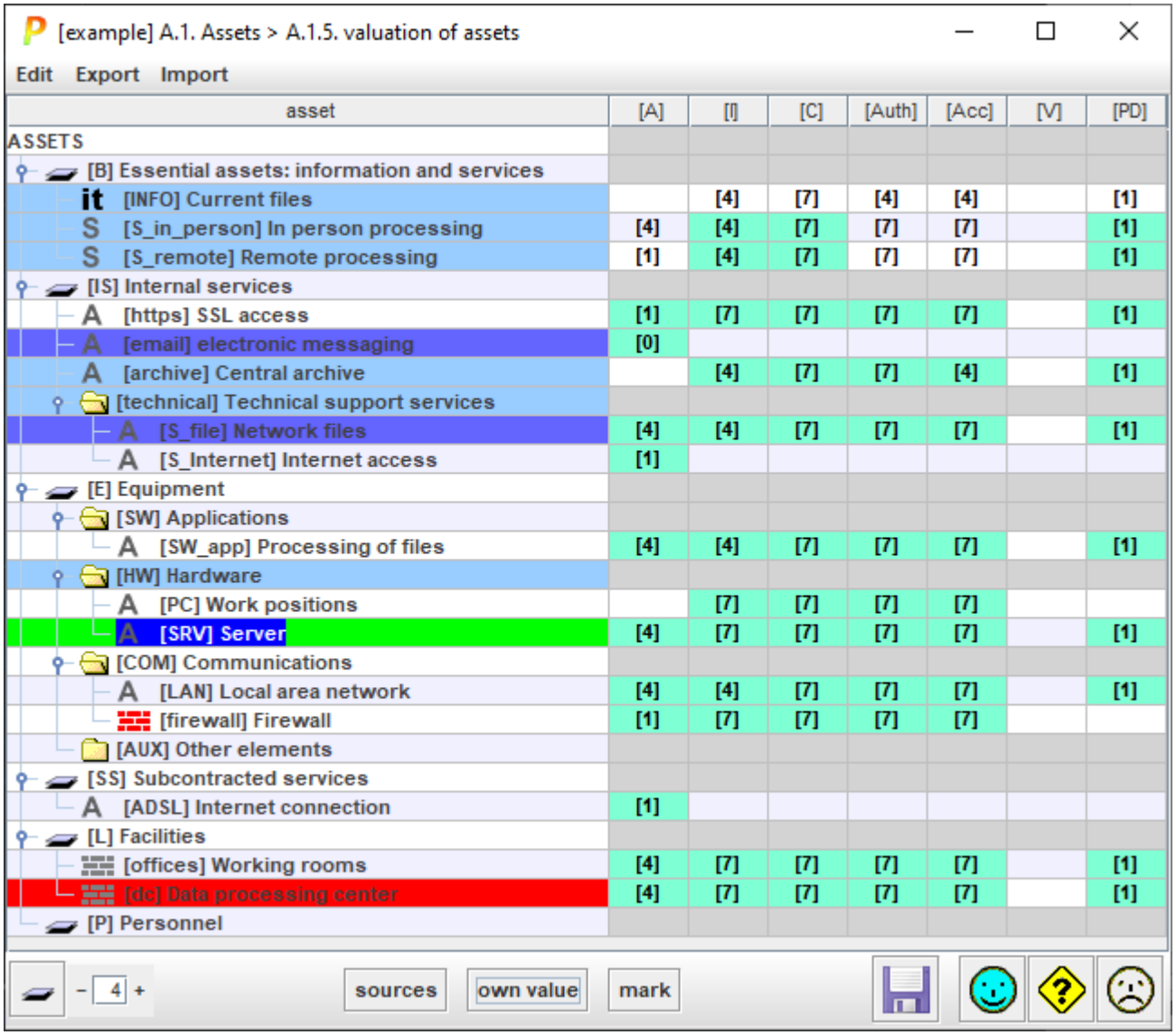
The screen allows to

- [for quantitative analysis] to introduce a numerical value
- to introduce a comment explaining why this value
- to select the criteria that apply from those in the library.
  It is important to try to use encoded criteria.

To discover where does the accumulated value come from …

- select the asset (row)
- click SOURCES

As an alternative, you may select an asset on the asset tree, and PILAR colours the assets above and below:



Assets above are shown in BLUE, while assets below are shown in RED.

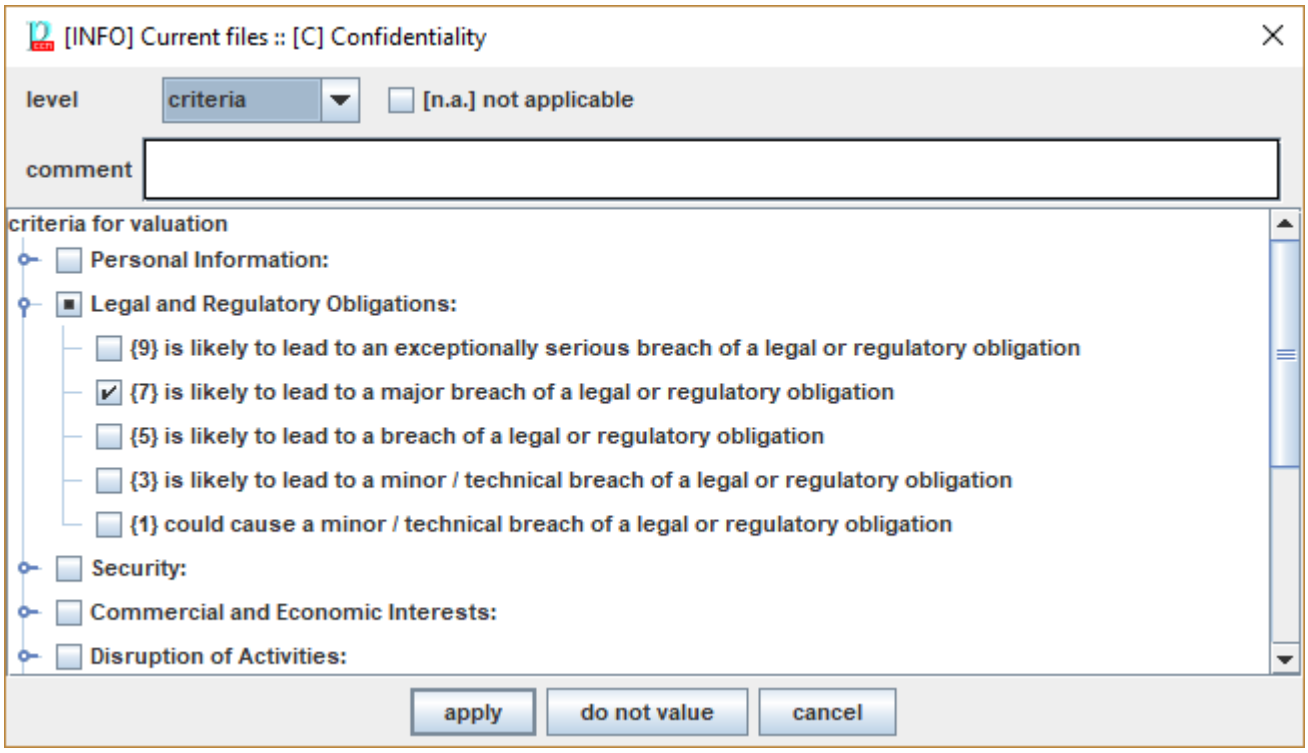
8.7.3 To set a qualitative valuation

A fast option is to click CTRL + or CTRL – to increase/decrease the valuation of an asset on a given dimension.

Alternatively, you may open a valuation screen where you may include comments and criteria for valuation.

To assign value to an asset

- select the asset (row) and dimension (column)
- double click



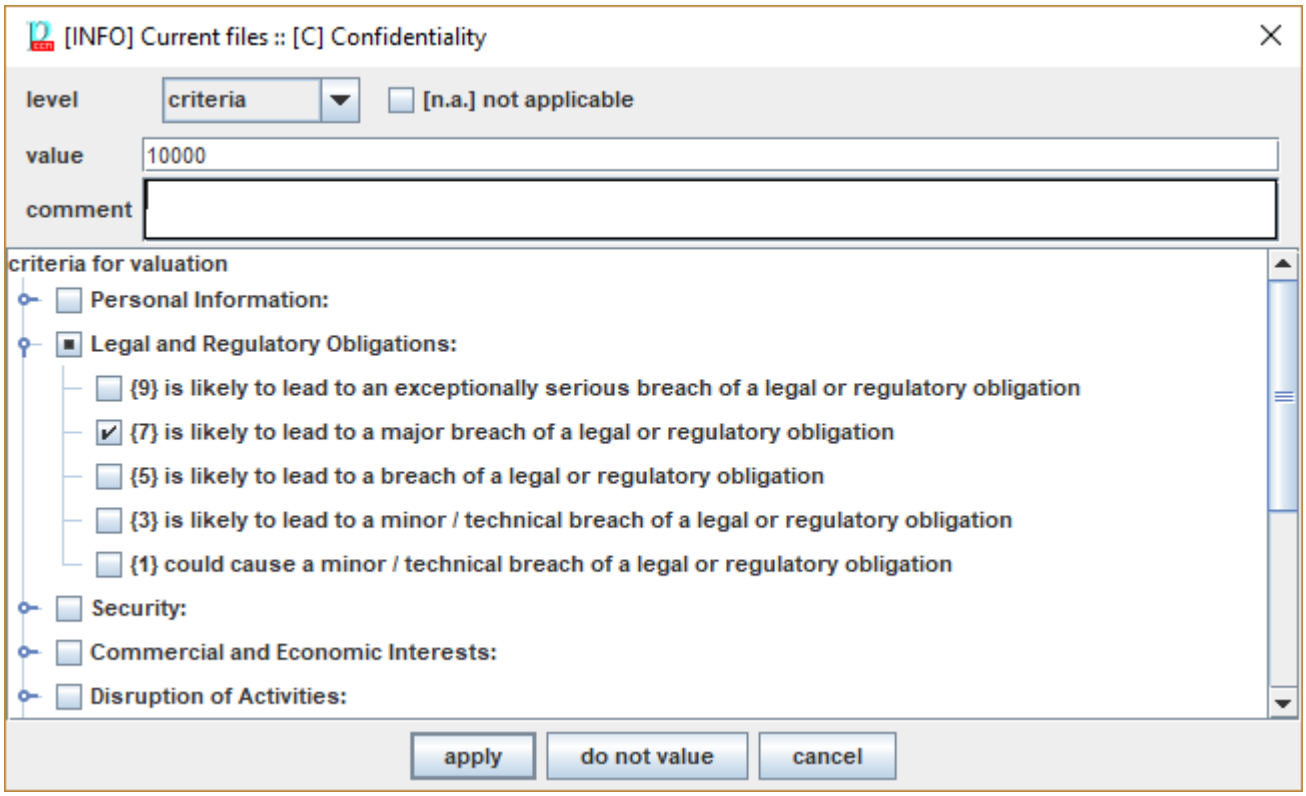
level combo	If you select "criteria" the value is decided by the highest-ranking criteria marked in panel. If you select any other value, that value is forced, ignoring the criteria (that are retained only for informative purposes).
[n.a.]	If the value has no sense for the asset, and its descendants, mark N.A. See "*To nullify a valuation*".
comment	A comment explaining the valuation.
panel	Criteria to rate an asset.
APPLY	Apply value and close.
DO NOT VALUE	Remove the value from the asset.
CANCEL	Close without modifying asset valuation.

8.7.4 To set a quantitative valuation

Quite similar to qualitative valuation, but now the user may provide a quantity, and also mark some criteria.

To assign value to an asset

- select the asset (row) and dimension (column)
- double click

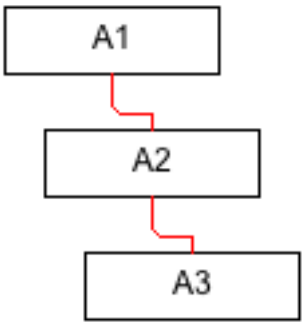


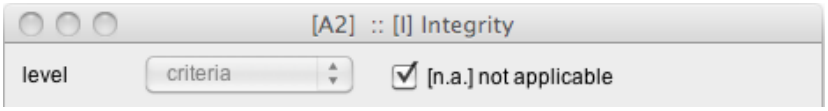
combo	Set the qualitative value. If you select "criteria" the value is decided by the highest-ranking criteria marked. If you select any other value, that value is forced, ignoring the criteria (that are retained only for informative purposes).
[na]	If the value has no sense for the asset, and its descendants, mark N.A. See "*To nullify a valuation*".
value	Set the quantitative value.
comment	A comment explaining the valuation.
panel	Criteria to rate an asset.
APPLY	Apply value and close.
DO NOT VALUE	Remove the value from the asset.
CANCEL	Close without modifying asset valuation.

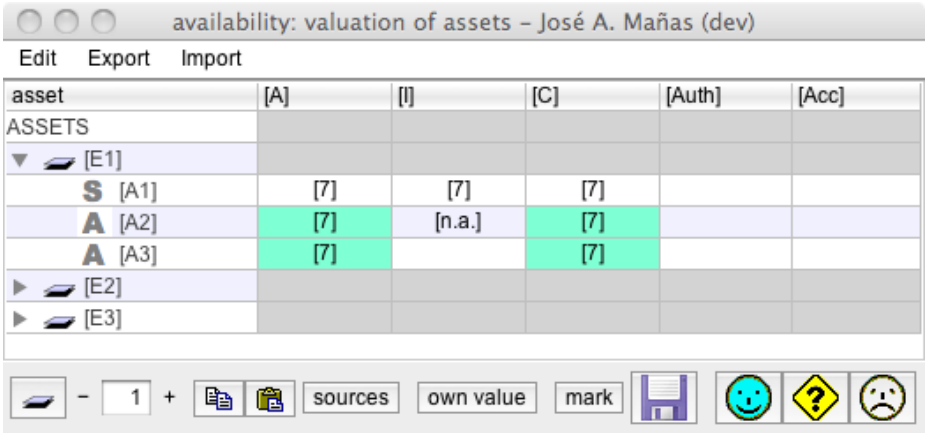
When PILAR has only a qualitative valuation, or only a quantitative valuation, she uses the "quantification criteria" to estimate the missing value.

8.7.5 To nullify a valuation

Assets accumulate the valuation inherited, by dependencies, from their superiors. If we want to cancel the transfer of value to a particular asset, and to prevent further propagation to the lower assets (by dependencies), in the panel of to determine the level, select N.A.







The effect is similar to adjusting the dependencies from the assets that contribute to the value that we want to cancel.

8.7.6 Availability valuation

The assessment of availability can be adjusted, in several ways:

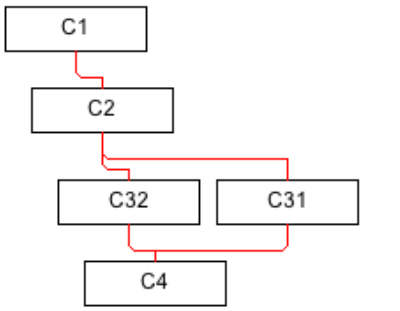
- establishing exact *dependencies* between assets
- *nullifying* the value
- marking some qualifiers (see below)

If the asset is marked as "[availability.easy]" (see asset classes), then the availability value is reduced by an order of magnitude (3 levels in the level rating scale). This adjustment will be reflected in the assessment of the impact of threats. The local value is reduced without affecting the value that is further propagated down the dependencies.

If the asset is marked as "[availability.none]" (see asset classes), then the availability value is reduced to zero. This adjustment will be reflected in the assessment of the impact of threats. The local value is reduced without affecting the value that is further propagated down the dependencies.

If the asset is marked as "[or]" and it depends on more than 1 child, availability is not forwarded to its children or to the following assets in the transfer chain. However, if the further down in the transfer chain, the various branches converge at a common asset, the availability value is recovered again. So, alternative paths do have no availability requirements, but a single point of failure does.

The following example shows how the redundant equipment C31 and C32 are not valued in availability, while the common asset, C4, recovers value. Note that other dimensions are not affected by classification as OR.



asset	[A]	[I]	[C]	[Auth]	[Acc]
ASSETS					
[E1]					
[E2]					
[E3]					
S [C1]	[7]		[7]		
A [C2] OR	[7]		[7]		
A [C31]			[7]		
A [C32]			[7]		
A [C4]	[7]		[7]		

8.8 Zones

Information systems may be protected by borders that separate internal assets from external assets. E.g. a firewall separates external world from internal assets. Borders are important defence elements where external attackers may be prevented from reaching internal assets. We need to identify zones, and connections between zones (aka interconnections)

Zone

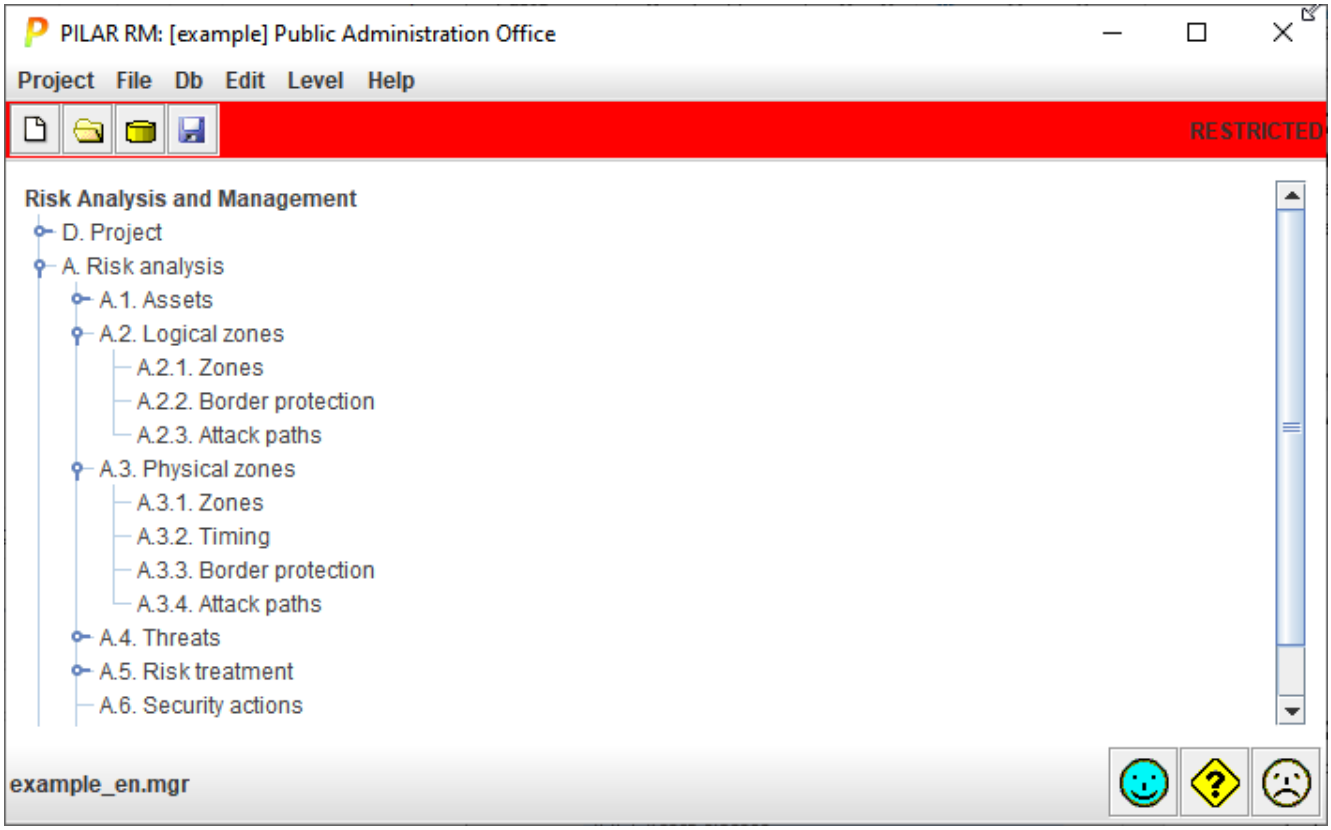
A zone refers to a collection of assets that manage some information. It's crucial to safeguard the flow of information between zones to prevent unauthorized access or the transmission of malicious code.

Connection between zones

The interconnection between zones is facilitated by a set of devices designed to furnish comprehensive protection services for the information exchanges between the interconnected zones. Borders regulate information ingress and egress.

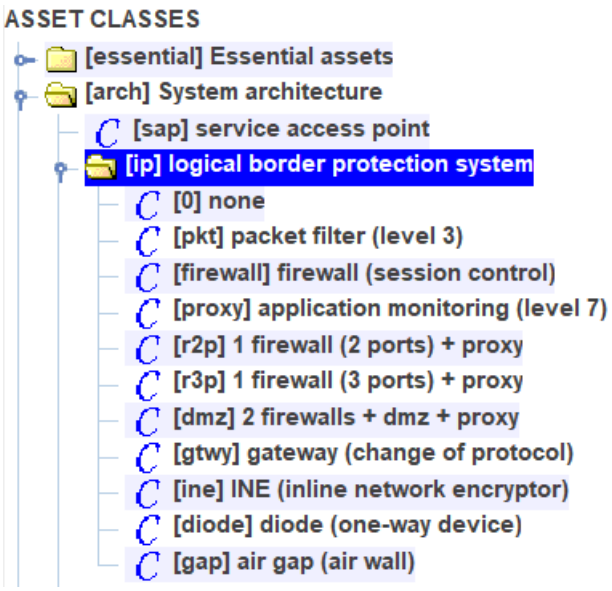
WARNING: physical zones are under revision.

Zone management is part of risk analysis.



8.8.1 Asset classes

PILAR knows there are zones when there are assets qualified as border protection:

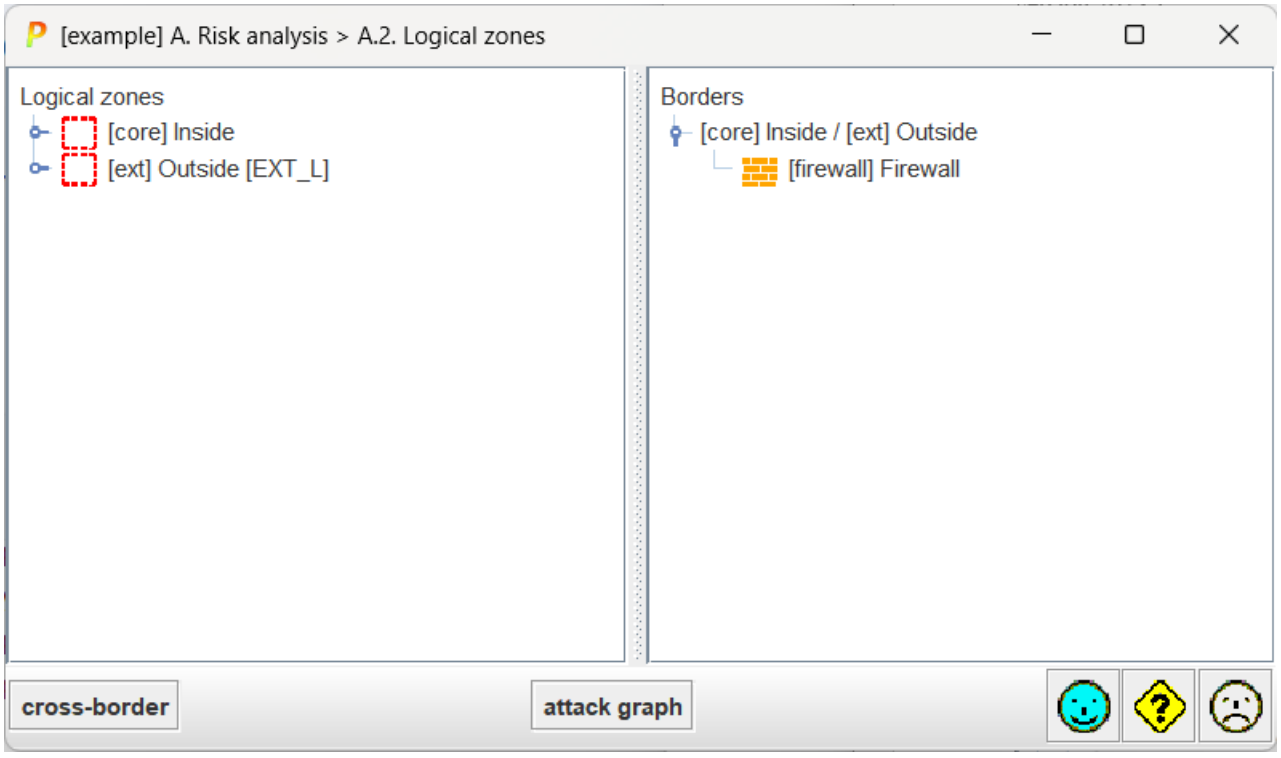


8.8.2 Zones and borders

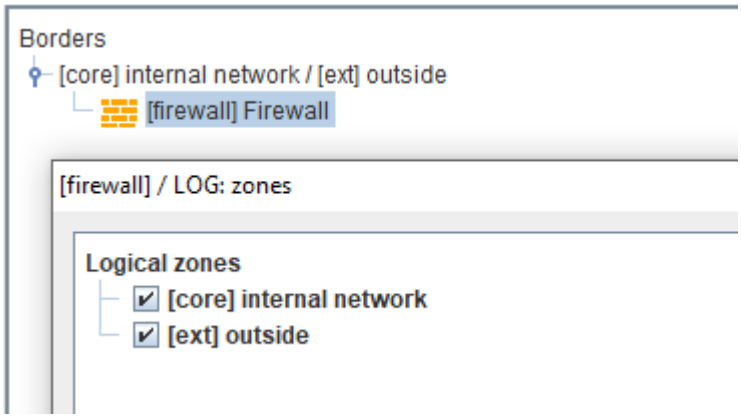
Currently only for logical borders.

Users may create zones separated by borders, making a difference between been in one zone or being in the border.

Standard approach is to place assets inside, outside, and on the border



Users may drag and drop assets between zones. To move an asset into a border or to remove it from the border, double click and edit:



Please, note that while an asset is in zone A, it cannot be simultaneously in another zone B, unless it is in the border. An asset may be part of more than one border; that is, it may connect more than 2 zones.

Right click on root “logical zones” to create new zones, and to use a wizard to propose a standard allocation of assets around declared borders.

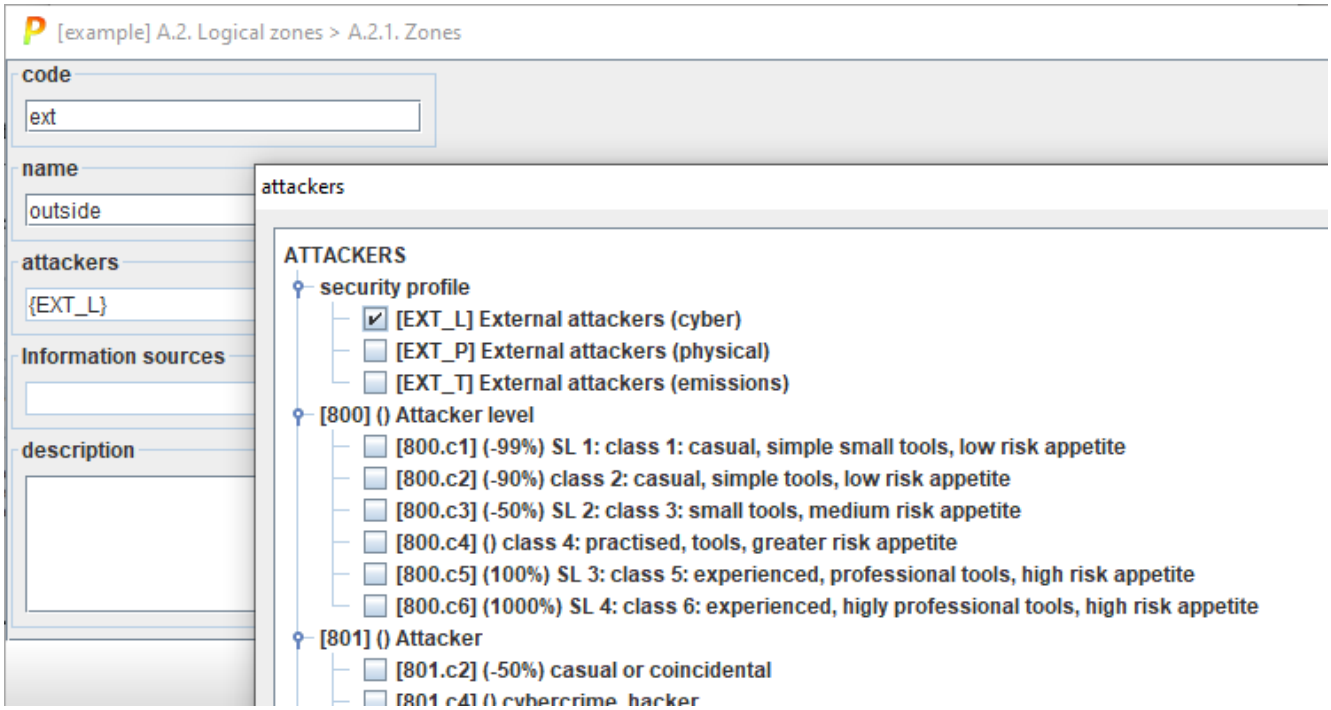
Right click on a zone to edit it.

Right click on an asset to edit it. Editing an asset means to set manually the zones where the asset can be reached. When the asset is in more than one zone, PILAR understand the asset is part of the border between those zones.

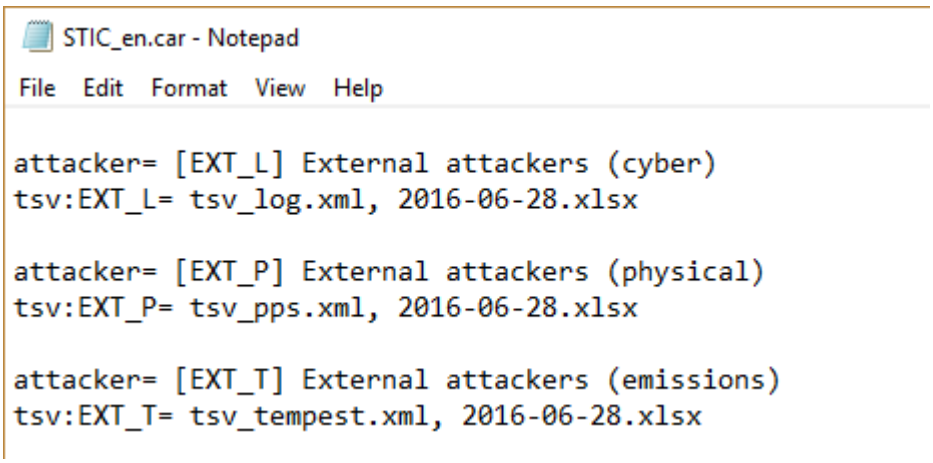
8.8.3 Zone definition

While creating a new zone, or editing it afterwards, users may determine its (unique) code, a descriptive name, information sources, and a verbose description (that may link to an internal web repository.

Most relevant, users may specify the attacker profile, for attacks starting from this zone.



Attack profiles are described by means of TSV specification files, referred from the configuration (CAR) file:



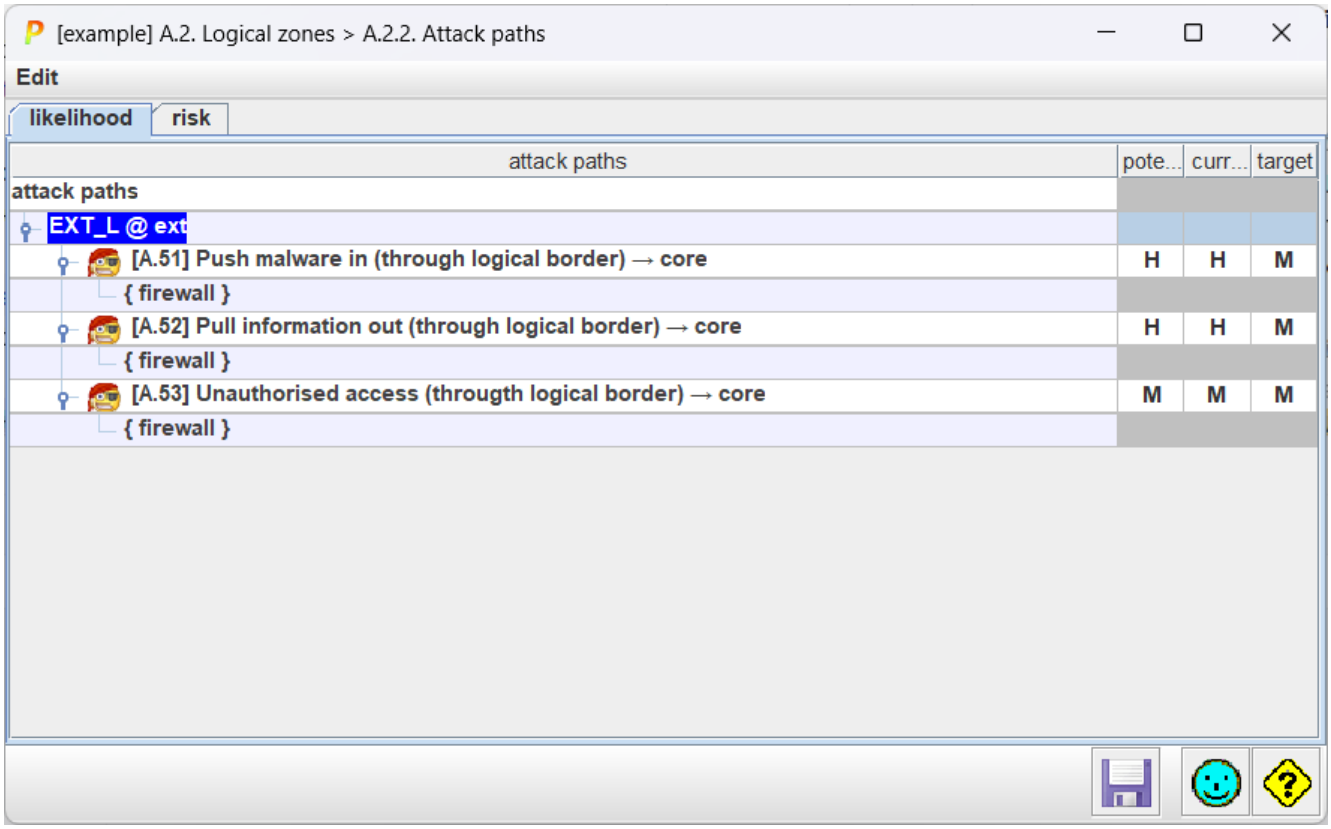
For a logical attacker like EXT_L, his capabilities on border system are described in tsv_log.xml. Once the border is passed, its capabilities are described by means of 2016-06-28.xlsx.

8.8.4 Attack paths

Currently only for logical borders.

This screen presents the paths that attackers may follow from external origin to target zones. For each threat and phase, PILAR presents the estimated likelihood (of success) and risk.

For **likelihood**, the screen looks like this



Let’s read it.

Row 1

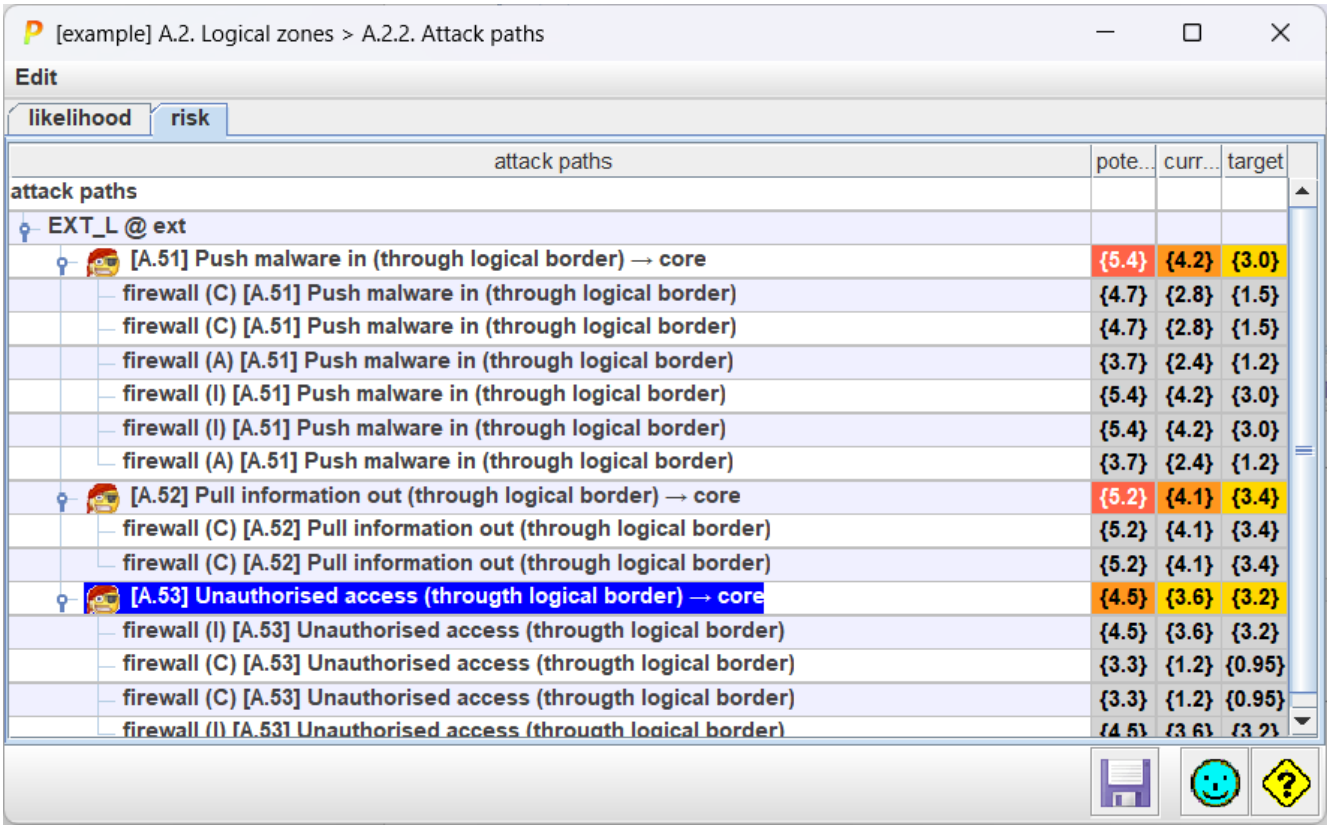
For external attackers EXT_L at ext zone.

Row 2 (and 4, and 6)

Exercising threat A.51, the attacker may push malware thru border device “firewall” (row 3) into internal zone “core”.

The columns present likelihood of the attack for each phase.

For **risk**, the screen looks like this

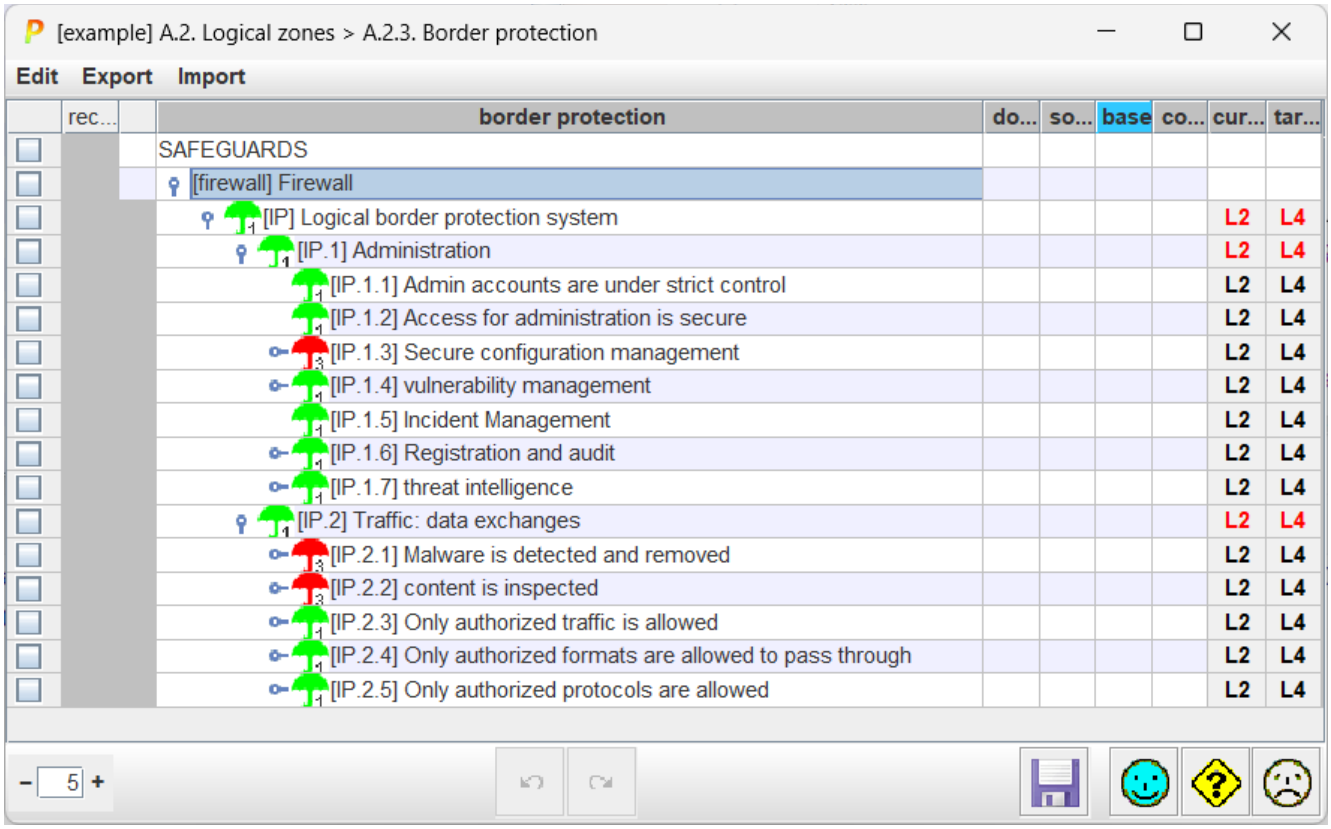


It is quite similar as for likelihood, but impact may affect more than one dimension, and PILAR presents one row for each.

8.8.5 Border protection

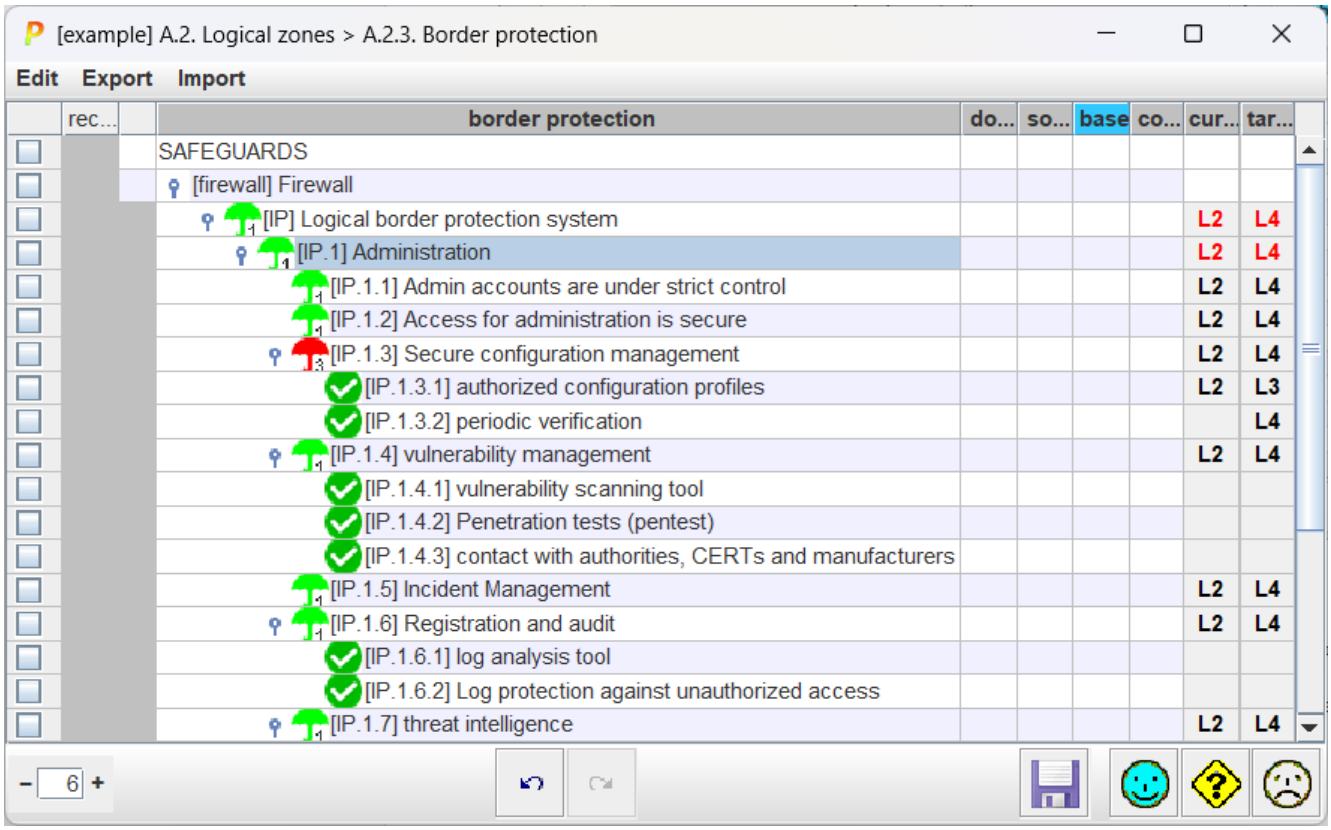
Here you specify security measures to protect the border.

The screen is like countermeasures (see *Safeguards*). For each border asset:



The protecting safeguards are organized into 2 levels:

- Effective level (umbrellas), where measures maturity is evaluated, and used to mitigate border threats.
- Documentation level (green circles), where items are presented (and may be valuated) to explain the value assigned to the encompassing effective row. These values are NOT used for risk mitigation.

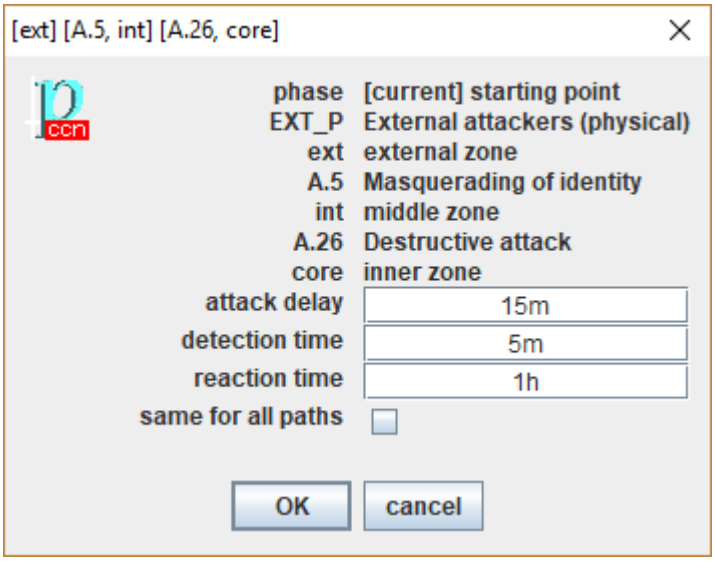


8.8.6 Time analysis

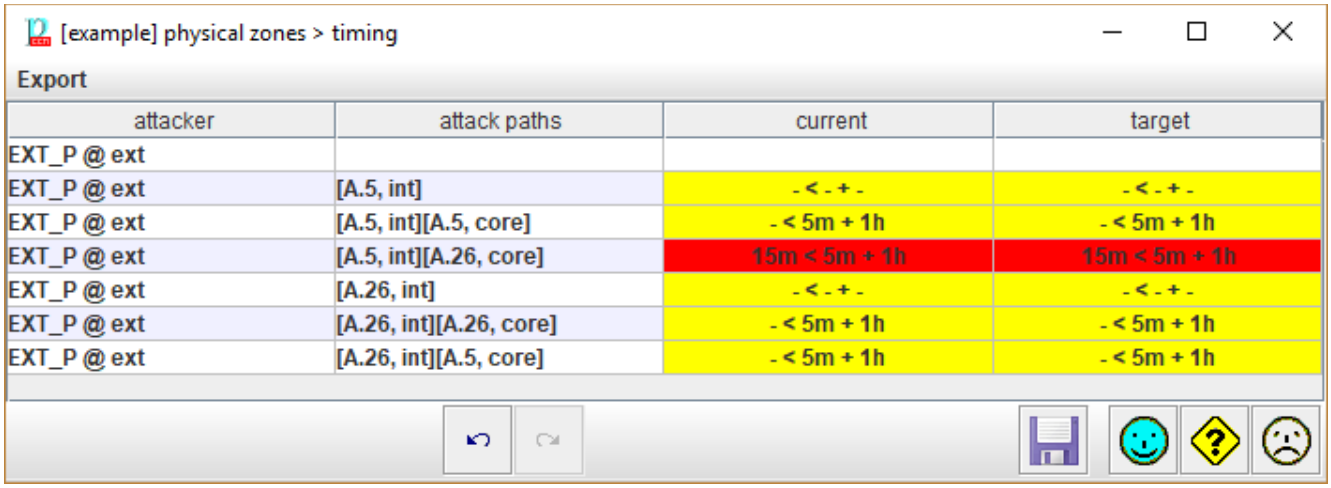
This analysis in only for physical attacks.

It compares the time required by the attacker to go through the border, against the time to detect plus the time to react.

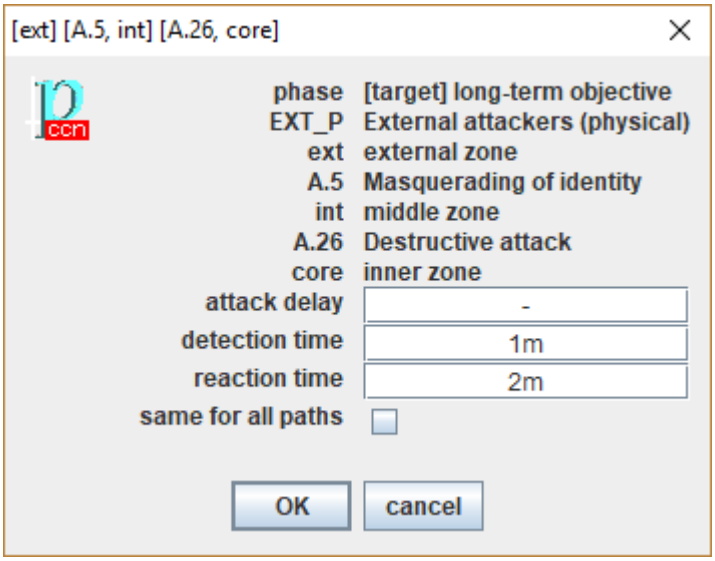
Let's see an example. There are 3 zones: external, intermediate, and internal. There is an external attacker that tries to get inside. The attacker requires 10 minutes. The border systems take 5 min to detect, and reaction requires 1 hour.



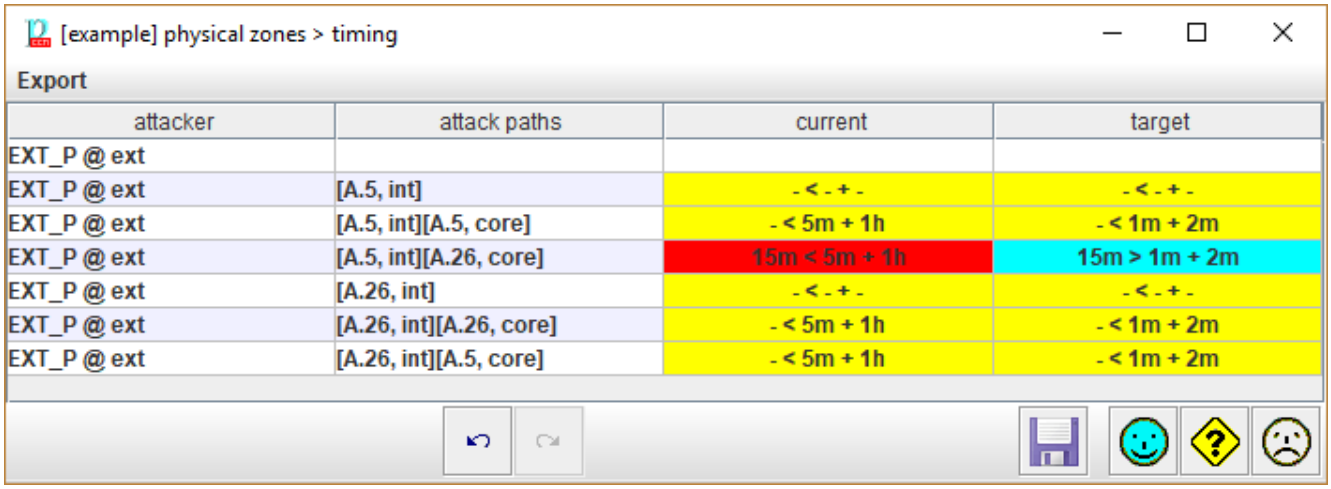
The system has a problem: the attacker is too fast for the protection system:



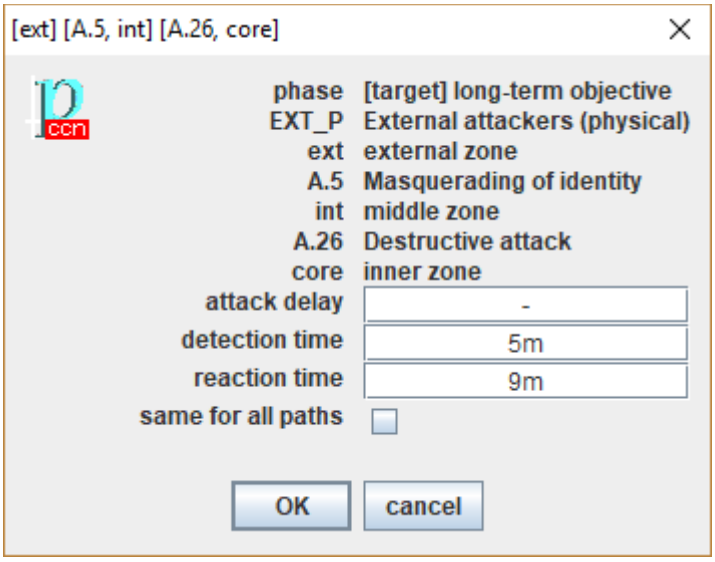
We can improve reaction for the target phase

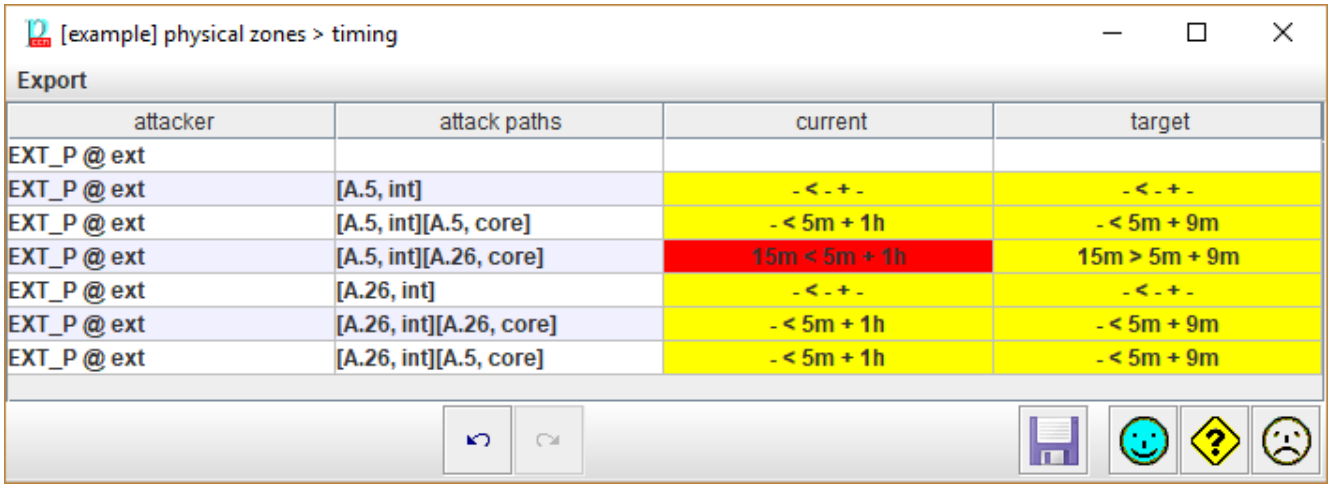


The attack is blocked



The time balance may be not so clear, and the chances of the attacker to succeed are not zero:





attacker	attack paths	current	target
EXT_P @ ext			
EXT_P @ ext	[A.5, int]	- < - + -	- < - + -
EXT_P @ ext	[A.5, int][A.5, core]	- < 5m + 1h	- < 5m + 9m
EXT_P @ ext	[A.5, int][A.26, core]	15m < 5m + 1h	15m > 5m + 9m
EXT_P @ ext	[A.26, int]	- < - + -	- < - + -
EXT_P @ ext	[A.26, int][A.26, core]	- < 5m + 1h	- < 5m + 9m
EXT_P @ ext	[A.26, int][A.5, core]	- < 5m + 1h	- < 5m + 9m

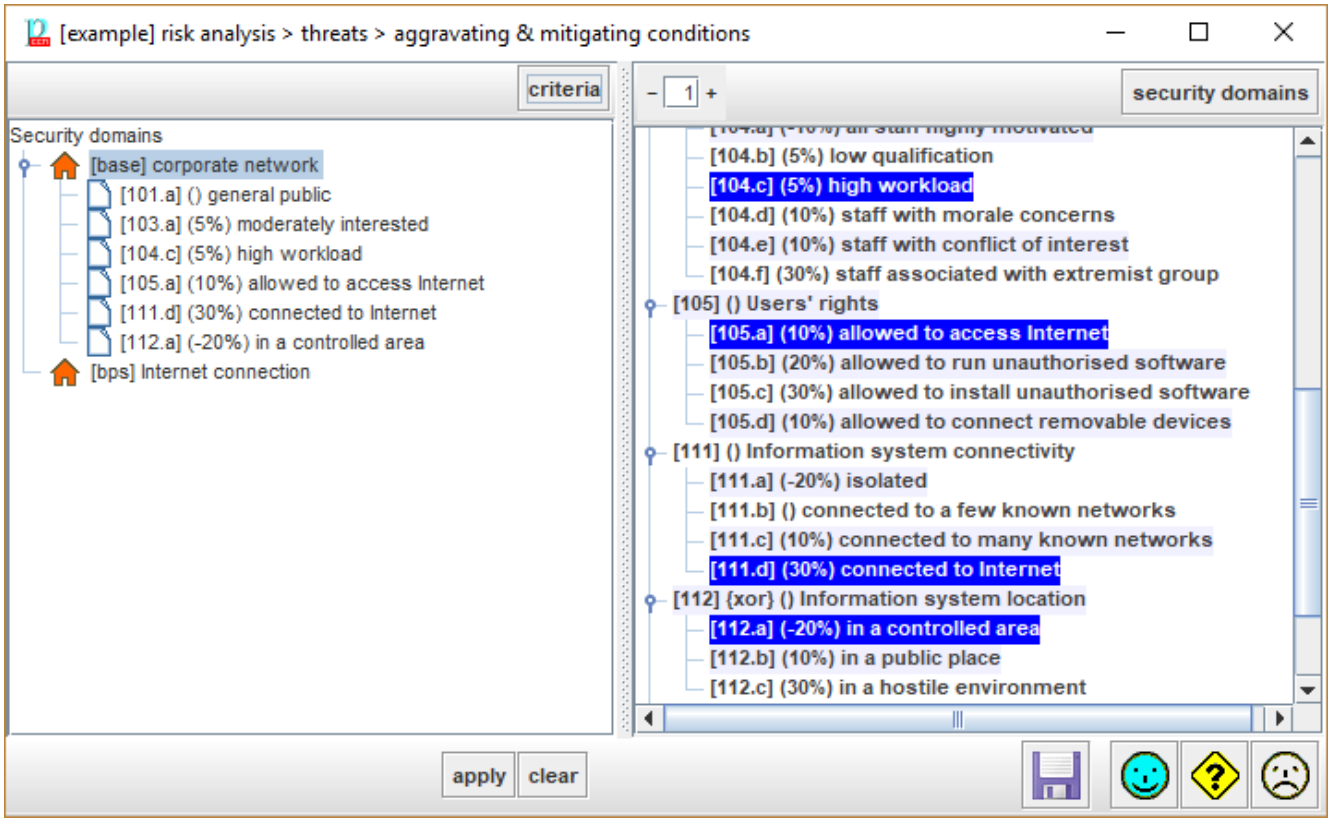
Attack paths where reaction time is fast enough, are removed. PILAR retains those where speed is not enough.

8.9 Threats

8.9.1 Aggravating & mitigating factors

This screen qualifies domains with a number of characteristics. The effect is to modify the standard values assigned from threat profile files.

If you modify the associations in this window, please, re-apply the library, or another TSV file (see "*Valuation of threats*". TSV is applied automatically if threats are set to automatic (see *Options / Threats*).



Top toolbars

criteria	Select one security domain in the left panel. Click CRITERIA and PILAR will select in the right panel the criteria applying to the selected domain.
- 1 +	Control the level of expansion of the criteria tree.
security domains	Select one criterion in the left panel. Click DOMAINS and PILAR will select the security domains in the right panel where the criterion applies.

Bottom toolbar

apply	Select one or more security domains in the left panel. Select one or more criteria in the right panel. Click APPLY to associate.
clear	Select one or more security domains in the left panel. Select one or more criteria in the right panel. Click CLEAR to dissociate.
	Saves current project either in a file, or in database (according to its source).

To associate a criterion to a domain

- select the domain (left panel)
- select the criterion (right panel)
- click APPLY

To remove a criterion association

- select the criterion (on the left panel)
- click CLEAR

To discover the criteria associated to a domain

- select the domain (on the left panel)
- click criteria (left panel, top)

To discover the domains subject to a vulnerability

- select the criterion (on the right panel)
- click DOMAINS (right panel, top)

8.9.2 Identification

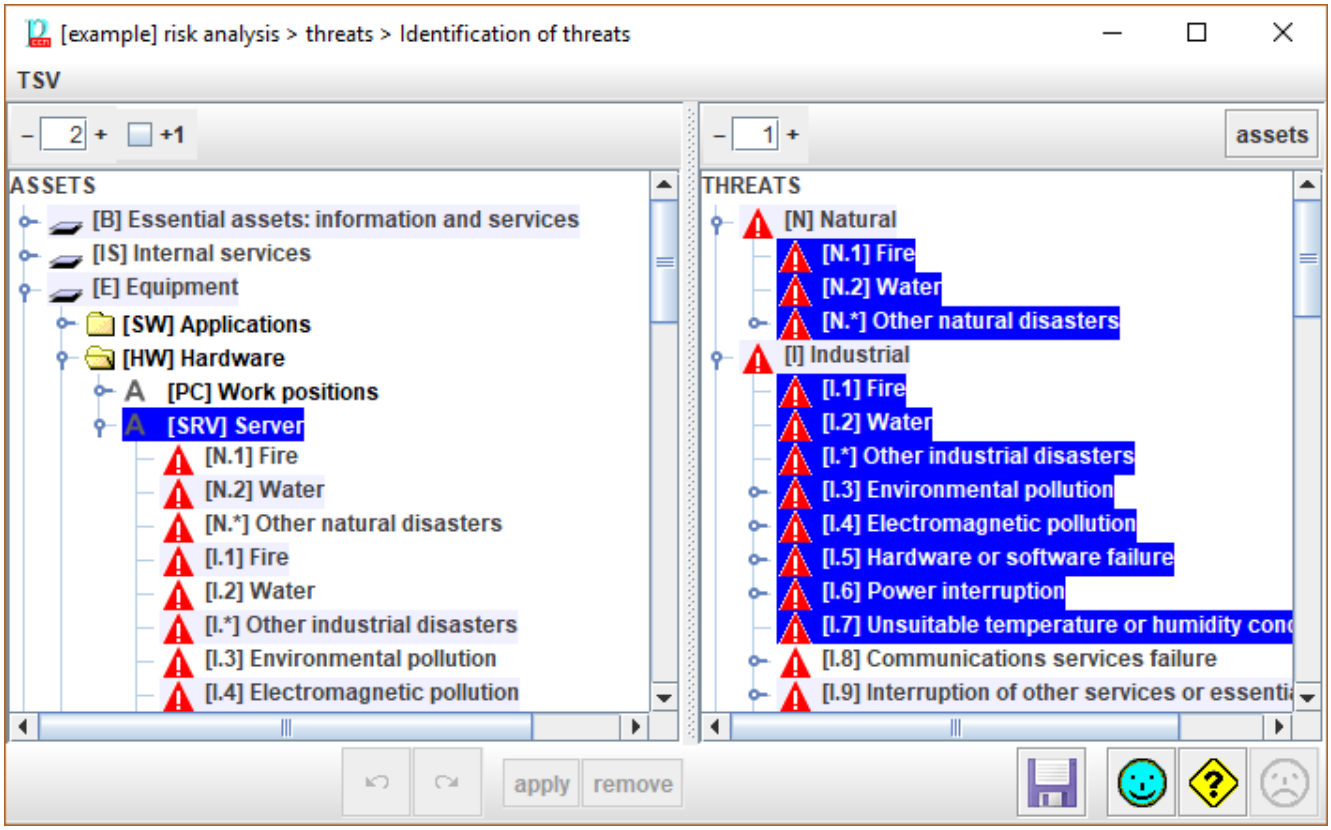
Quick start
Select automatic threats in *Options / Threats*. PILAR applies non-optional threats from TSV.

Not so quick start
Select MIX threats in *Options / Threats* By default, PILAR treats all assets as automatic and applies non-optional threats from TSV. You may remove / add threats as convenient. As a help, right click on an asset to check whether there are optional threats on that asset. Apply as convenient.

This screen lets us identify which threats are possible for each asset.

Please, note that if you are in automatic mode, some buttons are disabled:

- copy and paste
- XML import
- apply and remove
- undo / redo



Top menu TSV

TSV	See "*Threat Standard Values*

Top toolbar

– 1 +	Spinner to control the expansion of the assets tree.
+1	Adjust the effect of the spinner. If +1 is checked, PILAR shows the threats associated to an asset. If unchecked, the threats are not expanded.
– 1 +	Spinner to control the expansion of the threats tree.
assets	— Select one or more threats in the right panel. — Click ASSETS. PILAR selects on the left panel, the assets that are associated to the selected threats.

Bottom toolbar

	Undo last association of threats to assets
	Redo last undone association of threats to assets
apply	— Select one or more assets in the left panel — Select one or more threats in the right panel — Click APPLY PILAR associates the selected threats to the selected assets
remove	— Select one or more assets in the left panel — Select one or more threats in the right panel — Click REMOVE. PILAR dissociates the selected threats to the selected assets. Or — Select one or more threats in the left panel — Click REMOVE PILAR dissociates the selected threats from the associated assets.
	Saves current project either in a file, or in database (according to its source).

On assets (left panel)

- Right click > CURRENT
  - to select current threats on the right panel
- Right click > STANDARD
  - to select threats on the right panel (those in TSV, but optional ones)
- Right click > OPTIONAL
  - to select threats on the right panel (those in TSV marked as optional)

Options / Threats **are set to automatic.**

Some buttons are disabled:

- apply and remove
- undo / redo
- cancel and close

Options / Threats are set to **manual.**

- Apply and remove buttons are enabled.
- TSV is not applied by default

Options / Threats are set to **mix.**

- Apply and remove buttons are enabled.
- TSV is not applied by default

In manual mode and mix modes, you can associate threats to assets freely.

To assign TSV threats to an asset
(or a group, or a layer, or all of them)

- select asset(s), group(s), layer(s), or top node
- top menu TSV > apply

To assign a threat to an asset
(manual mode or mix mode and manual asset)

- select the asset on the left (one or more)
- select the threat on the right (one or more)
- click APPLY

To remove a threat from an asset
(manual mode or mix mode and manual asset)

- select the asset on the left (one or more)
- select the threat on the right (one or more)
- click REMOVE

or

- select the threat on the left (one or more)
- click on REMOVE

Which threats are associated to an asset?

- select the asset on the left
- right click > CURRENT

Which threats are associated to an asset as standard?

- select the asset on the left
- right click > STANDARD

Which threats are optionally associated to an asset?

- select the asset on the left
- right click > OPTIONAL

To "copy and paste" threats from an asset onto another
(manual mode or mix mode and manual asset)

- select the source asset on the left
- right click > CURRENT
- select the destination asset on the left (one or more)
- click APPLY

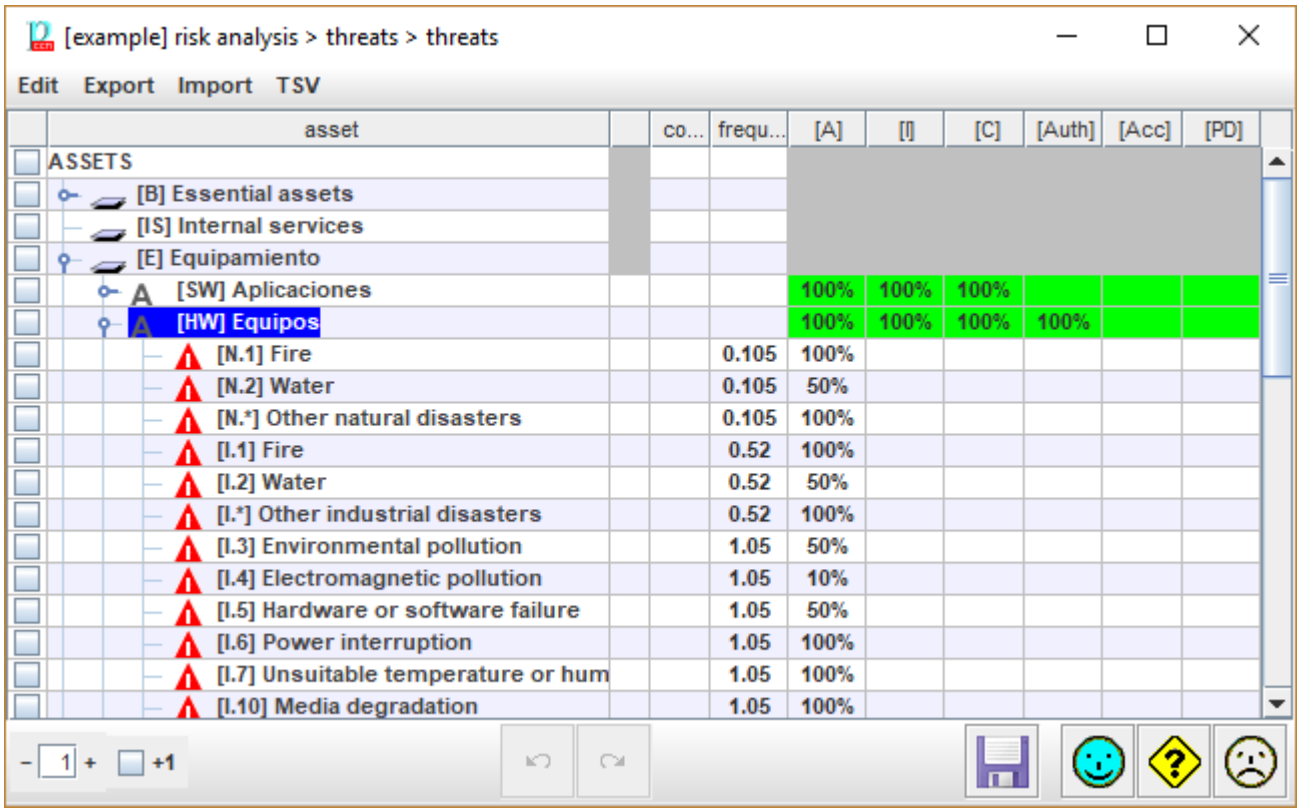
Which assets are subject to a threat?

- select the threat on the right (one or more)
- click ASSETS

8.9.3 Valuation

Quick start
If *Options / Threats* is set to automatic or mix mode, PILAR applies TSV values.

After determining which threats are relevant to each asset, let's rate them:



Top menu EDIT

Options	options – see *Edit_options*
copy	Select one or more value cells. Copy values to be pasted.
cut	Select one or more value cells. Cut values to be pasted.
paste	Select one or more destination cells. Paste the copied values. If the source range is 1 cell, and the destination covers several cells, the value is copied into all of them.

Top menu EXPORT

to CSV	Comma Separated Values (for excel)
to XML	eXtensible Markup Language

Top menu IMPORT

from XML	eXtensible Markup Language

Top menu TSV

TSV	See "*Threat Standard Values*
apply	apply tsv to selected assets / threats

Table

1		Click on checkboxes to check / uncheck. SHIFT-click to check a range. Click on column header to clear current selection.
2	**assets**	assets
3		shows the mode of each asset / threat: • red: manual, either one threat or all the threats for one asset • orange: within one asset, some threats are manual • transparent: automatic (TSV driven) In mix mode, click to change
4	**level**	This column presents likelihood. The format is decided at *Options / Likelihood*
5 …		These columns present degradation for each security dimension. The format is determined by *Options / Effects*

Bottom toolbar

	Spinner to control the expansion of the assets tree.
+1	Adjust the effect of the spinner. If +1 is checked, PILAR shows the threats associated to an asset. If unchecked, the threats are not expanded.
	Undo last changes.
	Redo last undone changes.
	Saves current project either in a file, or in database (according to its source).

NOTE. If *Options / Threats* are set to automatic, then some buttons are disabled:

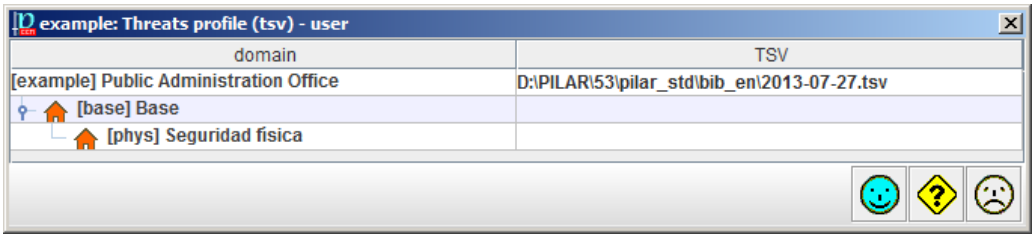
- copy & paste
- import from XML
- undo / redo

8.9.4 TSV – Threat Standard Values

You may edit threats manually or, much better, use a TSV file.

TSV files are explained under personalization in https://www.ar-tools.com/doc/

Either *identifying* threats or *valuating* them, you may click on TSV / LOAD to get a screen like this:



where you can specify a TSV file for the project, and different TSV files for different security domains. If a domain has no specific file, it uses the one of its enclosing domain, or the project file as a last resource.

For each asset, PILAR takes the security domain of the asset, and then finds the TSV file that applies.

The name and path of the TSV file(s) is stored along with the risk analysis project. When you open the project, PILAR tries to reload it, and checks that the file has not changed since it was last stored. PILAR complains if the process does not complete smoothly.

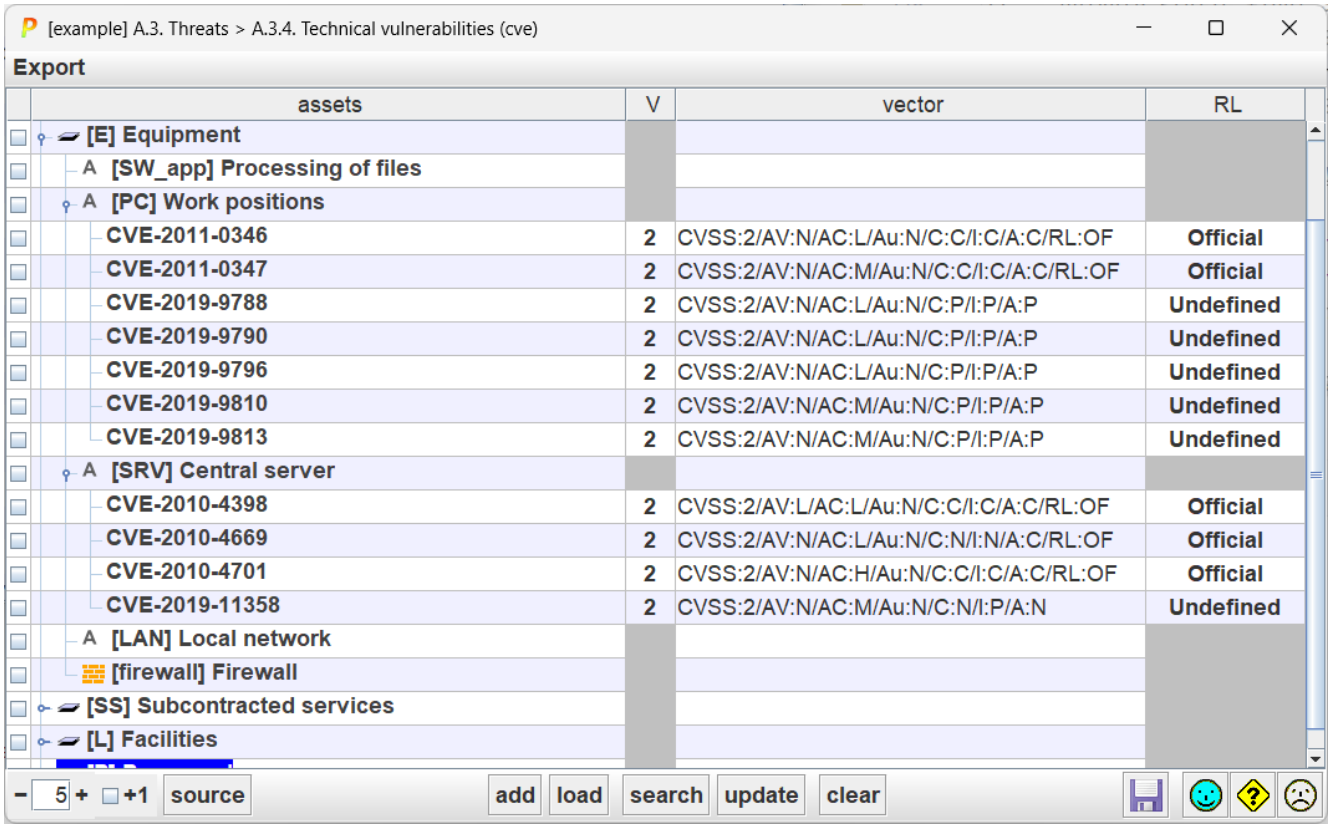
8.9.5 Technical vulnerabilities (CVE)

See

https://www.ar-tools.com/doc/

for information on CVE, and how PILAR uses them.

To associate CVE vulnerabilities to assets, assets may have *Assets / CPE* associated to them.



Table

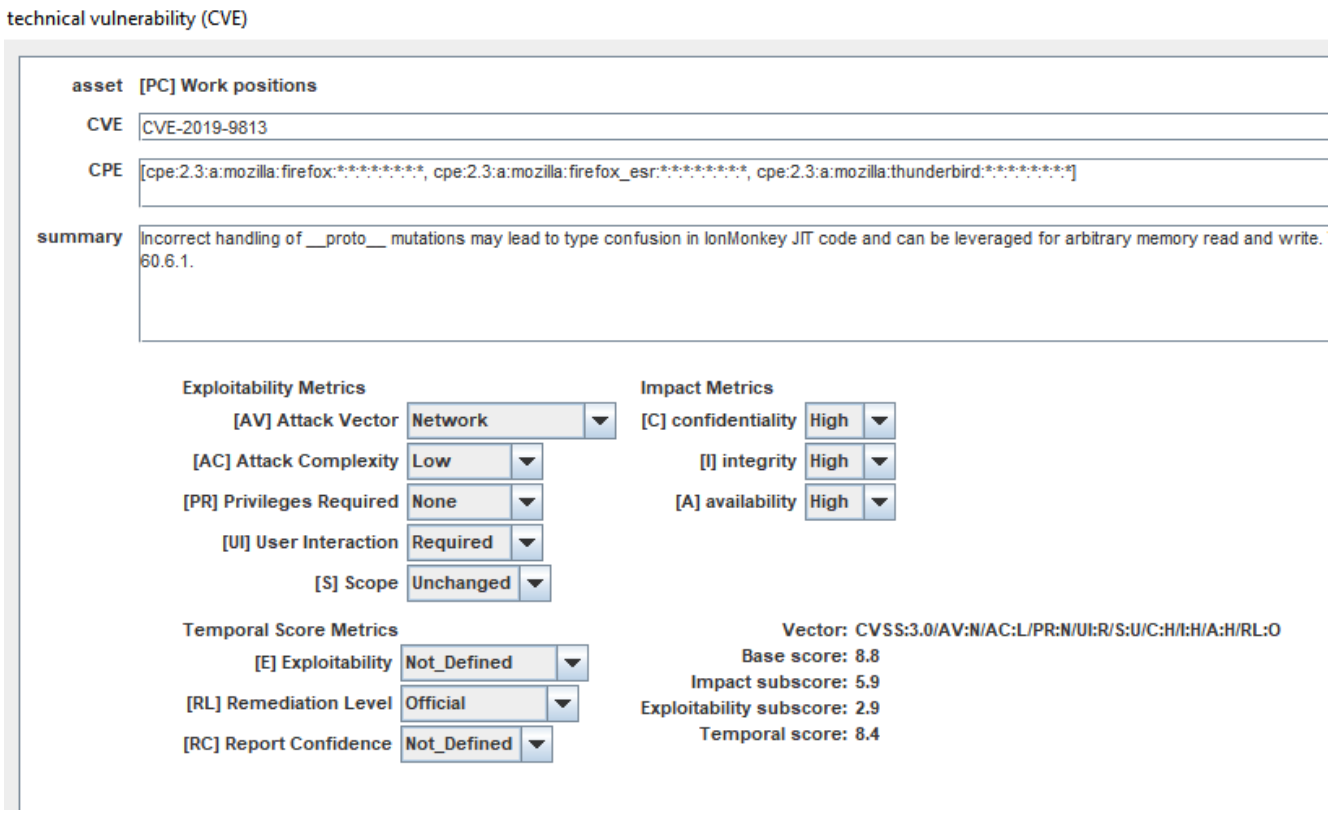
selection	Click on checkboxes to check / uncheck. SHIFT-click to check a range. Click on column header to clear current selection. Selection controls to which rows apply buttons ADD and SEARCH.
assets	A tree with the assets, and their associated CVE items.
Version	CVSS version; usually 2 or 3
vector	CVSS summary
RL	Remediation level (see CVSS)

Bottom toolbar

	Spinner to control the expansion of the assets tree.

+1	Adjust the effect of the spinner. If +1 is checked, PILAR shows the vulnerabilities CVE associated to an asset.
add	— Select one asset on left column. — Click ADD to introduce your vulnerability manually.
load	— Select one or more assets on the left column — click LOAD to associate a CVE read from an external file in XML or json format, according to NIST standard formats
search	— Select one or more assets on left column. — Click SEARCH PILAR loads vulnerabilities from the vulnerability database. To be precise, PILAR reads a file as those defined by the CVE project site for vulnerability distribution. The CPE names associated to the asset are used to discover matching vulnerabilities. You may use either XML or JSON standard formats.
update	Like SEARCH, but now the data from the database are updated into PILAR.
clear	— Select assets in the left column — Click CLEAR PILAR removes their associated vulnerabilities. Or — Select vulnerabilities in column — Click CLEAR PILAR removes the selected vulnerabilities from the corresponding assets.
	Saves current project either in a file, or in database (according to its source).

You may change these values by editing the vulnerability (double-click on the CVE name). You may edit CVSS version 3 parameters.



For backward compatibility, PILAR also supports CVSS version 2.

To enter a vulnerability manually

- select one or more assets
- click on ADD
- edit the data

To load a vulnerability for one or more assets

- select one or more assets
- click on LOAD
- choose XML or JSON file

To find vulnerabilities that apply to an asset

- select one or more assets
- click on SEARCH
- choose the XML or JSON file data

To update the vulnerabilities associated with an asset

- select one or more assets
- click on UPDATE
- choose the XML or JSON file data

To eliminate vulnerabilities associated with an asset

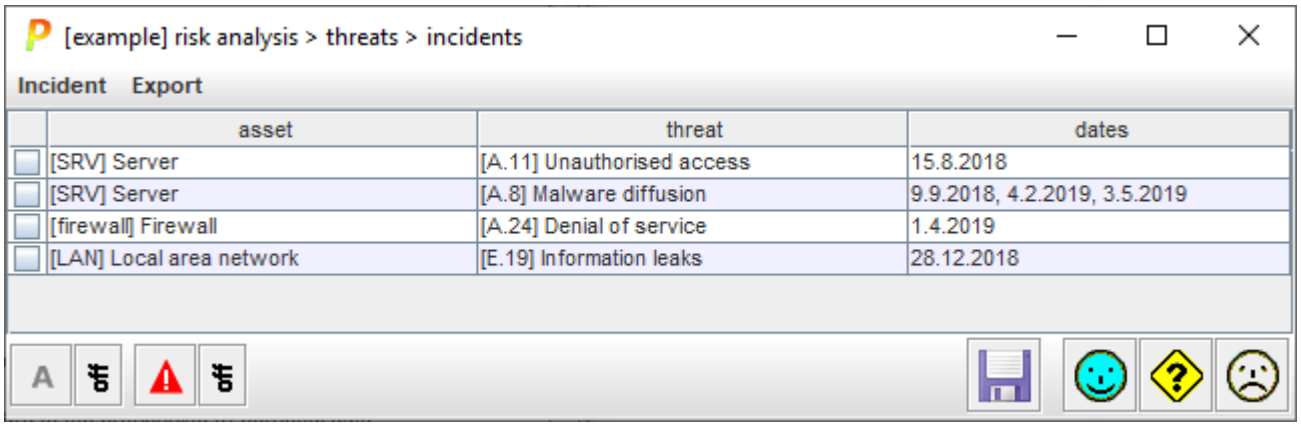
- select one or more assets
- click CLEAR

To edit the parameters characterizing a vulnerability associated with an asset

- double-click the vulnerability
- enter data in the edit screen

8.10 Incidents

You may make risk analysis more dynamic by inserting the observed incidents.



Top Menu

incident	new	create a new incident
	edit	edit an already existing incident: select on first column, then edit
	delete	remove an incident: select on first column, then delete
export	to CSV	what you see, to excel

Bottom bar

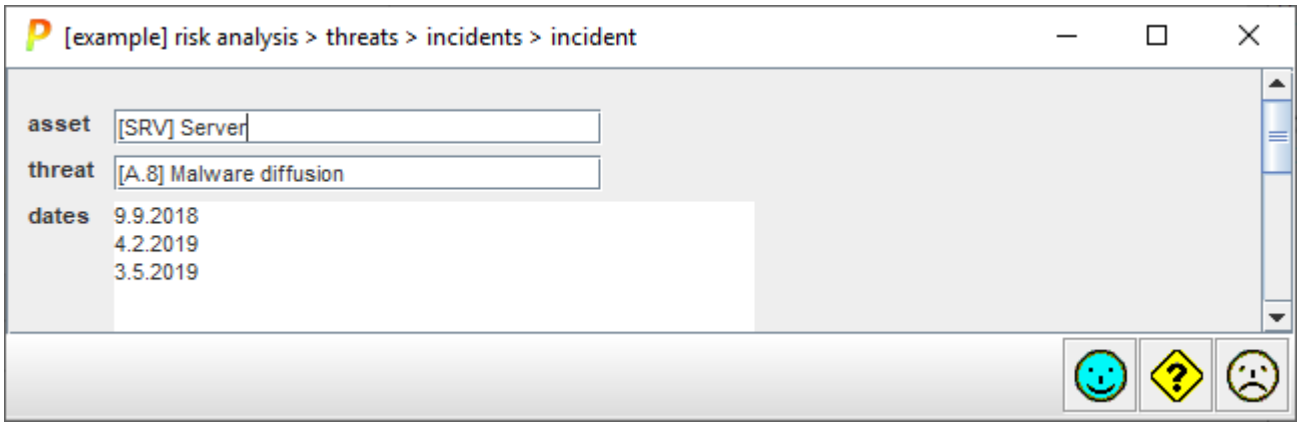
A off	You may select some assets, and activate the filter to see only those selected
off	You may select some threats, and activate the filter to see only those selected

You may click on headers to sort by asset, threat or last incident date.

PILAR will adapt threat likelihood to the reported incidents, overtaken data in TSV. This dynamic calculation of likelihood considers the observed rate of occurrence during the last year. In order to align incident dates with project phases, you need to associate a date to phases.

8.10.1 Edit one incident

Either on top menu (incident > edit) or double clicking on one line, you may edit one incident



Click on asset to select one asset. Click on threat to select one threat.

You may specify one or more dates when incidents occurred. The format is DAY.MONTH.YEAR. PILAR will sort by dates.

8.11 Safeguards

8.11.1 Aspect

Aspect the safeguard deals with:

- M for management
- T for technical
- PHY for physical security
- PER for personnel management

8.11.2 Type of protection

- 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 – procedure
- cert – certification or accreditation

8.11.3 Relative weight

Not every safeguard is equally important:

	highest weight	Critical.
	high weight	Very important.
	normal weight	Important.
	low weight	Interesting.
	assurance: certified components	

8.11.4 Hooks

Links may be associated to safeguards by means of hook-files. These are files in the library directory which name starts with the pattern “hooks-“. The content is formatted as **JSON**.

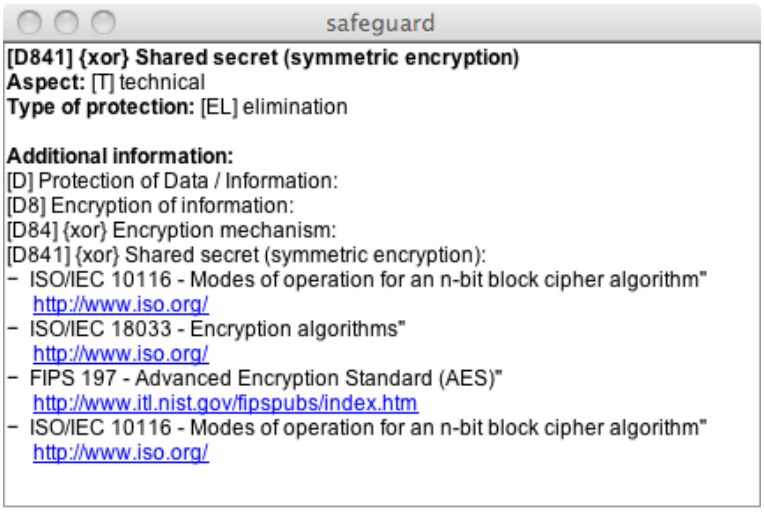
Let’s show an example:

/bib_en/hooks-sp800-53.json

```
{
  "encoding" : "áéíóú",
  "title" : "SP 800-53 rev.5",
  "defs" : [
    {
      "sm" : [ "ACb" ],
      "links" : [
        {
          "label" : "ACCESS CONTROL",
          "url" : "https://nvd.nist.gov/800-53/Rev4/family/ACCESS%20CONTROL"
        }
      ]
    },
    {
      "sm" : [ "AC-1", "AC-1(0)" ],
      "links" : [
        {
          "label" : "Policy and procedures",
          "url" : "https://nvd.nist.gov/800-53/Rev4/control/AC-1"
        }
      ]
    },
```

8.11.5 Additional information

Some more information for the safeguard is displayed in a new window. For instance:



8.11.6 On safeguards’ tree

When you right-click on the safeguards tree, you may …

edit

Presents a domain-phase view of the maturity values. See below.

copy

The code and name of the safeguard are copied onto the clipboard.

copy path

The code and name of the safeguard, and all her ancestors, are copied onto the clipboard.

full text

The code and name of the safeguard are presented in a new window.

full path

The code and name of the safeguard, and all her ancestors, are presented in a new window.

close father

The father of this node in the tree is collapsed.

close brothers

This node, and its brothers in the tree, are collapsed.

…

On some safeguards, PILAR can provide some more information.

When a safeguard is from SP800-53, or there is a relation to a security measure in SP800-53, PILAR jumps to the corresponding web information page. Since the web URL may change, the base URL can be modified in the configuration file:

`bib_xx/hooks-sp800-53.json`

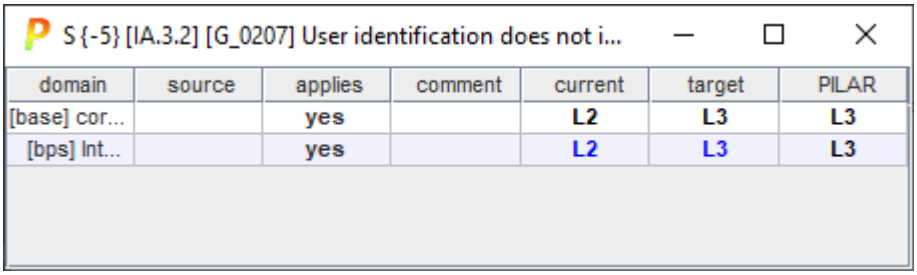
See *safeguards / hooks*

additional information

Some more information for the safeguard is displayed in a new window.

See "*Safeguards / Additional information*"

Domain-phase view. Clicking on a safeguard (right click > EDIT) you may have a one-safeguard view of maturity values covering all the domains and all the phases

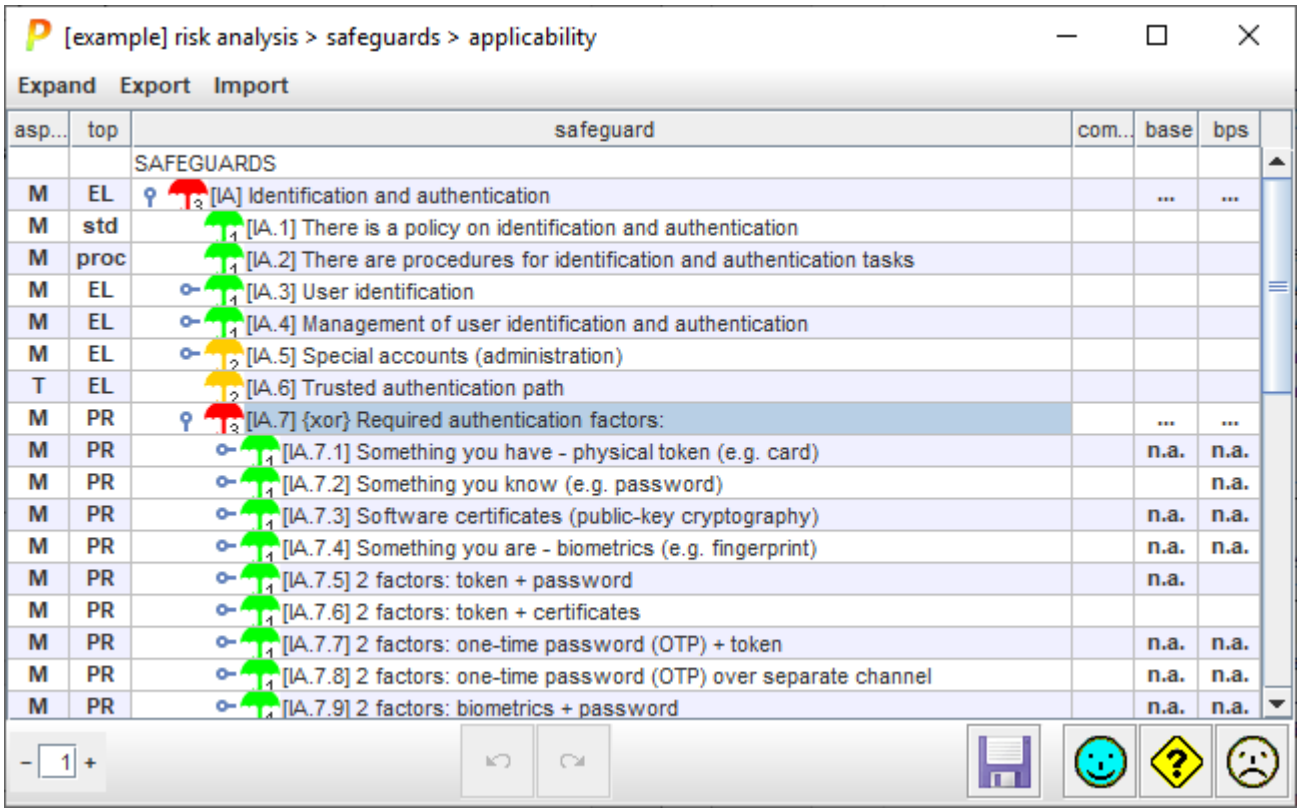


User values are in black over white; while calculated values are in cyan.

8.11.7 Applicability summary

This screen presents a summary of the safeguards that apply in each security domain.

It refers to the current applicability stage.



Please note that some safeguards may be later disabled per project phase.

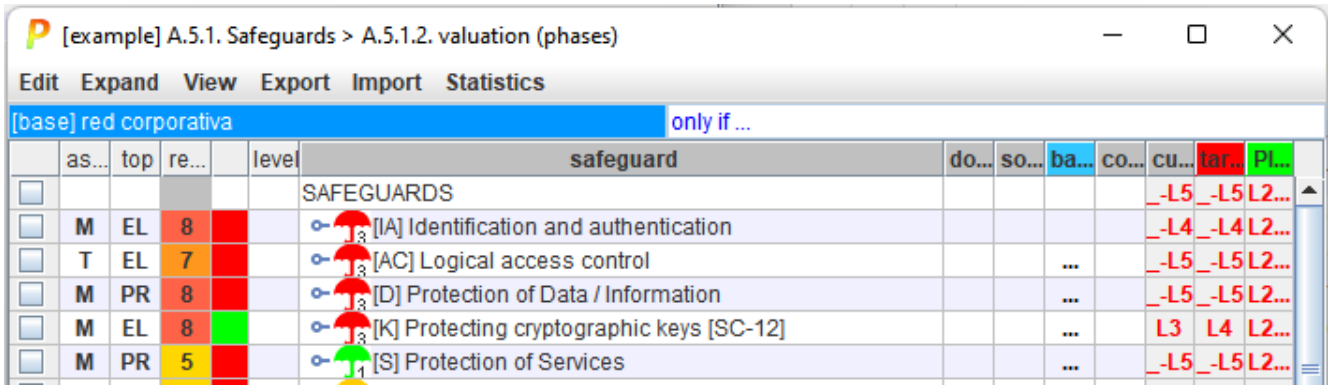
8.11.8 Valuation (phases)

Quick start

1. Go to the cell at row **SAFEGUARDS**, and column **CURRENT**. Select it.
2. Right click and select the maturity level that roughly matches your system (for example L2).
3. You can visit safeguards below, to any level of detail, and refine you overall estimate.

If you have a plan in mind …

4. Go to the cell at row SAFEGUARDS, and column TARGET. Select it.
5. Right click and select the maturity level that you aim to.



Top menu EDIT

copy	the maturities selected are copied onto the clipboard
paste	The maturities in the clipboard are pasted on the cells selected
find	See "*Safeguards / Find*" below.

Top menu EXPAND

unevaluated safeguards	expands the tree down to safeguards that are not evaluated
recommendation = 0	expands the tree down to safeguards which recommendation is grey
n.a.	expands the tree down to safeguards marked as n.a.;
{xor}	expands the tree down to the safeguards that are mutually exclusive; candidates for selections
doubts	expand the tree down to safeguards marked with doubts
selection	within XOR nodes, expand to the selected child
perimeter	see *Perimeters*

Top menu EXPORT

SoA	*SOA – Statement of Applicability*
to CSV	The visible rows are copied to a CSV file; for excel. There are 2 formats. A simple one is useful for human readers; while the second one is structured in such a way that you may edit externally and reimport it into PILAR.
to XML	The visible rows are copied to an XML file
report	The values are copied to a textual file (RTF or HTML)
< Lx	A report is generated with the safeguards below a given threshold
< target	A report is generated with the safeguards below target phase.

	See "*Safeguards / Reference and target phases*" below.

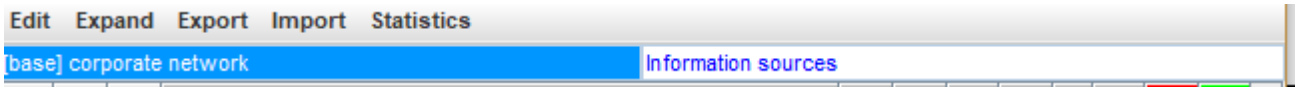
Top menu IMPORT

from CSV	Read maturity values from a CSV file
from XML	Read maturity values from an XML file
import (mgr)	
import (db)	

Top menu STATISTICS

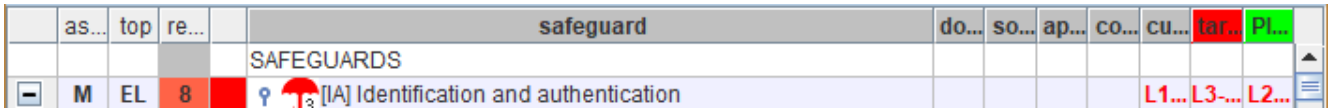
by domain	Generates a summary of the evaluated safeguards by security domain.

Top bands



security domain	There may be different safeguards for different domains. Click to select the domain you want to edit.
only if …	Click to select some safeguards based on attributes. After that, PILAR will prune the tree to show only the parts of the tree related to the selected items. You may select different criteria to match • safeguards that apply or that do not apply • information sources • countermeasure level

8.11.8.1 Central table



1		Selection
2	**aspect**	See "*Safeguards / Aspect*".
3	**top**	See "*Safeguards / Type of protection*".
4	**recommendation**	It is a rank in the range [null .. 10], estimated by PILAR considering 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 safeguard. That is, PILAR does not know which risk this safeguard is good for.

		(o) - PILAR thinks it is an overkill ("too much"). (u) - PILAR thinks it is an under-kill ("not enough"). Right-click to open a new window with a summary of the rational for the recommendation; that is, the assets and dimensions to which the safeguard will apply.
5	**traffic light**	See "*Safeguards / Reference and target phases*" below.
6		Safeguards tree. You double click to collapse / expand the tree. You may right-click to access to "*Safeguards / tree*".
7	**doubts**	Click to mark / unmark the row. The mark is typically used to remember that there are issues waiting for an answer. The mark "floats" to the top level to highlight the problem.
8	**sources**	Click to associate information sources to the safeguard and its children.
9	**applicability**	All safeguards apply by default. Nevertheless, you may mark safeguards as not applicable. It implies that PILAR will ignore them. Ignoring safeguards is somehow risky in the sense that you may inhibit PILAR from working with measures that are useful. Non-applicability shall be justified, and the reason recorded as a comment.
10	**comment**	Click to associate comments to the safeguard.
…		Project phases. See "*Safeguards / Maturity valuation*" below.

On applicability

- left click
  - to select / unselect; if a countermeasure is marked as not applicable, all of its children become not applicable; if some children apply and some do not, the countermeasures above are marked as "…".
- right click

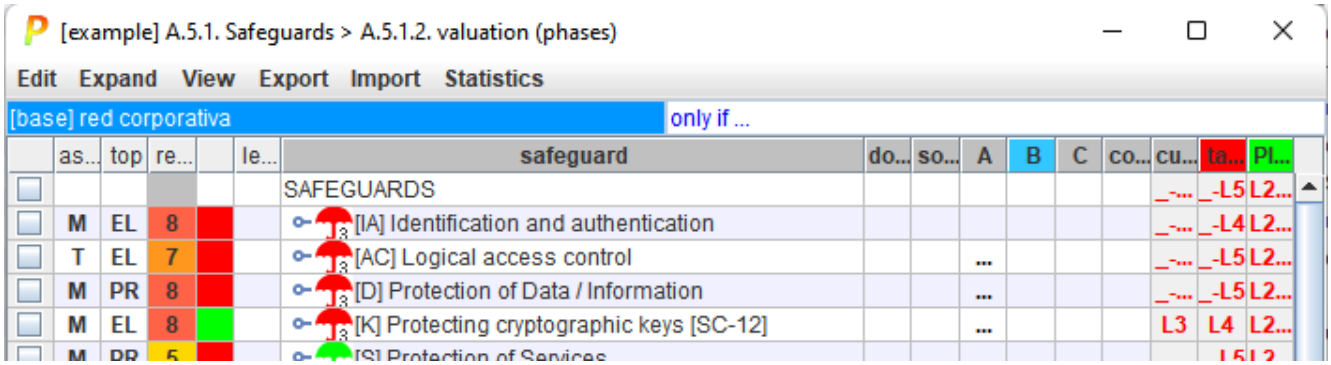
clear	remove all applicability marks
recommendation	follows recommendation; that is all safeguards that are not recommended are marked as n.a.
only if …	retains only safeguards mapped from one or more security profiles
n.a.	mark every safeguard as n.a.
push down values	applicability is copied to other security domains under current one
copy	applicability values are copied from security domain above

Example. If we have 2 security domains: A on top of B, then

- when presenting A, push-down-values translates applicability values from A to B
- when presenting B, copy translates applicability values from A to B

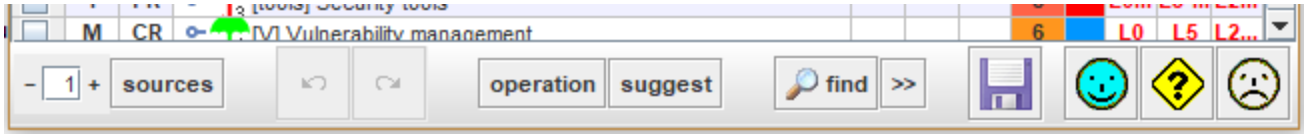
Applicability stages

When there are more than one applicability stages, the previous options apply independently to each one. You will have a column for each stage, while the current stage is highlighted in blue



You may click on applicability stage headers to select the current one.

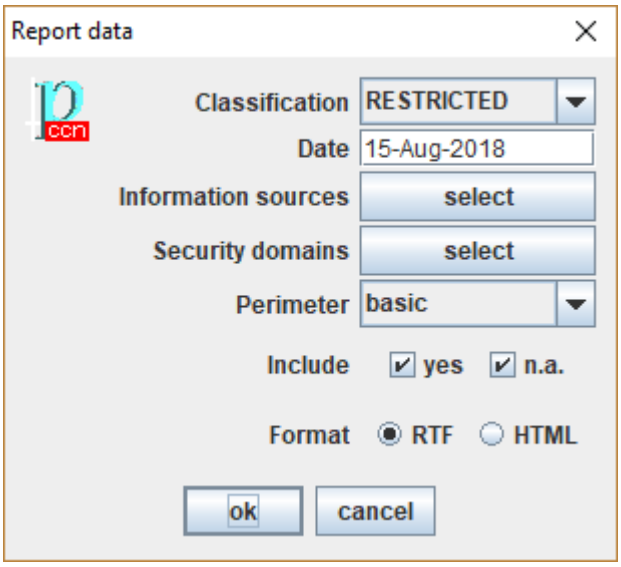
8.11.8.2 Bottom tool bar



	Spinner to control the expansion of the safeguards tree.
sources	Select one or more sources, and PILAR will select the safeguards associated to them.
	Undo last changes.
	Redo last undone changes.
operation	See "*Safeguards / Valuation / Operations*"
suggest	See "*Safeguards / Suggest*"
	See "*Safeguards / Find*"
>>	See "*Safeguards / Find*"
	Saves current project either in a file, or in database (according to its source).

8.11.8.3 SoA – Statement of Applicability

It is a relevant document for some auditors and auditing practices. It collects the safeguards that apply or not.



It is important to know what applies in order to focus inspection on those that apply.

It is also important to know what does not apply, since auditors might disagree.

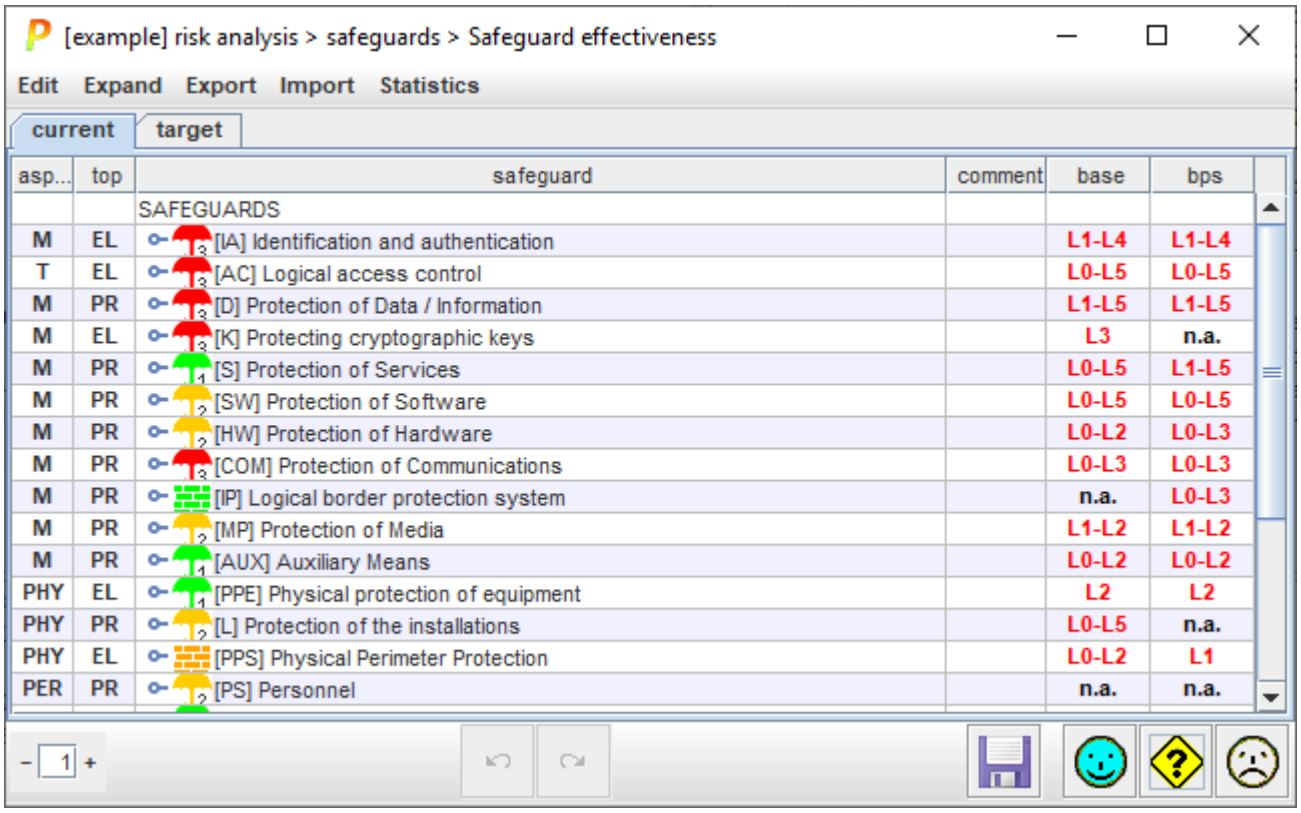
Sometimes, "n.a." means that the safeguard would apply, but it is not justified (the risk does not justify the resources needed).

Fields explained:

Classification	Establishes the marking of the report. A minimal marking is established in the *Project data*. Here you can raise it.
Date	Default date for the report is TODAY.
Information sources	if marked, filter by information source
Security domains	You may select a few security domains to be used in the report. By default, all domains are printed.
Perimeter	See *Perimeters*
Include	You may include the safeguards that apply, those that do not apply, or all of them
Format	PILAR generates either RTF for documents, or HTML for intranet.

8.11.9 Valuation (domains)

Quite like "*Valuation of safeguards per domain*" but now columns are security domains, and tabs are project phases.



8.11.10 Reference and target phases

The traffic light gives a fast indication on whether the level of maturity is enough or not.

To calculate the colour of the light, PILAR uses 2 references:

GREEN: target maturity

- click the right button at the header of the phase to use as target

the head of the selected column is painted GREEN

RED: assessed maturity

- click on the header of the phase you want to evaluate

the header of the selected phase becomes RED

Using the above information, PILAR chooses a colour:

traffic light colour code	
BLUE	if the maturity at the RED phase is higher than the maturity at the GREEN phase
GREEN	RED maturity is aligned with target
YELLOW	the RED maturity is poor: should be enhanced
RED	the RED maturity is too poor: must be enhanced
GREY	if the safeguard does not apply

Here you have an example.

The red phase, 3m is the assessed phase.

The green phase, PILAR, is the target phase.

The traffic lights, first column, follow the difference between phases red and green.

	current	3m	1y	target	PILAR
		_-L5	_-L5	_-L5	L4-L5
					L4
		L0			L4
		L1			L5
		L2			L4
		L3			L4
		L4			L4
		L5			L4
		L4			L4
		L4			L4

8.11.11 Safeguard maturity valuation

The cells collect the maturity of each safeguard in each project phase.

The value is either a maturity level L0 – L5, or n.a. (not applies), or empty. For mathematical purposes, "n.a." is not taken into account.

If a cell is empty, PILAR will reuse the level in the previous phase or in the next security domain (See "*Options / Security domains and project phases*". If after that search the cell is still empty, PILAR uses the value specified in "*Risk treatment*".

Maturity levels are assigned to single safeguards, black text. For groups of safeguards, PILAR shows the range (min-max) ignoring cells that do not apply (n.a.). The aggregation in ranges propagates upwards the tree up to the top level.

colour code	
red characters	when the value is calculated from others
black on white	when the value is explicit
black on yellow	when the value comes from a security domain below

To change a value in a cell, you may

- right-click and choose
- select a maturity in the maturity combos in the bottom tool bar
- select one or more cells (rows and columns), and use EDIT menu to copy & paste

On the valuation cells, you may move maturity value from one phase, security domain, or project to another:

copy tree

PILAR copies the maturity of the cells in the current row, and in the corresponding sub-tree, to be pasted later

paste tree

PILAR pastes the values copied before

Note that the values can go from one phase to another phase, from one domain to another, and even from one project to another project; but they always apply to the same sub-tree.

Please, note as well that copy-paste only works within the application. You may not copy in PILAR and paste in another application.

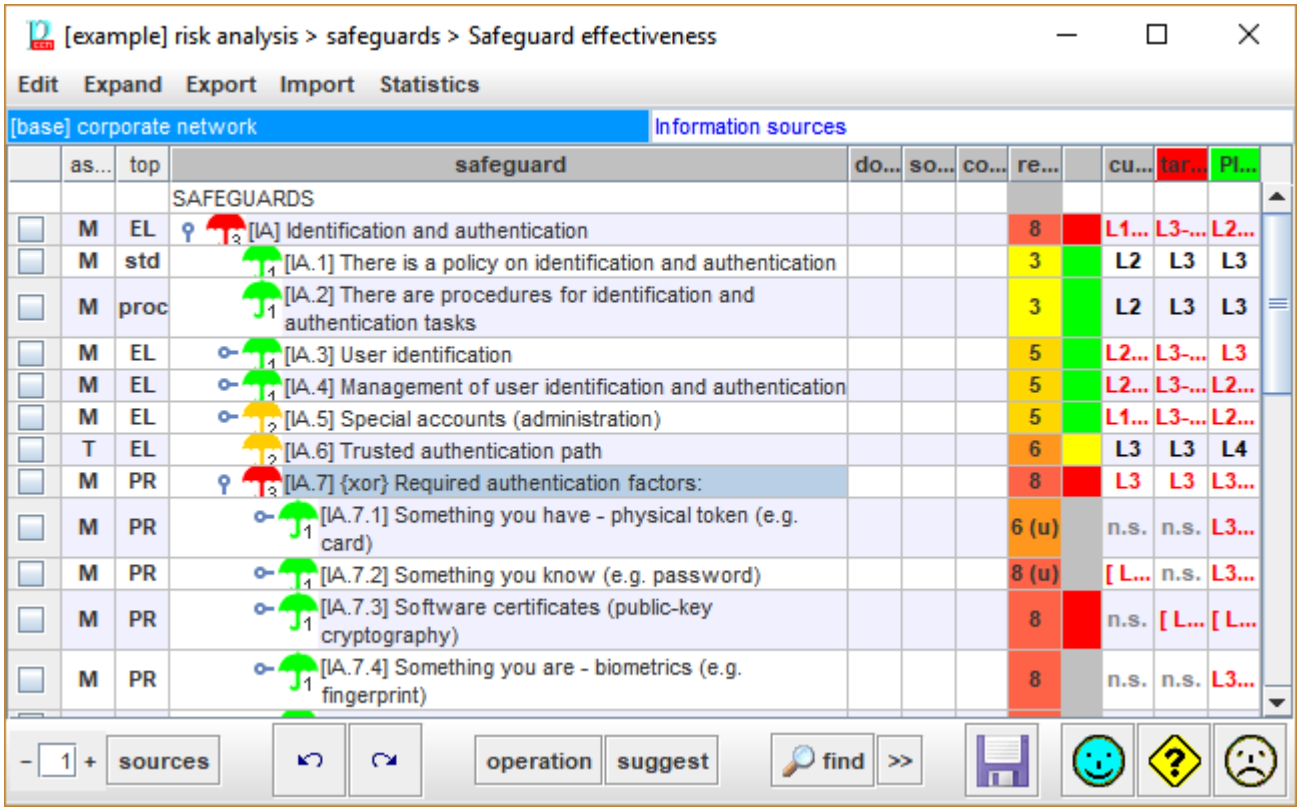
XOR safeguards

When a tree branch is labelled as XOR, you may choose which one of its children is the one to take into account.

right-click > select

In the example below, for the I&A mechanism, we have selected

- passwords in phase ‘current’
- token + password in phase ‘target’



The other children are marked as n.s. (not selected).

8.11.12 Operation combo

PILAR can apply a set of standard operations to cells selected from the columns for maturity assessment.

APPLY

applies the selected maturity value to the selected cell(s)

FILL

applies the selected maturity value to the selected cell(s) if empty

PREDICT

looks around and fills empty cells with an average maturity;

it is useful when new versions of the tool introduce new items that are likely to deserve the same maturity as items around

SIMPLIFY

removes values that may be inherited either from the domain below or from the phase before;

it is useful if you plan to change the relative order of phases

MINIMAL

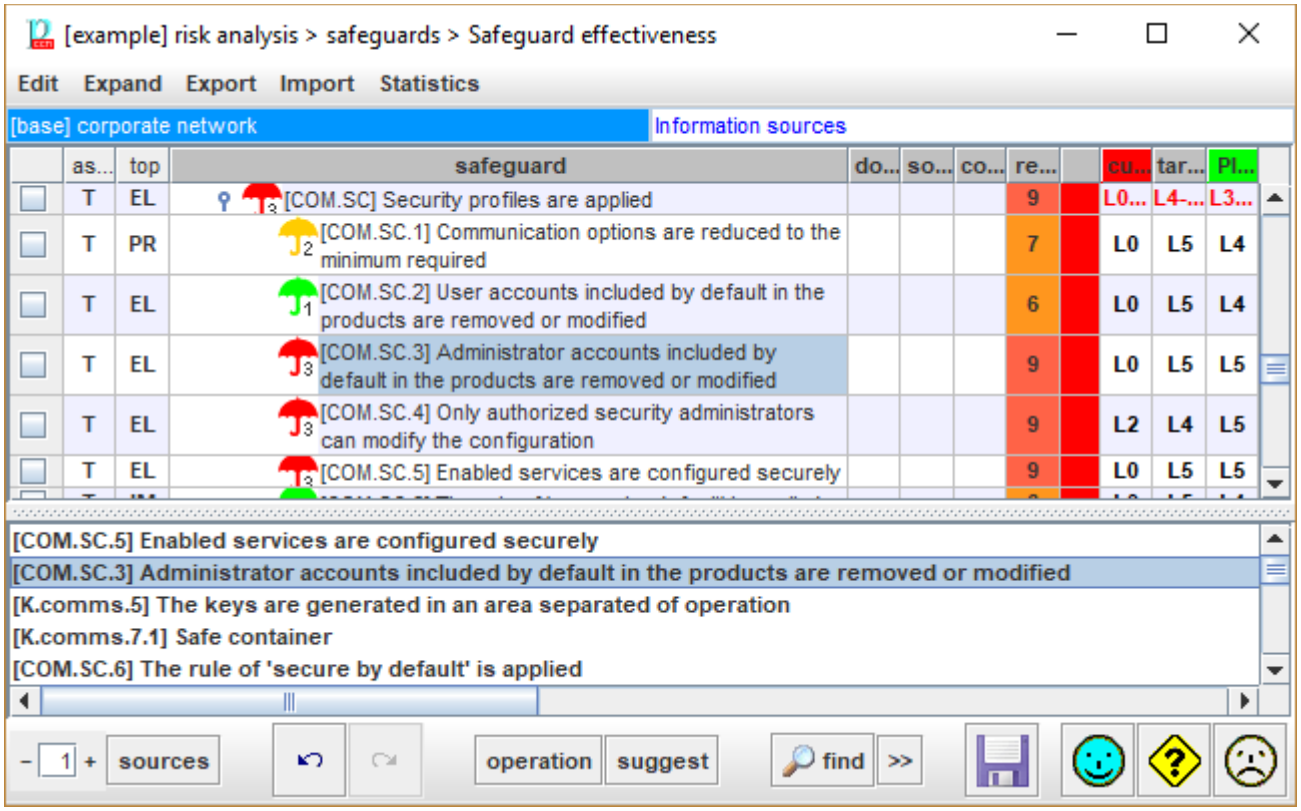
taking into account the recommendation, PILAR suggests that maturity values considered minimum to meet the needs of the system. Merely heuristic, with the intention of making a reference below which should not operate the system

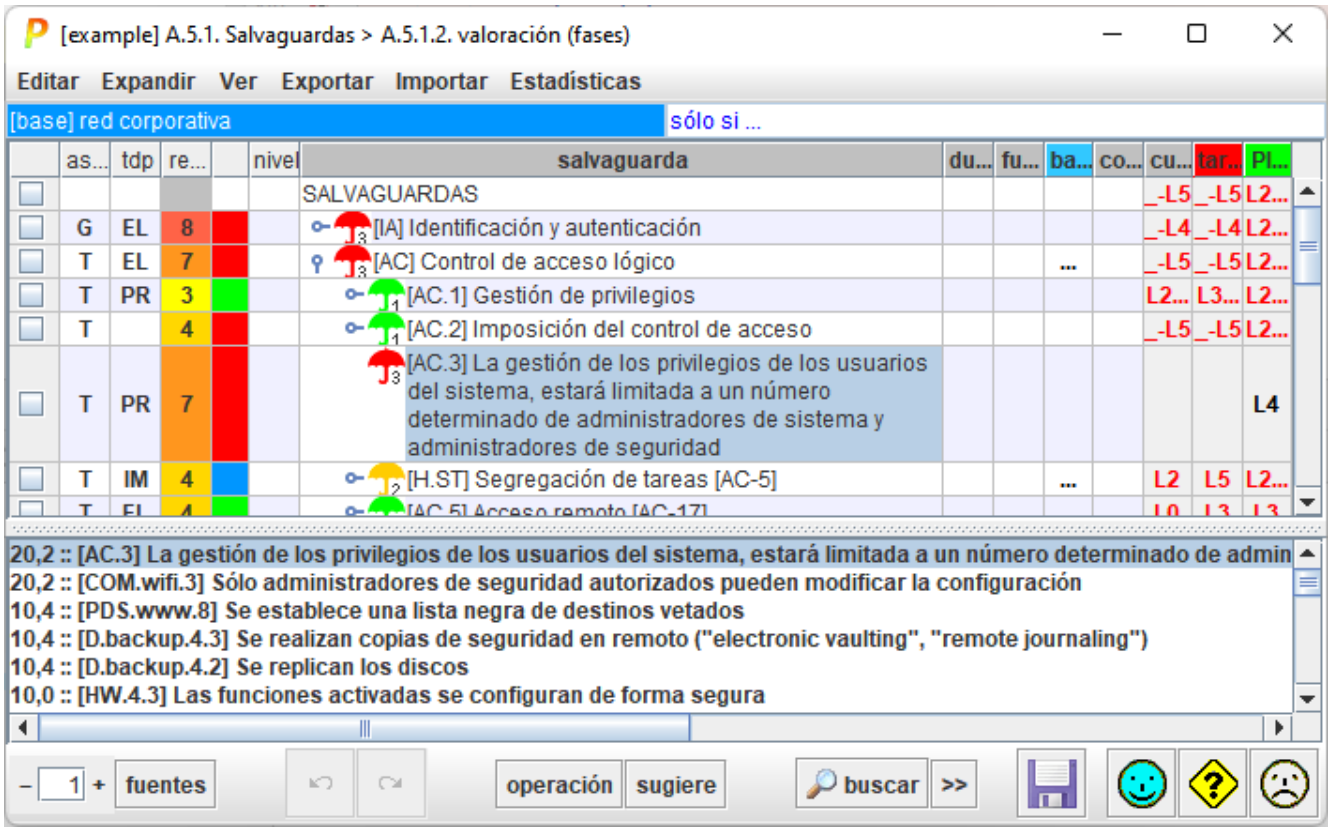
RECOMMENDATION

taking into account the recommendation, PILAR suggests a maturity values that it considers adequate to meet the needs of the system. Merely heuristic, with the intention of making a decent reference to operate the system

8.11.13 Suggest operation

Select a project phase: click on the header column, which shall become RED. Click on SUGGEST. PILAR splits the window so that in the bottom pane there is a list of safeguards, sorted by interest. Interest is a ranking assigned by PILAR based on the safeguard recommendation and current maturity. Click on the safeguard to locate it on the top panel.





8.11.14 Find

PILAR can search through safeguards using certain criteria:

CHANGES (phases | domains)

jumps along the tree, stopping at safeguards that change from one (phase | domain) to another

WORSENING

looks for safeguards which value decreases when we move along increasing phases

THRESHOLD

generates a report with the safeguards below a given maturity threshold

< TARGET

looks for safeguards which maturity is below the maturity in the target column (the column with the green header)

N.A.

looks for safeguards which are valued as “n.a.” (not applicable) in some phase

UNEVAUATED SAFEGUARDS

looks for unevaluated safeguards (white hole)

XOR

looks for xor-safeguards, those where you have to select an option

COMMENT

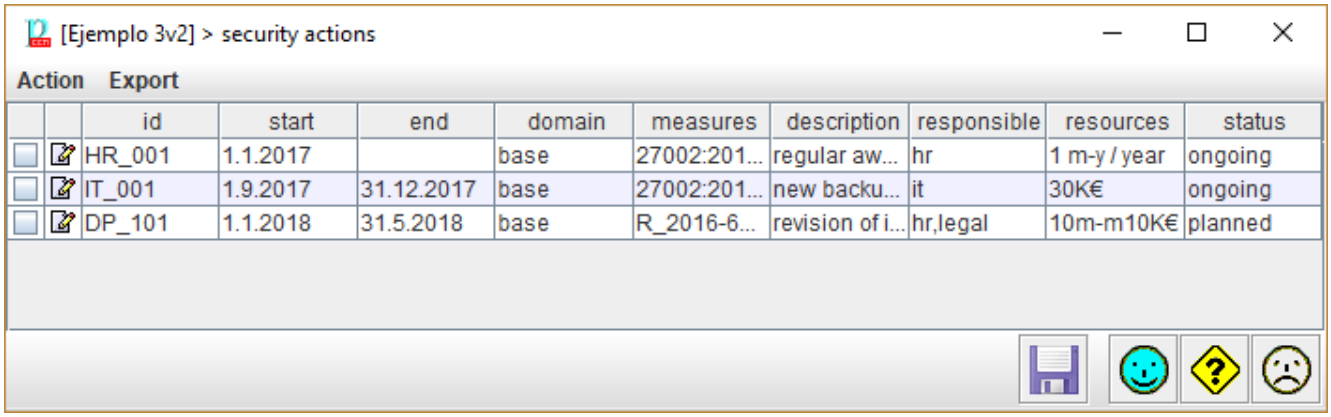
looks for safeguards with comments

>>

repeats the last find operation from the current position of the cursor

8.12 Security actions

PILAR allows the identification of security actions that are activities with a beginning and an end that act on a subset of safeguards or controls. This grouping does not change the mathematical calculations of risk, it simply allows a project management approach.



Top toolbar

Action	**new** to create a new row **edit** to modify a row **delete** to delete a row
Export	**CSV** table to CSV for Excel **XML** table to XML

Bottom toolbar

	Saves current project either in a file, or in database (according to its source).
	OK. The changes are saved, and the screen is closed.
	CANCEL. The changes are undone, and the screen is closed.
	HELP. Jumps into this help files.

Table

	Allows you to select some rows; click to select or forget; with the shift key you

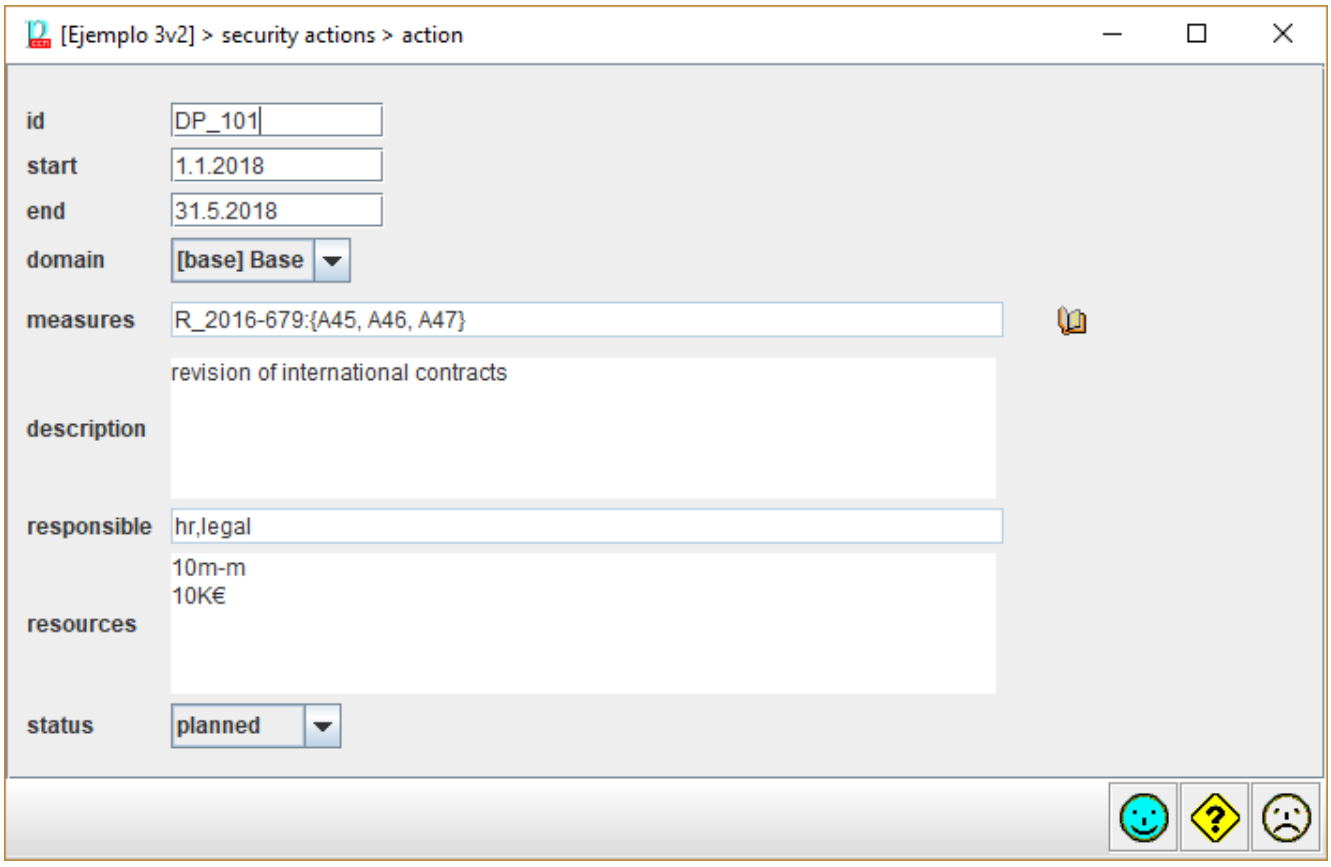
	can select a range
	Click to edit the row
id	Row identifier; it should be a unique identifier, without duplicates
start	Starting date. Format day.month.year.
end	Final date. Format day.month.year.
domain	Security domain.
measures	References security measures, either safeguards or profile controls
description	A textual description.
responsible	Reference to information sources
resources	Textual description of the resources required, typically human and economic effort.
status	{ planned, ongoing, suspended, done }

You may SHIFT-UP to move one or more selected actions one step upwards.

You may SHIFT-DOWN to move one or more selected actions one step downwards.

8.12.1 Security action

It allows entering data describing the action.



id

Row identifier; it should be a unique identifier, without duplicates

start

Starting date. Format day.month.year; example: 21.12.2002

fin

Final date. Format day.month.year; example: 21.12.2002

measures

click to select security measures; they can be technical safeguards or controls from some evaluation profile

Click to assess the maturity of selected safeguards and controls

domain

select the security domain on which you act

description

describe the actuation; free text

responsible

reference information sources

resources

Textual description of the resources required, typically human and economic effort; free text

status

{ planned, ongoing, suspended, done }

8.13 Risk scenarios

In its classic version, PILAR associates ICT threats with system assets, threats that affect ICT dimensions (confidentiality, integrity, etc.) and calculates the mitigating effect of ICT security measures to estimate residual risk.

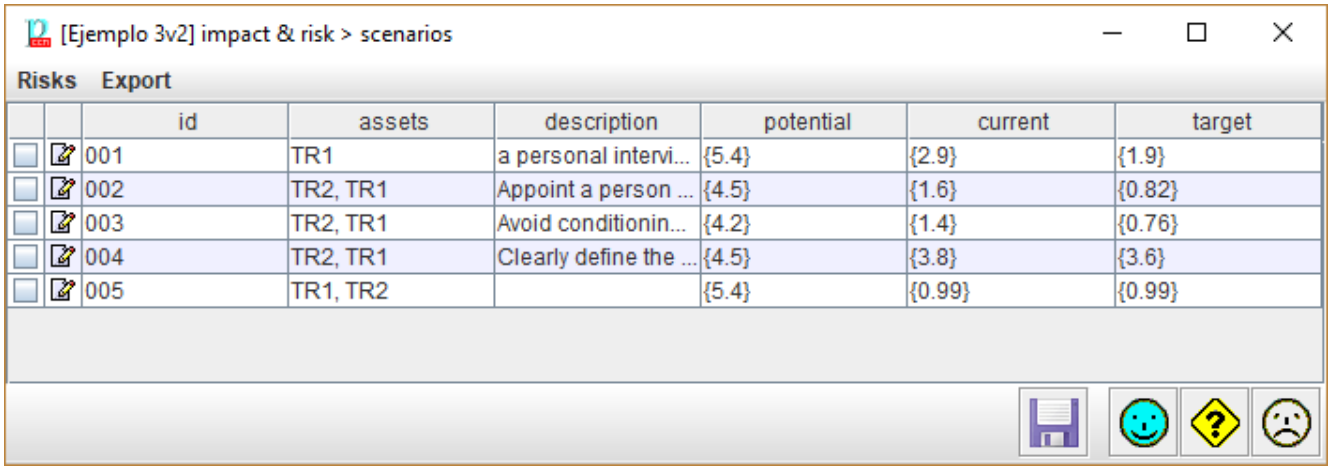
The same approach:

$$\frac{assets \times threats}{security\ measures}$$

can be applied in wider scenarios. In what follows we will apply it to the legal aspects (legal risk) of the assets that have value because of their personal character.

The approach is to associate threats on the legal aspects of the processing of personal data and apply measures that address such threats.

The value is determined by the valuation of the asset in the privacy dimension. The threat must be identified together with its impact on the value of the asset and the estimated probability of occurrence (ARO). The measures that are adopted reduce the risk. All this within the unified framework for estimating potential and residual risks.



Top toolbar

Risk	**new** to create a new row **edit** to modify a row **delete** to delete a row
Export	**CSV** table to CSV for Excel **XML** table to XML

Bottom toolbar

	Saves current project either in a file, or in database (according to its source).
	OK. The changes are saved, and the screen is closed.
	CANCEL. The changes are undone, and the screen is closed.
	HELP. Jumps into this help files.

Table

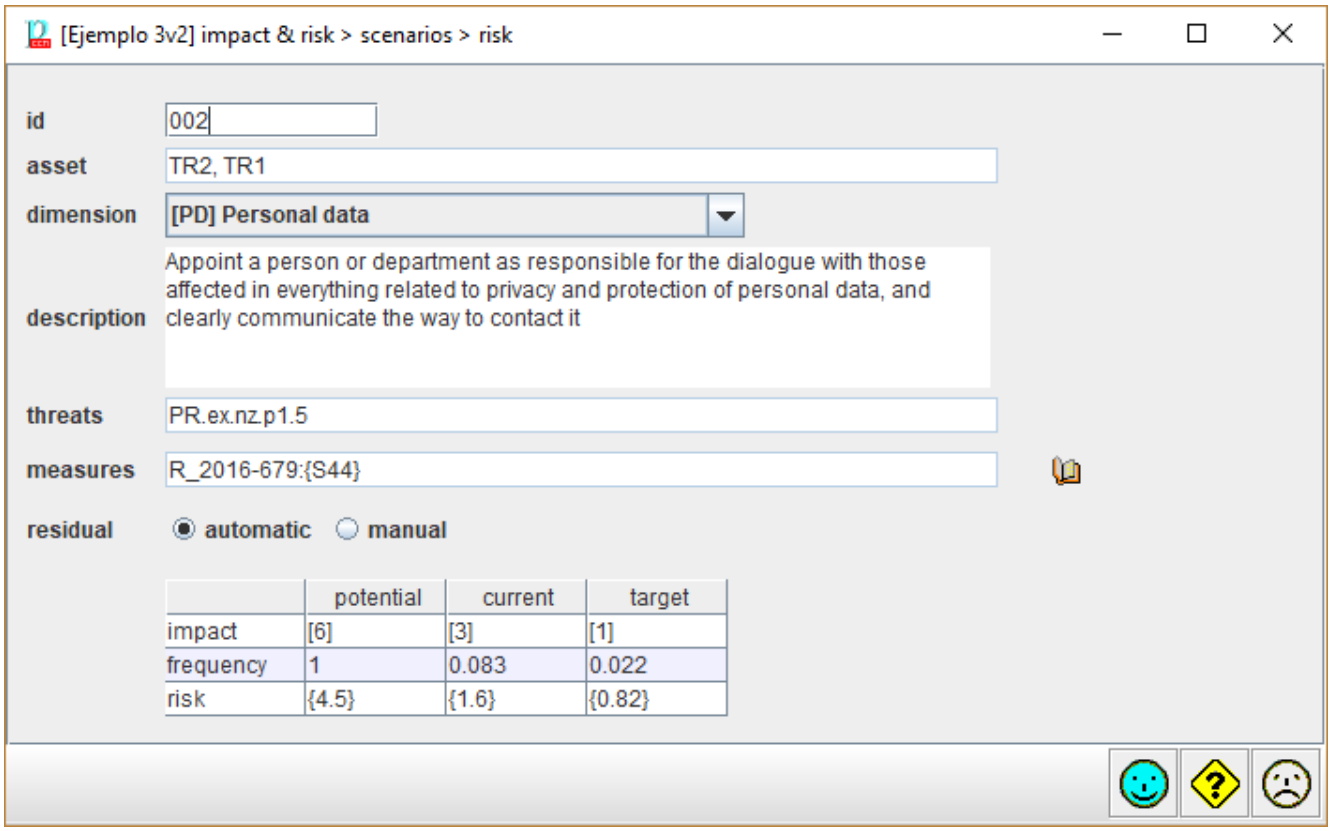
	Allows you to select some rows; click to select or forget; with the shift key you can select a range
	Click to edit the row
id	Row identifier: it should be a unique identifier, without duplicates
assets	One or more assets involved in the described scenario.
description	A textual description. It shall describe both the threat scenario and the measures to counter it.
phases	As many columns as projects phases, starting with the potential phase (inherent risk). It shows the residual risk in each phase.

You may SHIFT-UP to move one or more selected scenarios one step upwards.

You may SHIFT-DOWN to move one or more selected scenarios one step downwards.

8.13.1 Edit one risk scenario

It allows entering data describing the risk scenario.



id

Row identifier; it should be a unique identifier, without duplicates

asset

Click to select one or more assets involved in the described scenario.

dimension

Click on combo to select the affected dimension.

description

Describe the actuation; free text; it shall describe the threats, and the measures to counter them.

threats

Click to select one or more threats from the catalogue of PILAR.

measures

click to select security measures; they can be technical safeguards or controls from some evaluation profile

Click to assess the maturity of selected safeguards and controls

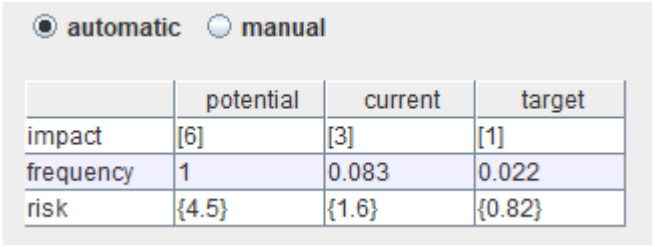
residual

Risk evaluation may be automatic or manual.

To select safeguards and controls, PILAR can suggest elements that seem appropriate for the dimension and threat used. It is just a suggestion.

8.13.2 Automated estimation of residual risk

Once the safeguards and controls have been selected with an effect on the described scenario, we can see their valuation in terms of maturity ( ) and ask to apply that maturity as a risk mitigator. This, for each phase of the project, including the pseudo recommendation phase of PILAR.



	potential	current	target
impact	[6]	[3]	[1]
frequency	1	0.083	0.022
risk	{4.5}	{1.6}	{0.82}

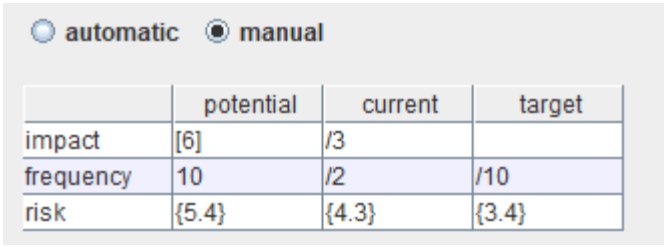
The potential impact is the value assigned to the asset in the dimension concerned.

The potential frequency is entered manually.

PILAR calculates the other entries in the table.

8.13.3 Manual calculus of residual risk

In manual mode, we will indicate to what extent the impact and probability are reduced in each phase of the project



	potential	current	target
impact	[6]	/3	
frequency	10	/2	/10
risk	{5.4}	{4.3}	{3.4}

The potential impact is the value assigned to the asset in the dimension concerned.

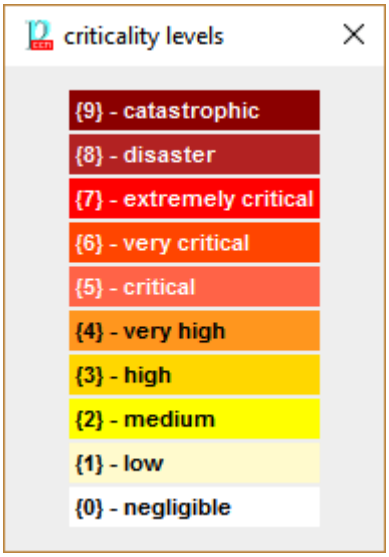
The potential frequency is entered manually.

In each phase, we can indicate the estimated reduction. The most normal approach is to apply a reducing ratio. PILAR calculates the risk given the estimated impact and likelihood.

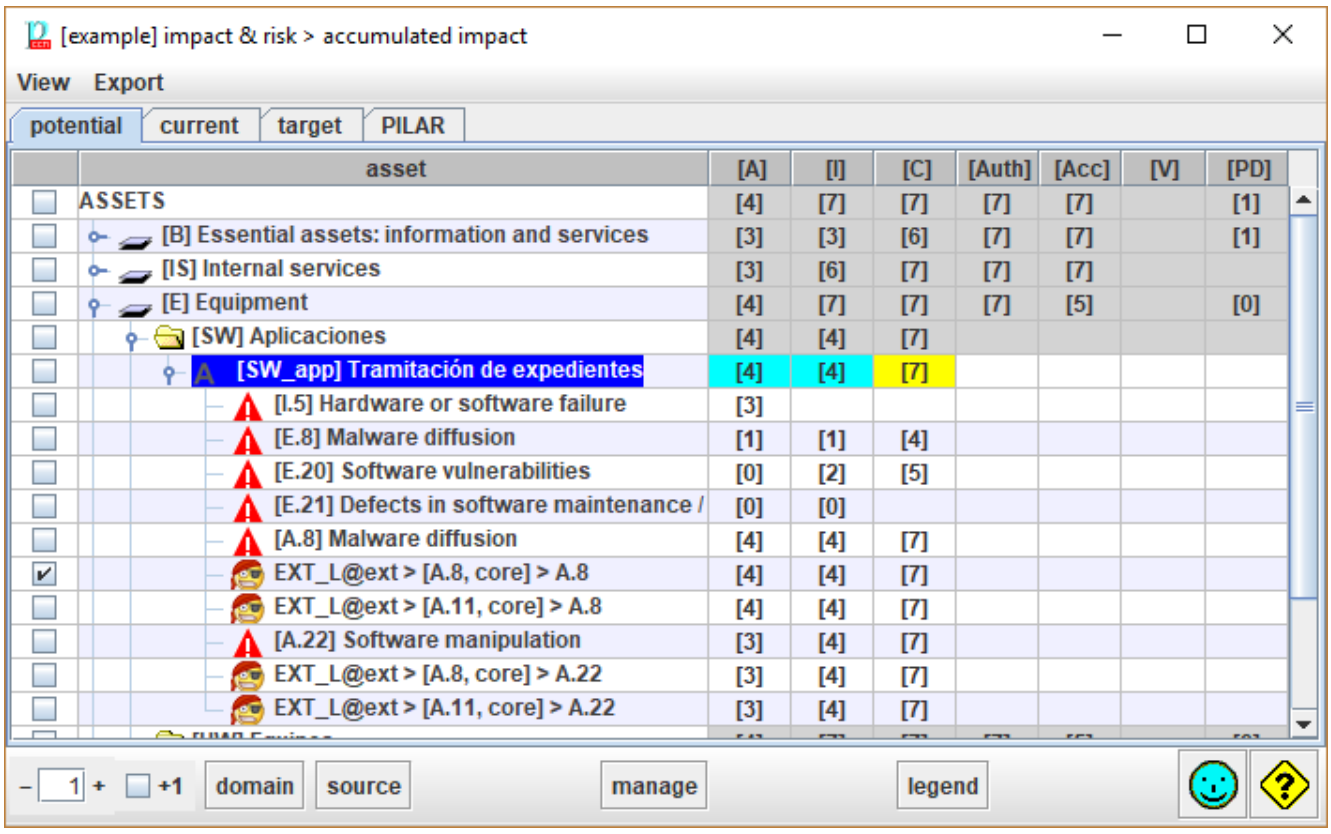
8.14 Impact & risk

8.14.1 Criticality levels – Colour encoding

PILAR presents risk levels as criticality levels, in the range 0.00 to 9.9, with a colour to enhance visibility:



8.14.2 Accumulated impact



There is one tab per project phase. Click to switch.

Pseudo phase “potential” shows inherent impact without safeguards.

Top menu VIEW

layers	tree organized by layers, then assets
logical zones	tree organized by logical zones, then assets
physical zones	tree organized by physical zones, then assets
threats	tree organized by threats, then assets

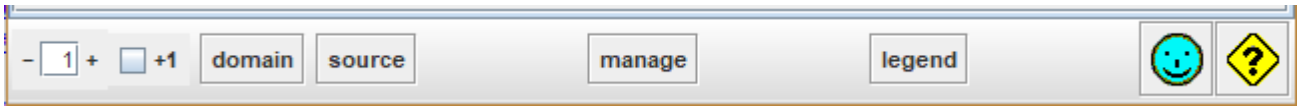
Top menu EXPORT

html	Exports selected rows to an html file for the web.
csv	Exports selected rows to a csv file for excel.
xml	Exports values to an xml file.
db	Exports values to a database. Only if the license enables the usage of SQL.

Table columns

selection	Click on checkboxes to check / uncheck. SHIFT-click to check a range. Click on column header to clear current selection. Selects rows to manage (see below)
assets	Assets and threats
dimensions	One column per security dimension. Click on header to switch to *alternate view*
	Impact value. Impacts are evaluated on threats, and summarised for assets, groups of assets, layers, and whole project.

Bottom toolbar

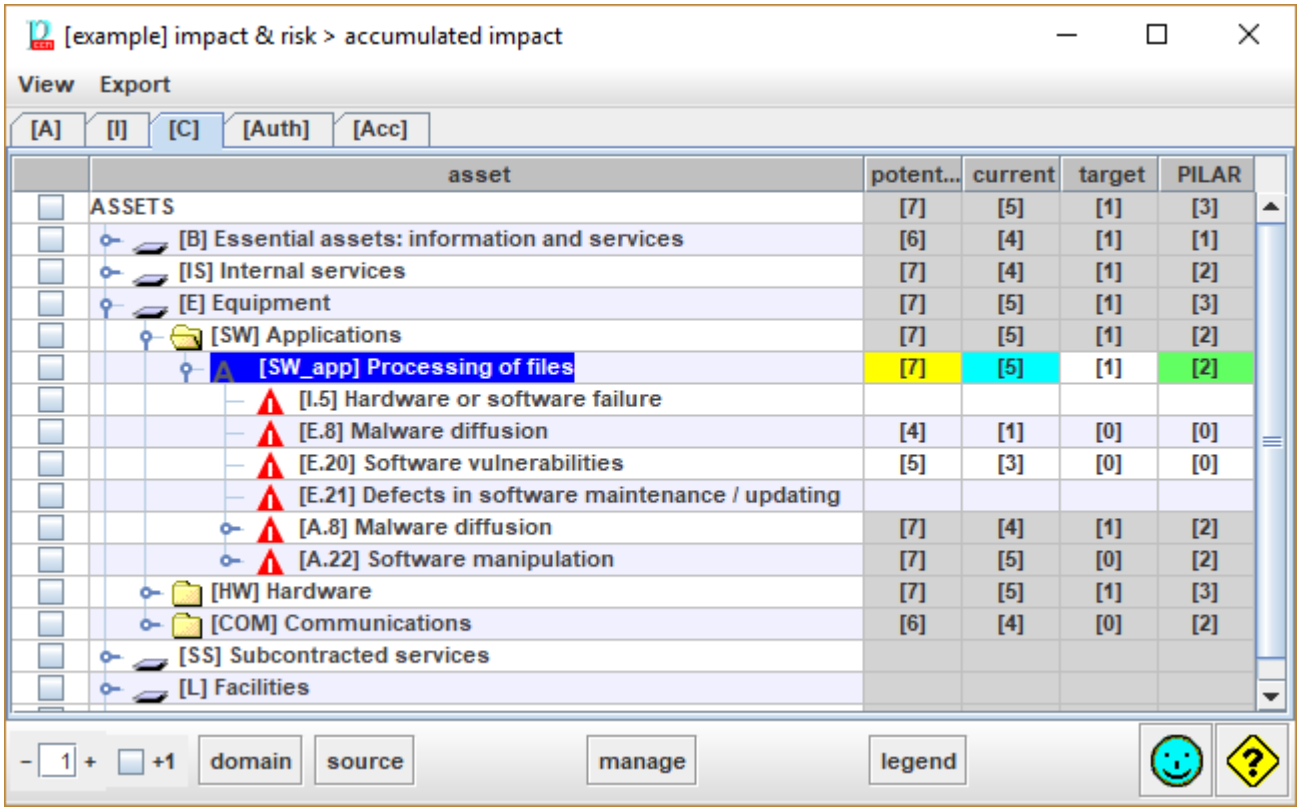


	Spinner to control the expansion of the assets tree. Expands down to assets. If [+1]is selected, it further expands threats.
+1	Modifier for assets tree expansion. If checked, threats are expanded.
domain	Select a security domain and PILAR will select the assets that belong to it.
source	Select one or more information sources and PILAR will select the assets associated to them.

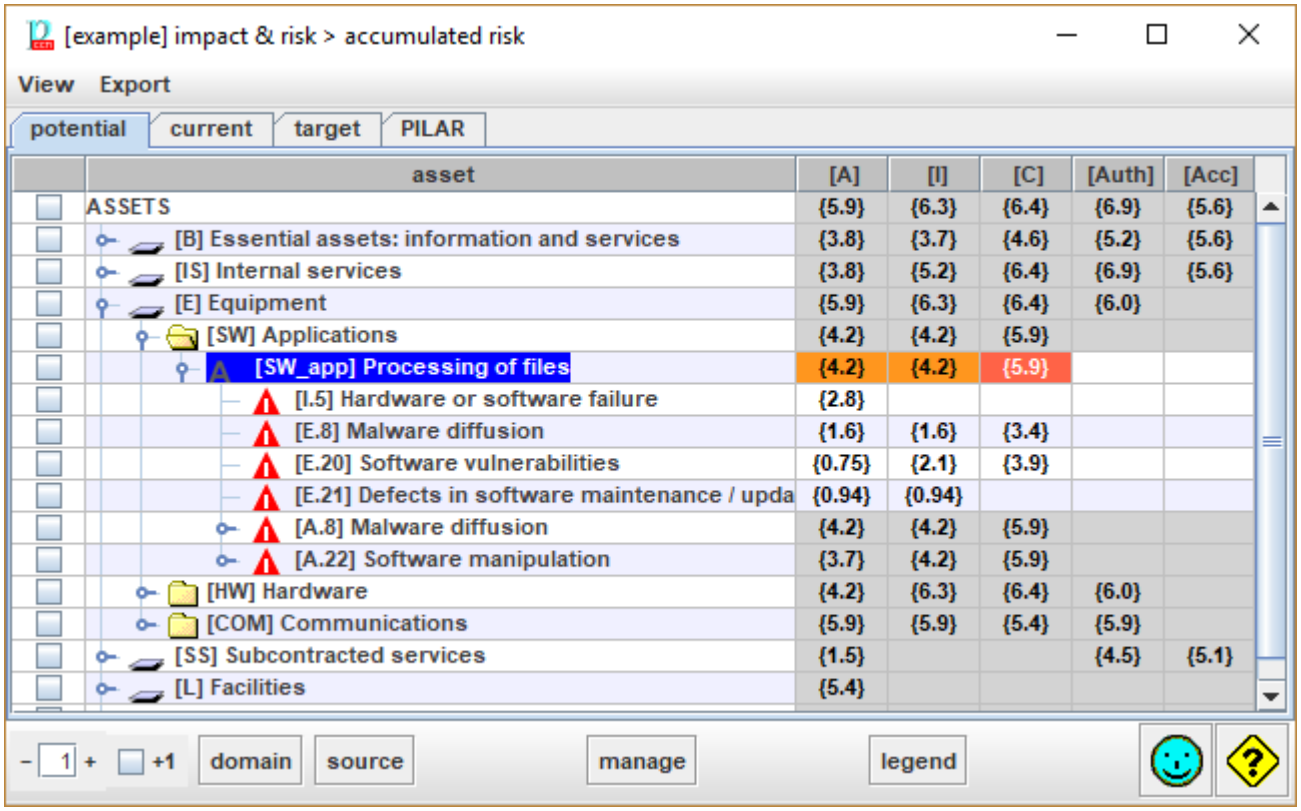
manage	For the rows selected in column 1, PILAR collects the risks, and jumps to the screen, considering only the selected risks.
legend	displays impact levels and colours

8.14.2.1 Alternate view

When you click on a column header, PILAR switches between columns and tabs:



8.14.3 Accumulated risk



Top menu VIEW

layers	tree organized by layers, then assets
logical zones	tree organized by logical zones, then assets
physical zones	tree organized by physical zones, then assets
threats	tree organized by threats, then assets

Top menu EXPORT

html	Exports selected rows to an html file for the web.
csv	Exports selected rows to a csv file for excel.
xml	Exports values to an xml file.
db	Exports values to a database. Only if the license enables the usage of SQL.

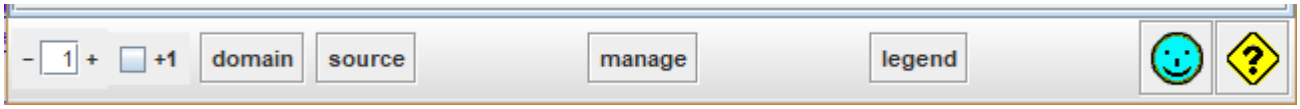
There is one tab per project phase. Click to switch.
Pseudo phase “potential” shows inherent risk without safeguards.

Table columns

selection	Click on checkboxes to check / uncheck.

	SHIFT-click to check a range. Click on column header to clear current selection. Selects rows to manage (see below)
assets	Assets and threats
dimensions	One column per security dimension. Click on header to switch to *alternate view*
	Impact value. Impacts are evaluated on threats, and summarised for assets, groups of assets, layers, and whole project.

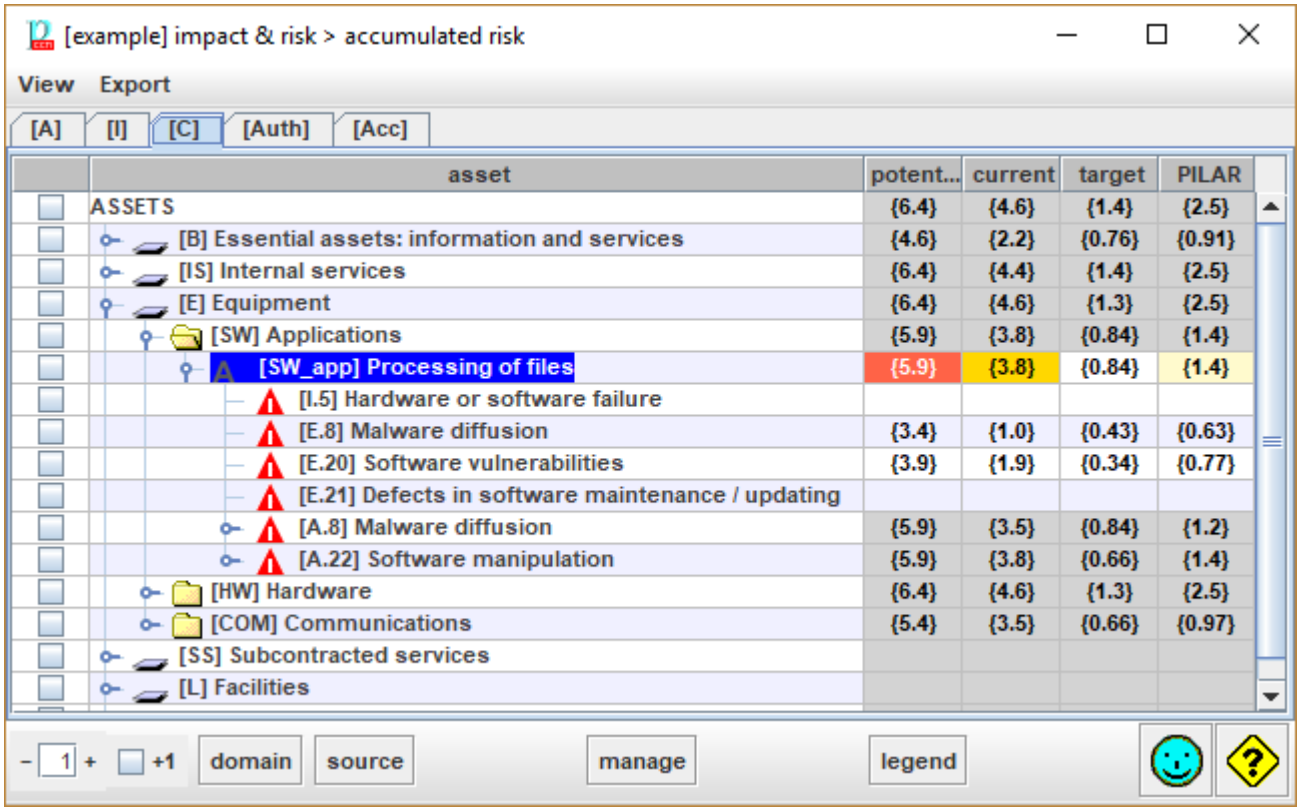
Bottom toolbar



	Spinner to control the expansion of the assets tree. Expands down to assets. If [+1] is selected, it further expands threats.
+1	Modifier for assets tree expansion. If checked, threats are expanded.
domain	Select a security domain and PILAR will select the assets that belong to it.
source	Select one or more information sources and PILAR will select the assets associated to them.
manage	For the rows selected in column 1, PILAR collects the risks, and jumps to the screen, considering only the selected risks.
legend	displays risk levels and colours

8.14.3.1 Alternate view

When you click on a column header, PILAR switches between columns and tabs:



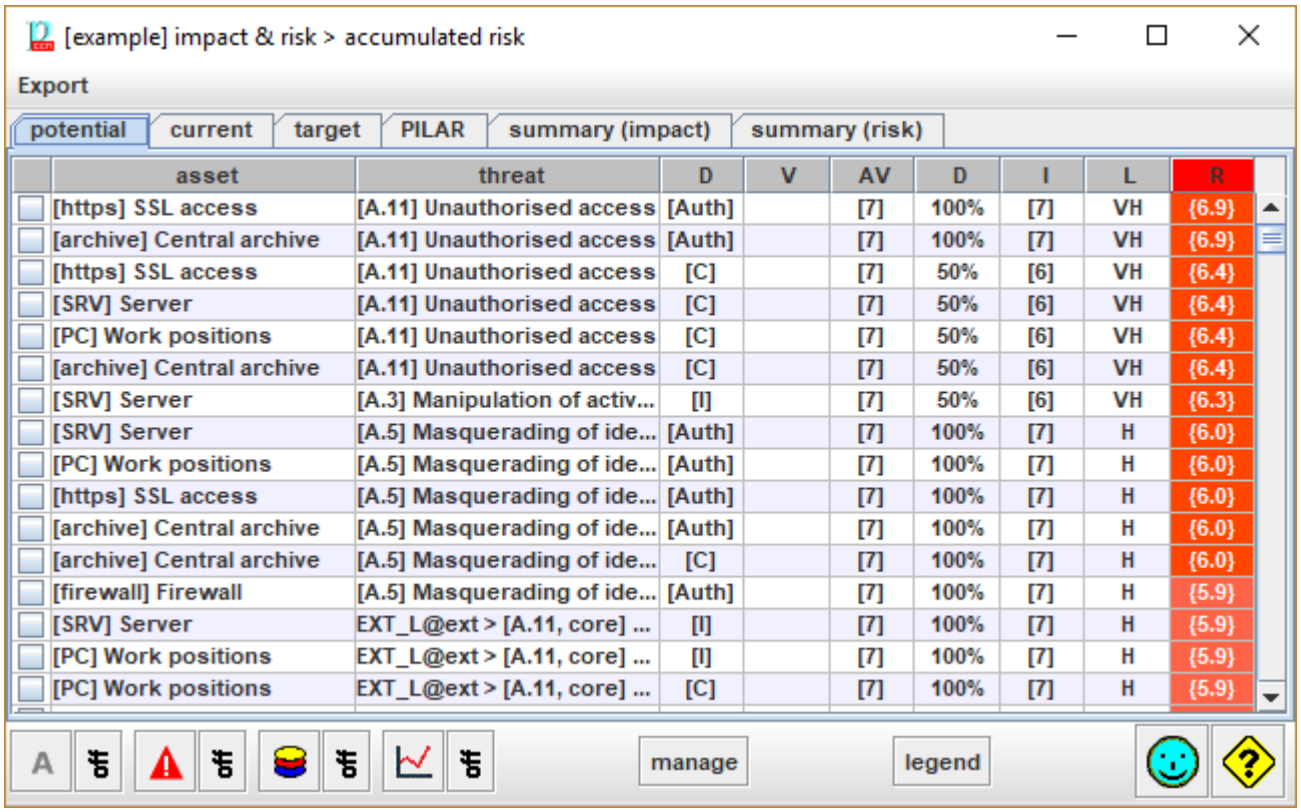
8.14.4 Accumulated impact and risk table

One tab per project phase. Click to switch.

Pseudo phase “potential” shows inherent risk without safeguards.

See *summary (impact)*

See *summary (risk)*



asset	threat	D	V	AV	D	I	L	R
[https] SSL access	[A.11] Unauthorised access	[Auth]		[7]	100%	[7]	VH	{6.9}
[archive] Central archive	[A.11] Unauthorised access	[Auth]		[7]	100%	[7]	VH	{6.9}
[https] SSL access	[A.11] Unauthorised access	[C]		[7]	50%	[6]	VH	{6.4}
[SRV] Server	[A.11] Unauthorised access	[C]		[7]	50%	[6]	VH	{6.4}
[PC] Work positions	[A.11] Unauthorised access	[C]		[7]	50%	[6]	VH	{6.4}
[archive] Central archive	[A.11] Unauthorised access	[C]		[7]	50%	[6]	VH	{6.4}
[SRV] Server	[A.3] Manipulation of activ...	[I]		[7]	50%	[6]	VH	{6.3}
[SRV] Server	[A.5] Masquerading of ide...	[Auth]		[7]	100%	[7]	H	{6.0}
[PC] Work positions	[A.5] Masquerading of ide...	[Auth]		[7]	100%	[7]	H	{6.0}
[https] SSL access	[A.5] Masquerading of ide...	[Auth]		[7]	100%	[7]	H	{6.0}
[archive] Central archive	[A.5] Masquerading of ide...	[Auth]		[7]	100%	[7]	H	{6.0}
[archive] Central archive	[A.5] Masquerading of ide...	[C]		[7]	100%	[7]	H	{6.0}
[firewall] Firewall	[A.5] Masquerading of ide...	[Auth]		[7]	100%	[7]	H	{5.9}
[SRV] Server	EXT_L@ext > [A.11, core] ...	[I]		[7]	100%	[7]	H	{5.9}
[PC] Work positions	EXT_L@ext > [A.11, core] ...	[I]		[7]	100%	[7]	H	{5.9}
[PC] Work positions	EXT_L@ext > [A.11, core] ...	[C]		[7]	100%	[7]	H	{5.9}

Table columns

Click on column header to use it to sort rows. The header of the selected column is shown in red background.

- asset – the assets
- threat – the threats
- dimension – the security dimension
- V – the own value of the asset, if any
- AV – the value accumulated on the asset
- D – degradation (see *Options / Effects*
- I – the impact
- L – the likelihood (see *Options / Likelihood*
- risk – the risk

Top menu EXPORT

csv	Exports values to a CSV file, for excel.
xml	Exports values to an XML file.
db	Exports values to a database.

Bottom toolbar

	To view only a few assets. Click on the image to select the assets to view.

	Click ON / OFF to switch whether the filter applies or not.
	To view only a few threats. Click on the image to select the threats to view. Click ON / OFF to switch whether the filter applies or not.
	To view only a few security dimensions. Click on the image to select the dimensions to view. Click ON / OFF to switch whether the filter applies or not.
	To view only a few risks. Click on the image to select the risks to view. You may specify a percentage for impact, and a percentage for risk. Typical values are 10%, and 10%, selecting the highest 10% of impact, and the highest 10% or risk (that is, the top-right of the impact-likelihood table).  0% means no impact / risk. 100% means any impact / risk. That is, nothing is filtered out. Click ON / OFF to switch whether the filter applies or not.
manage	For the rows selected in column 1, PILAR collects the risks, and jumps to the safeguard valuation screen, only taking into account the selected risks.
legend	See *Risks / Criticality levels & color encoding*

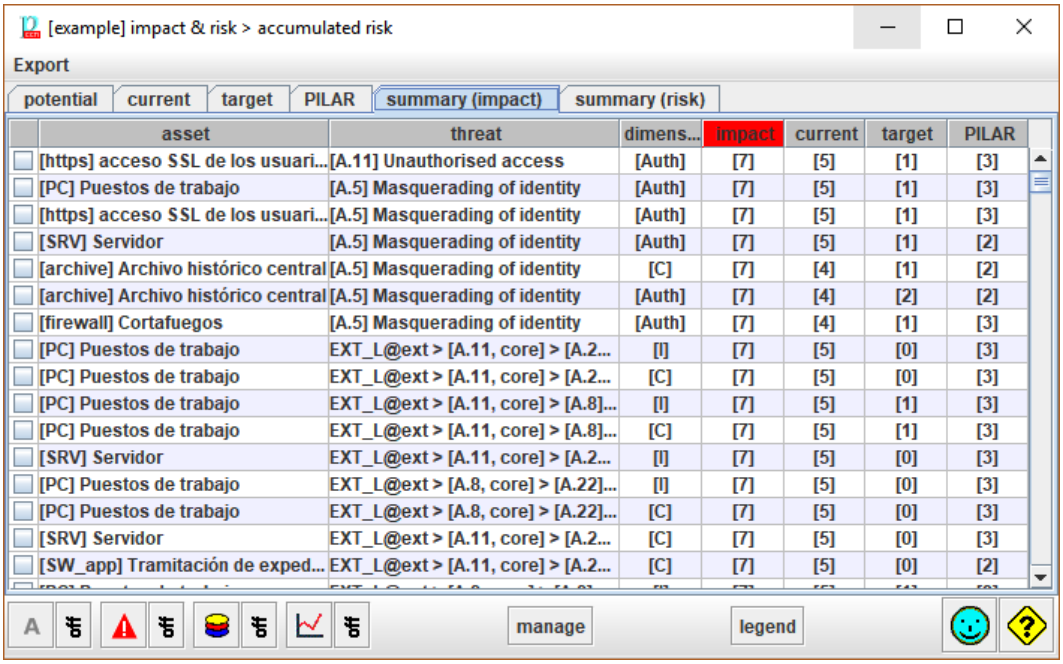
Initially, rows are sorted according to criticality (risk), then impact, then likelihood.

Click on any header to sort by the corresponding column:

assets	sorted according to their position in the assets' tree (ascending)
threats	sorted according to their position in the threats' tree (ascending)
dimension	sorted according to their position in the dimensions' list (ascending)
V	sorted by asset's value (descending)
A	sorted by the accumulated value (descending)
D	sorted by degradation (descending)
I	sorted by impact (descending)
F	sorted by likelihood (descending)
risk	sorted by risk (descending)

8.14.4.1 Impact summary

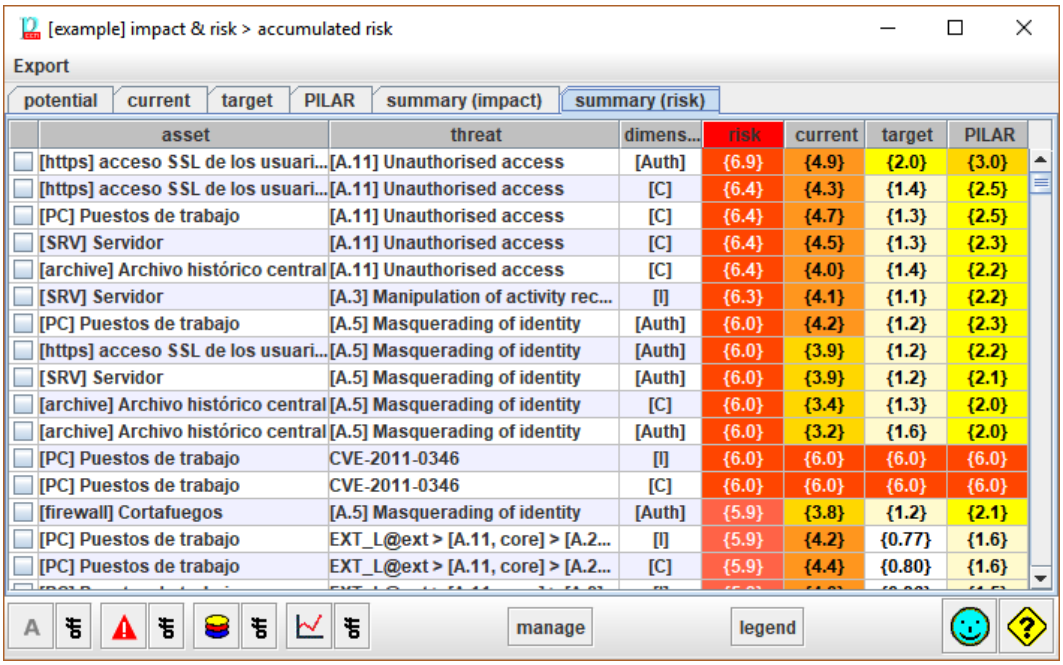
PILAR presents the evolution of impact along project phases.



asset	threat	dimens...	impact	current	target	PILAR
[https] acceso SSL de los usuari...	[A.11] Unauthorised access	[Auth]	[7]	[5]	[1]	[3]
[PC] Puestos de trabajo	[A.5] Masquerading of identity	[Auth]	[7]	[5]	[1]	[3]
[https] acceso SSL de los usuari...	[A.5] Masquerading of identity	[Auth]	[7]	[5]	[1]	[3]
[SRV] Servidor	[A.5] Masquerading of identity	[Auth]	[7]	[5]	[1]	[2]
[archive] Archivo histórico central	[A.5] Masquerading of identity	[C]	[7]	[4]	[1]	[2]
[archive] Archivo histórico central	[A.5] Masquerading of identity	[Auth]	[7]	[4]	[2]	[2]
[firewall] Cortafuegos	[A.5] Masquerading of identity	[Auth]	[7]	[4]	[1]	[3]
[PC] Puestos de trabajo	EXT_L@ext > [A.11, core] > [A.2...	[I]	[7]	[5]	[0]	[3]
[PC] Puestos de trabajo	EXT_L@ext > [A.11, core] > [A.2...	[C]	[7]	[5]	[0]	[3]
[PC] Puestos de trabajo	EXT_L@ext > [A.11, core] > [A.8]...	[I]	[7]	[5]	[1]	[3]
[PC] Puestos de trabajo	EXT_L@ext > [A.11, core] > [A.8]...	[C]	[7]	[5]	[1]	[3]
[SRV] Servidor	EXT_L@ext > [A.11, core] > [A.2...	[I]	[7]	[5]	[0]	[3]
[PC] Puestos de trabajo	EXT_L@ext > [A.8, core] > [A.22]...	[I]	[7]	[5]	[0]	[3]
[PC] Puestos de trabajo	EXT_L@ext > [A.8, core] > [A.22]...	[C]	[7]	[5]	[0]	[3]
[SRV] Servidor	EXT_L@ext > [A.11, core] > [A.2...	[C]	[7]	[5]	[0]	[3]
[SW_app] Tramitación de exped...	EXT_L@ext > [A.11, core] > [A.2...	[C]	[7]	[5]	[0]	[2]

8.14.4.2 Risk summary

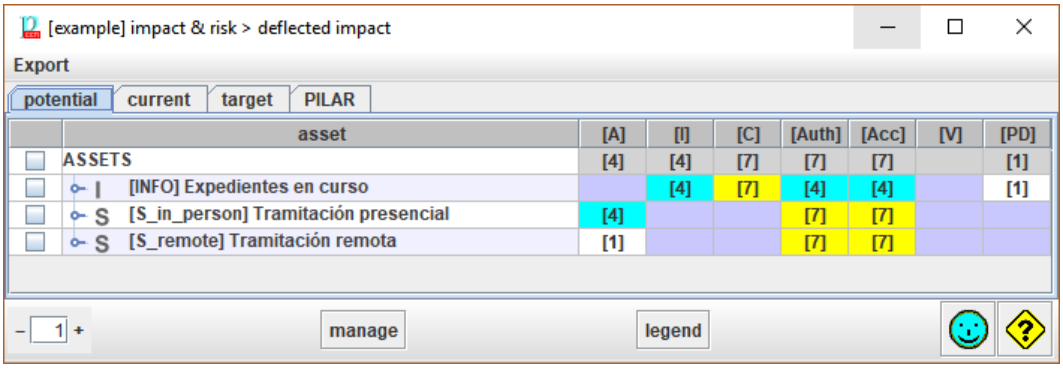
PILAR presents the evolution of risk along project phases.



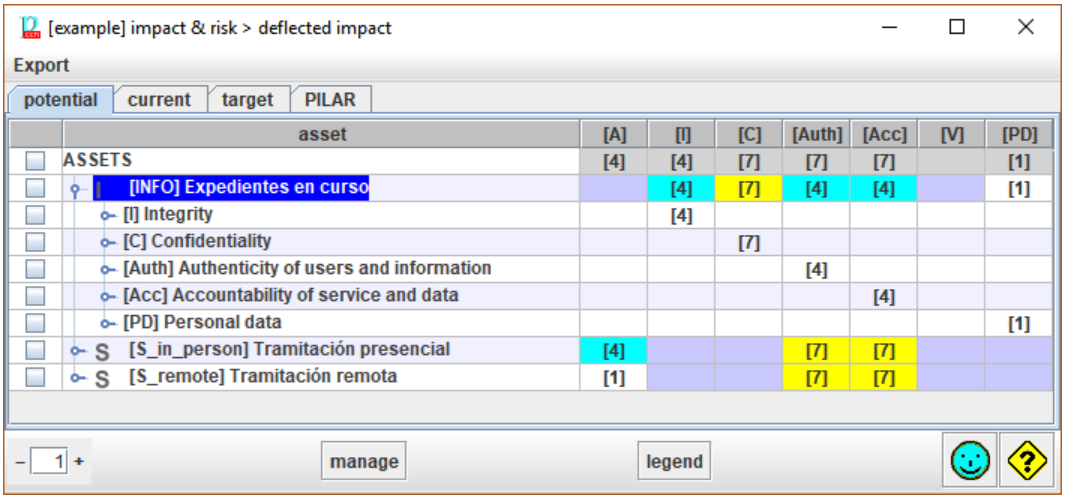
asset	threat	dimens...	risk	current	target	PILAR
[https] acceso SSL de los usuari...	[A.11] Unauthorised access	[Auth]	{6.9}	{4.9}	{2.0}	{3.0}
[https] acceso SSL de los usuari...	[A.11] Unauthorised access	[C]	{6.4}	{4.3}	{1.4}	{2.5}
[PC] Puestos de trabajo	[A.11] Unauthorised access	[C]	{6.4}	{4.7}	{1.3}	{2.5}
[SRV] Servidor	[A.11] Unauthorised access	[C]	{6.4}	{4.5}	{1.3}	{2.3}
[archive] Archivo histórico central	[A.11] Unauthorised access	[C]	{6.4}	{4.0}	{1.4}	{2.2}
[SRV] Servidor	[A.3] Manipulation of activity rec...	[I]	{6.3}	{4.1}	{1.1}	{2.2}
[PC] Puestos de trabajo	[A.5] Masquerading of identity	[Auth]	{6.0}	{4.2}	{1.2}	{2.3}
[https] acceso SSL de los usuari...	[A.5] Masquerading of identity	[Auth]	{6.0}	{3.9}	{1.2}	{2.2}
[SRV] Servidor	[A.5] Masquerading of identity	[Auth]	{6.0}	{3.9}	{1.2}	{2.1}
[archive] Archivo histórico central	[A.5] Masquerading of identity	[C]	{6.0}	{3.4}	{1.3}	{2.0}
[archive] Archivo histórico central	[A.5] Masquerading of identity	[Auth]	{6.0}	{3.2}	{1.6}	{2.0}
[PC] Puestos de trabajo	CVE-2011-0346	[I]	{6.0}	{6.0}	{6.0}	{6.0}
[PC] Puestos de trabajo	CVE-2011-0346	[C]	{6.0}	{6.0}	{6.0}	{6.0}
[firewall] Cortafuegos	[A.5] Masquerading of identity	[Auth]	{5.9}	{3.8}	{1.2}	{2.1}
[PC] Puestos de trabajo	EXT_L@ext > [A.11, core] > [A.2...	[I]	{5.9}	{4.2}	{0.77}	{1.6}
[PC] Puestos de trabajo	EXT_L@ext > [A.11, core] > [A.2...	[C]	{5.9}	{4.4}	{0.80}	{1.6}

8.14.5 Deflected impact

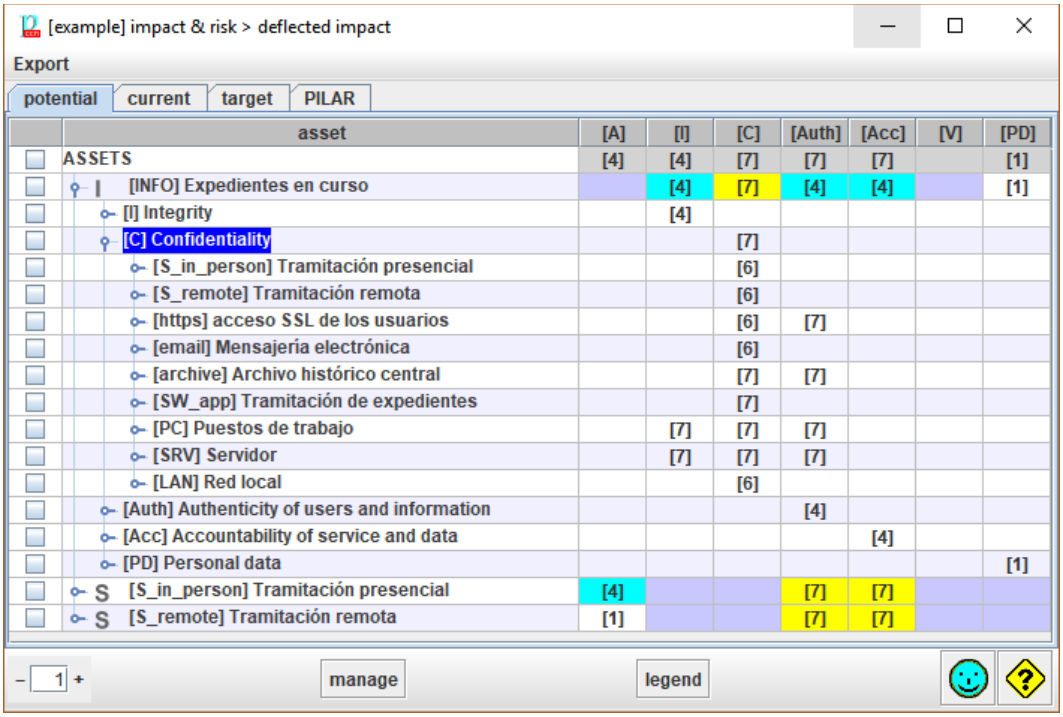
PILAR presents the deflected impact on assets with an explicit value:



You may expand the tree to split each dimension apart

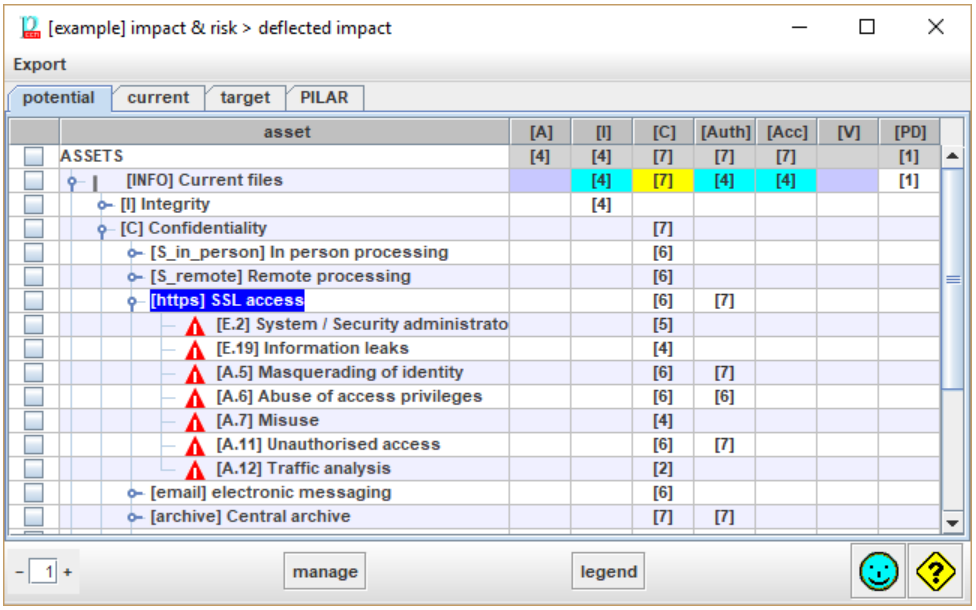


You may further expand the tree to inspect how each dimension is affected on assets below:



asset	[A]	[I]	[C]	[Auth]	[Acc]	[V]	[PD]
ASSETS	[4]	[4]	[7]	[7]	[7]		[1]
[INFO] Expedientes en curso		[4]	[7]	[4]	[4]		[1]
[I] Integrity		[4]					
[C] Confidentiality			[7]				
[S_in_person] Tramitación presencial			[6]				
[S_remote] Tramitación remota			[6]				
[https] acceso SSL de los usuarios			[6]	[7]			
[email] Mensajería electrónica			[6]				
[archive] Archivo histórico central			[7]	[7]			
[SW_app] Tramitación de expedientes			[7]				
[PC] Puestos de trabajo		[7]	[7]	[7]			
[SRV] Servidor		[7]	[7]	[7]			
[LAN] Red local			[6]				
[Auth] Authenticity of users and information				[4]			
[Acc] Accountability of service and data					[4]		
[PD] Personal data							[1]
S [S_in_person] Tramitación presencial	[4]			[7]	[7]		
S [S_remote] Tramitación remota	[1]			[7]	[7]		

And so on, down to the level of single threats:



asset	[A]	[I]	[C]	[Auth]	[Acc]	[V]	[PD]
ASSETS	[4]	[4]	[7]	[7]	[7]		[1]
[INFO] Current files		[4]	[7]	[4]	[4]		[1]
[I] Integrity		[4]					
[C] Confidentiality			[7]				
[S_in_person] In person processing			[6]				
[S_remote] Remote processing			[6]				
[https] SSL access			[6]	[7]			
[E.2] System / Security administrato			[5]				
[E.19] Information leaks			[4]				
[A.5] Masquerading of identity			[6]	[7]			
[A.6] Abuse of access privileges			[6]	[6]			
[A.7] Misuse			[4]				
[A.11] Unauthorised access			[6]	[7]			
[A.12] Traffic analysis			[2]				
[email] electronic messaging			[6]				
[archive] Central archive			[7]	[7]			

One tab per project phase. Click to switch.
Pseudo phase “potential” shows inherent impact without safeguards

Top menu EXPORT

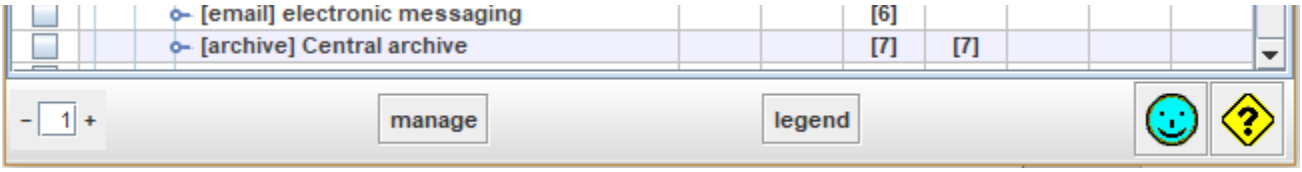
html	Exports selected rows to an html file for the web.
csv	Exports selected rows to a csv file for excel.

xml	Exports values to an xml file.
db	Exports values to a database. Only if the license enables the usage of SQL.

Table columns

1	**selection**	Click on checkboxes to check / uncheck. SHIFT-click to check a range. Click on column header to clear current selection. Selects rows to manage (see below)
2	**assets**	Assets tree. 1st level: assets with a value: deflected impact. 2nd level: split down of security dimensions: deflected impact. 3rd level: assets below (in dependency tree): accumulated impact. 4th level: threats impacting the assets: accumulated impact.
3 …	**dimensions**	One column per security dimension. Click on header to switch to alternate view.

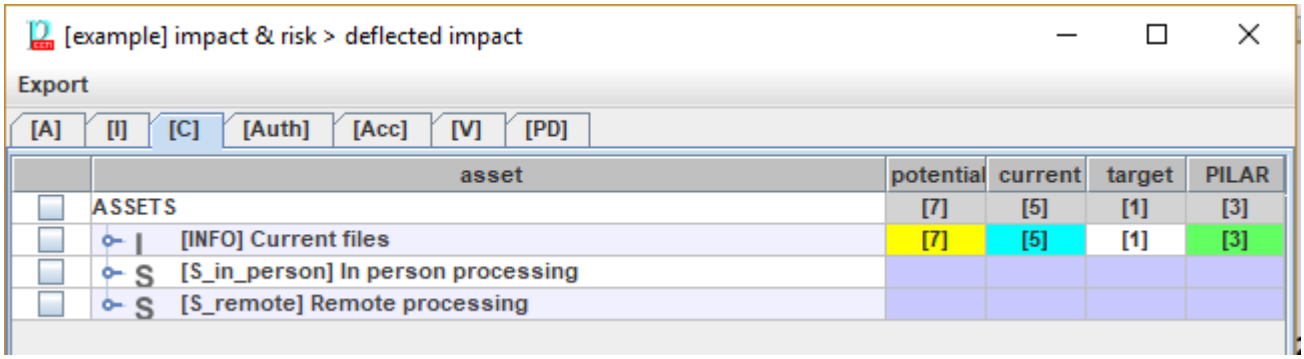
Bottom toolbar



	Spinner to control the expansion of the assets tree.
manage	For the rows selected in column 1, PILAR collects the risks, and jumps to the safeguard valuation screen, only taking into account the selected risks.
legend	displays impact levels and colours

8.14.5.1 Alternate view

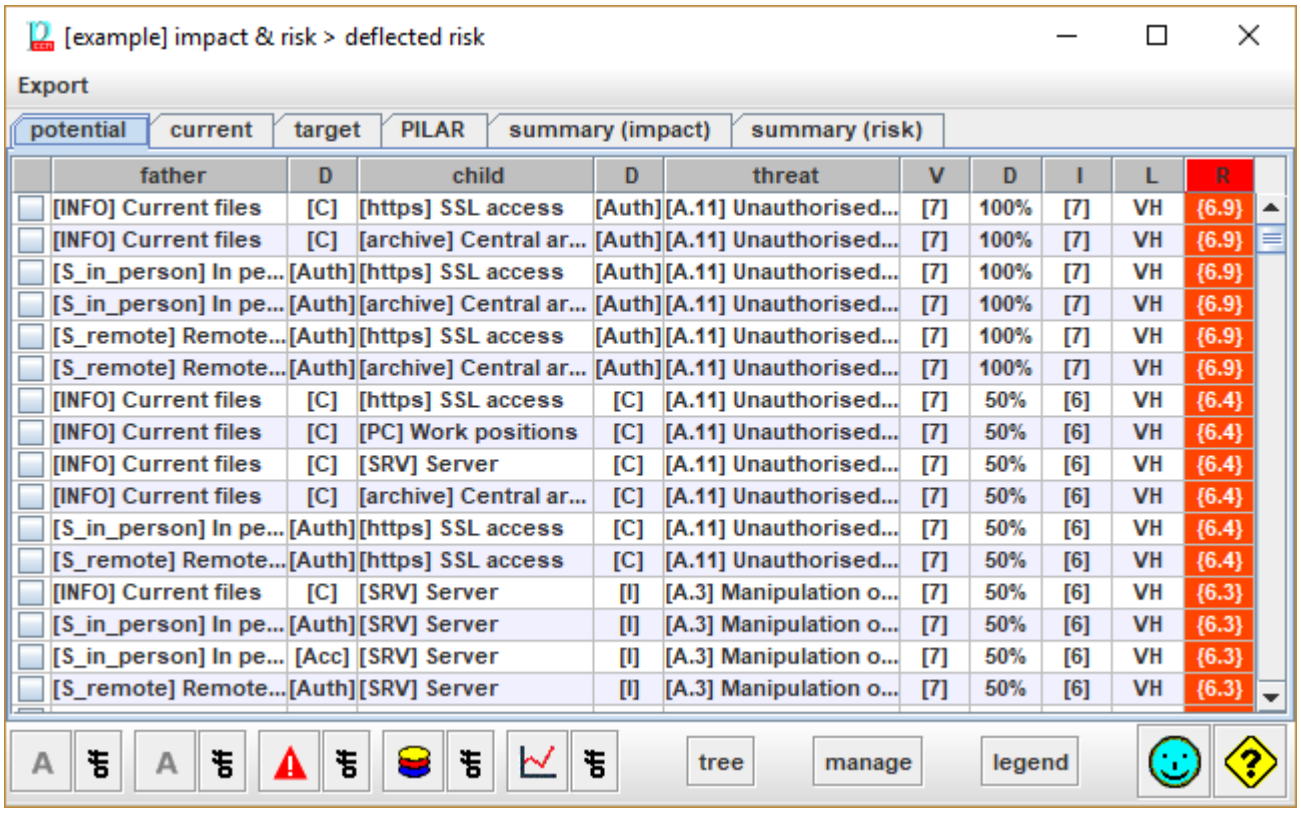
When you click on the header of a security dimension column, PILAR switches between columns and tabs, and presents the following image:



8.14.6 Deflected risk

Similar to *Deflected impact*, but presents risk values instead of impact values.

8.14.7 Deflected impact and risk table



One tab per project phase. Click to switch.

Pseudo phase “potential” shows inherent risk without safeguards.

- See *summary (impact)*
- See *summary (risk)*

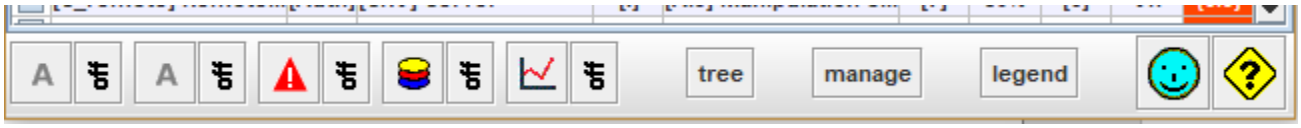
Top menu EXPORT

csv	Exports selected rows to a csv file for excel.
xml	Exports values to an xml file.
db	Exports values to a database. Only if the license enables the usage of SQL.

Table columns

1	selection	
2	father	The asset above: the one with value where the consequences of the threat are deflected.
3	dimension above	the consequences of the thread are on this dimension
4	child	The asset below: where the threat occurs.
5	dimension below	The dimension affected by the threat on the asset below.
6	threat	The threat
7	value	The value of the asset above on the dimension above.
8	degradation	The degradation caused by the threat on the dimension of the asset
9	impact	Impact of the threat on the dimension of the asset above.
10	likelihood	Likelihood of the threat on the asset. The label on the header follows the option selected to present likelihood (see *Options / Likelihood*

Bottom toolbar



	Filter assets above. To view only a few assets. Click on the image to select the assets to view. Click ON / OFF to switch whether the filter applies or not.
	Filter assets below. To view only a few assets. Click on the image to select the assets to view. Click ON / OFF to switch whether the filter applies or not.
	To view only a few threats. Click on the image to select the threats to view.

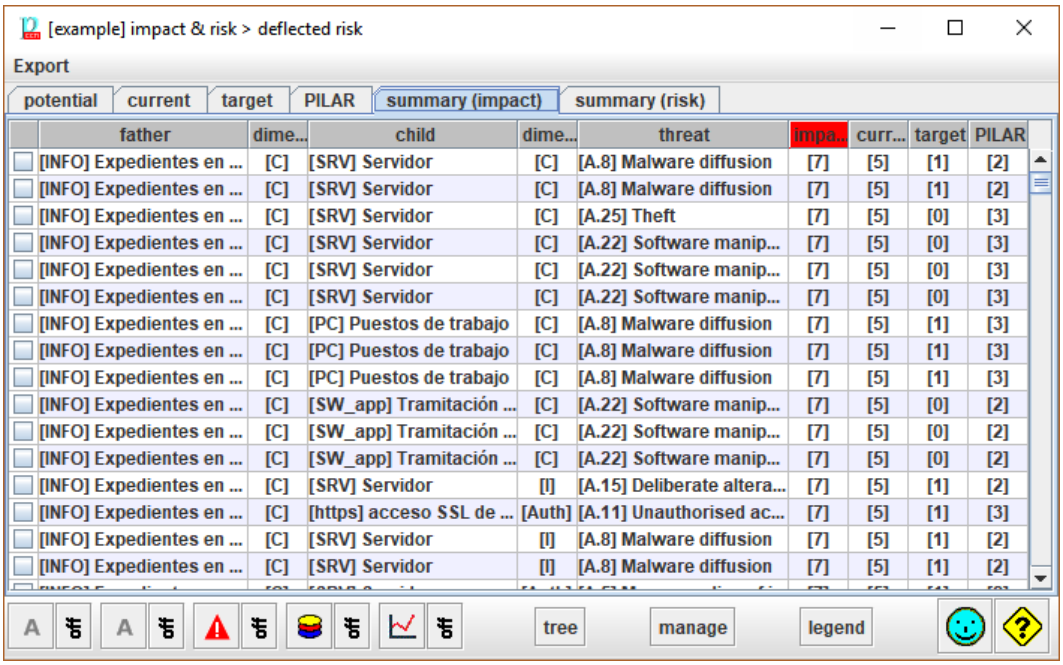
	Click ON / OFF to switch whether the filter applies or not.
	To view only a few security dimensions. Click on the image to select the dimensions to view. Click ON / OFF to switch whether the filter applies or not.
	To view only a few risks. Click on the image to select the risks to view. You may specify a percentage for impact, and a percentage for risk. Typical values are 10%, and 10%, selecting the highest 10% of impact, and the highest 10% or risk (that is, the top-right of the impact-likelihood table). 0% means no impact / risk. 100% means any impact / risk. That is, nothing is filtered out. Click ON / OFF to switch whether the filter applies or not.
TREE	
manage	Select one or more rows. For the rows selected, PILAR collects the risks, and jumps to the safeguard valuation screen, only taking into account the selected risks.
legend	See *Risks / Criticality levels & color encoding*

Rows are sorted according to criticality (risk), then impact, then likelihood.

Click on any header to sort by the corresponding column.

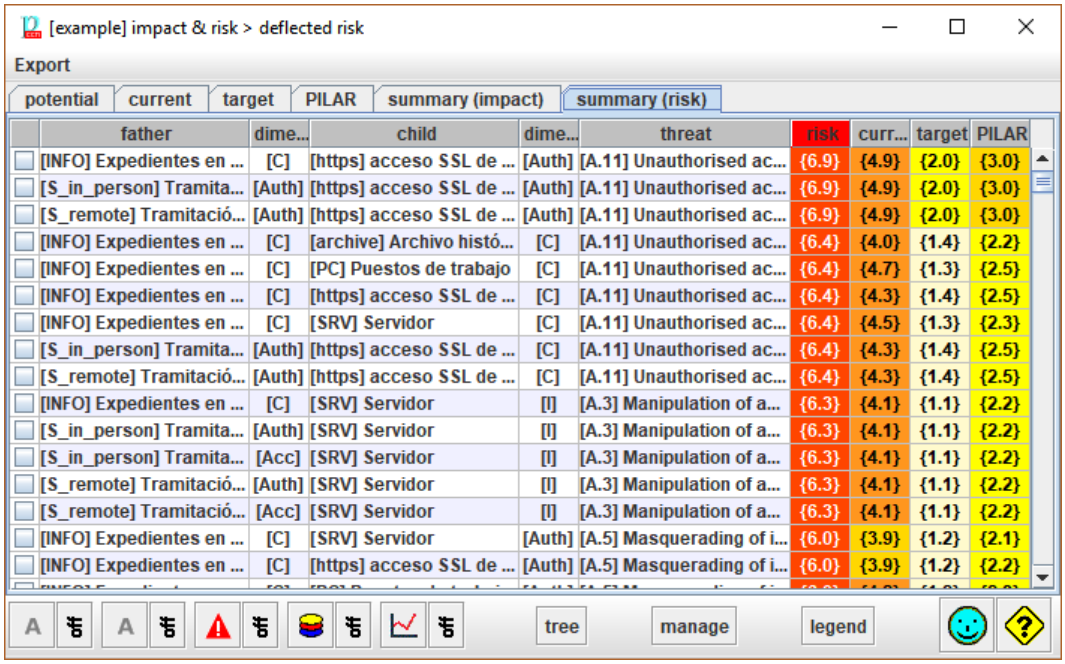
8.14.7.1 Impact summary

PILAR presents the evolution of the impact along project phases.



8.14.7.2 Risk summary

PILAR presents the evolution of risk along project phases.



father	dime...	child	dime...	threat	risk	curr...	target	PILAR
[INFO] Expedientes en ...	[C]	[https] acceso SSL de ...	[Auth]	[A.11] Unauthorised ac...	{6.9}	{4.9}	{2.0}	{3.0}
[S_in_person] Tramita...	[Auth]	[https] acceso SSL de ...	[Auth]	[A.11] Unauthorised ac...	{6.9}	{4.9}	{2.0}	{3.0}
[S_remote] Tramitació...	[Auth]	[https] acceso SSL de ...	[Auth]	[A.11] Unauthorised ac...	{6.9}	{4.9}	{2.0}	{3.0}
[INFO] Expedientes en ...	[C]	[archive] Archivo histó...	[C]	[A.11] Unauthorised ac...	{6.4}	{4.0}	{1.4}	{2.2}
[INFO] Expedientes en ...	[C]	[PC] Puestos de trabajo	[C]	[A.11] Unauthorised ac...	{6.4}	{4.7}	{1.3}	{2.5}
[INFO] Expedientes en ...	[C]	[https] acceso SSL de ...	[C]	[A.11] Unauthorised ac...	{6.4}	{4.3}	{1.4}	{2.5}
[INFO] Expedientes en ...	[C]	[SRV] Servidor	[C]	[A.11] Unauthorised ac...	{6.4}	{4.5}	{1.3}	{2.3}
[S_in_person] Tramita...	[Auth]	[https] acceso SSL de ...	[C]	[A.11] Unauthorised ac...	{6.4}	{4.3}	{1.4}	{2.5}
[S_remote] Tramitació...	[Auth]	[https] acceso SSL de ...	[C]	[A.11] Unauthorised ac...	{6.4}	{4.3}	{1.4}	{2.5}
[INFO] Expedientes en ...	[C]	[SRV] Servidor	[I]	[A.3] Manipulation of a...	{6.3}	{4.1}	{1.1}	{2.2}
[S_in_person] Tramita...	[Auth]	[SRV] Servidor	[I]	[A.3] Manipulation of a...	{6.3}	{4.1}	{1.1}	{2.2}
[S_in_person] Tramita...	[Acc]	[SRV] Servidor	[I]	[A.3] Manipulation of a...	{6.3}	{4.1}	{1.1}	{2.2}
[S_remote] Tramitació...	[Auth]	[SRV] Servidor	[I]	[A.3] Manipulation of a...	{6.3}	{4.1}	{1.1}	{2.2}
[S_remote] Tramitació...	[Acc]	[SRV] Servidor	[I]	[A.3] Manipulation of a...	{6.3}	{4.1}	{1.1}	{2.2}
[INFO] Expedientes en ...	[C]	[SRV] Servidor	[Auth]	[A.5] Masquerading of i...	{6.0}	{3.9}	{1.2}	{2.1}
[INFO] Expedientes en ...	[C]	[https] acceso SSL de ...	[Auth]	[A.5] Masquerading of i...	{6.0}	{3.9}	{1.2}	{2.2}

9 Security profiles (EVL)

Security profiles are collections of safeguards that aim to protect a system. Security profiles may focus on some specific aspects or may be general. There are security profiles that are widely recognized and can be checked for compliance.

PILAR maps security profiles to her safeguards in such a way that:

- you may estimate to which extend the system is compliant
- PILAR may estimate the residual risk after satisfying the profile
- you may work with several profiles in a coordinated manner

Let's use ISO/IEC 27002 (2013) as an example.

To load it into PILAR, you need the corresponding .EVL file

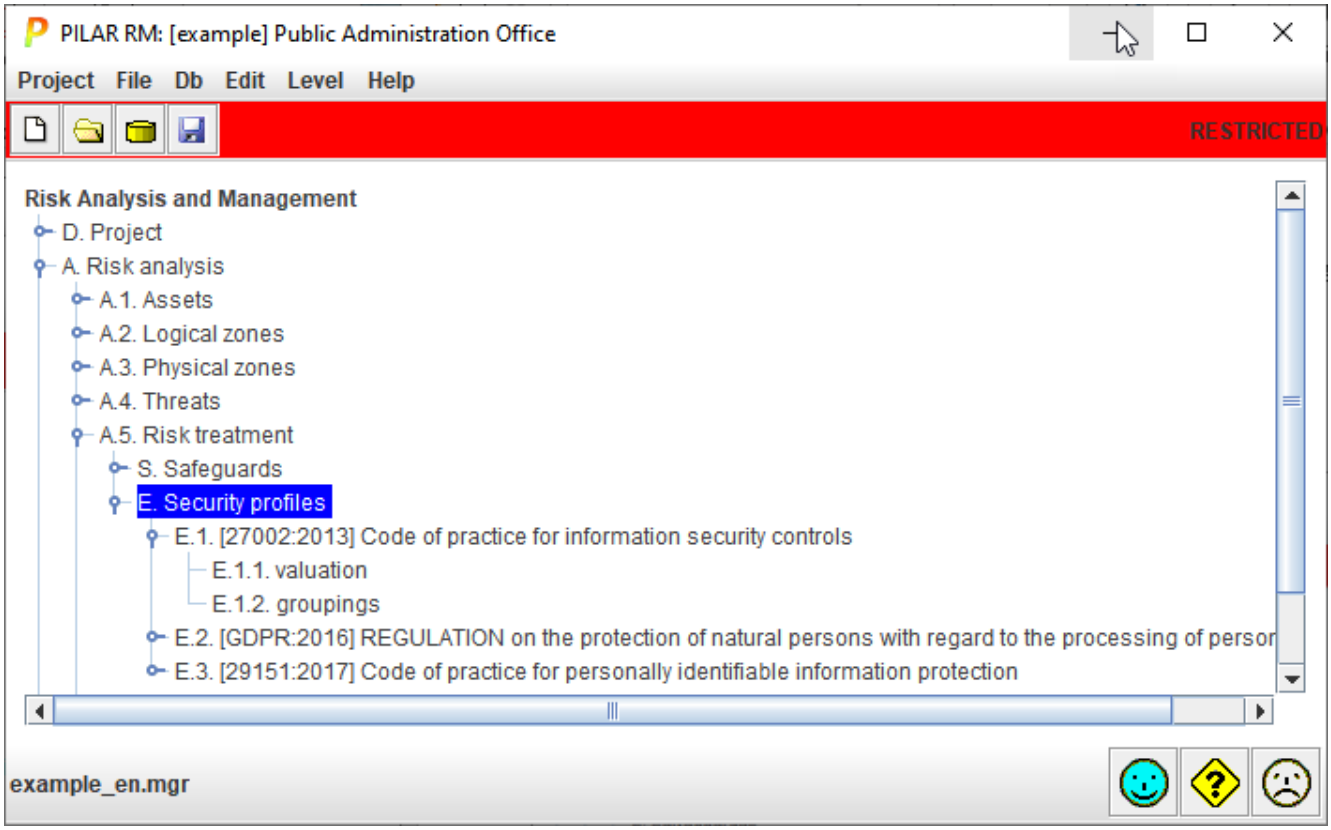
```
bib_en/27002_2013_*_en.evl
```

and you have to configure PILAR to load it on start (alternatively, you may load later, through the user interface). From the configuration file:

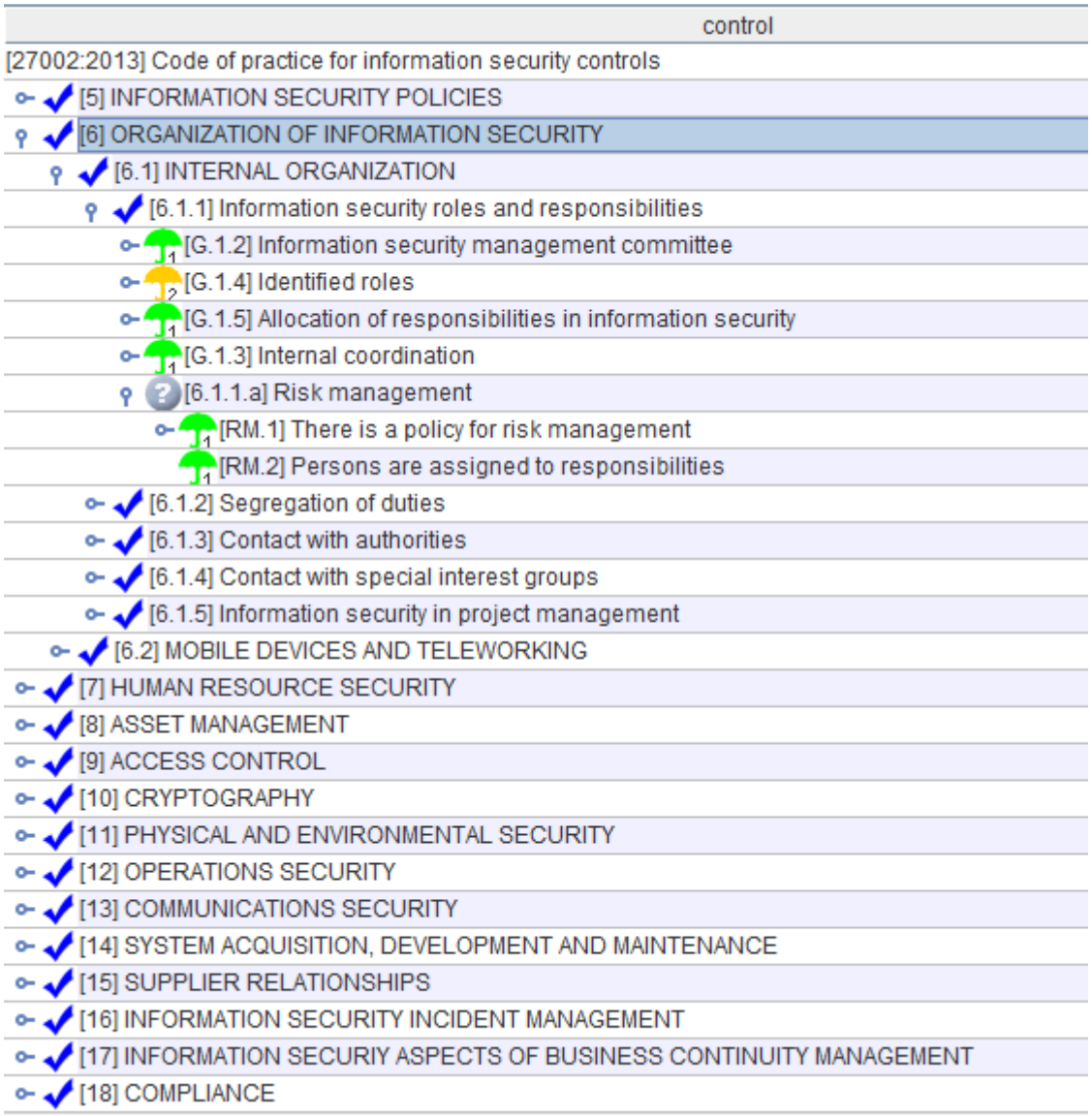
STIC_en.car

```
profile= 27002_2013_ * _en.evl
```

In the GUI, the loaded profiles appear as:



And, getting into valuation, we find the collection of controls of the standard:

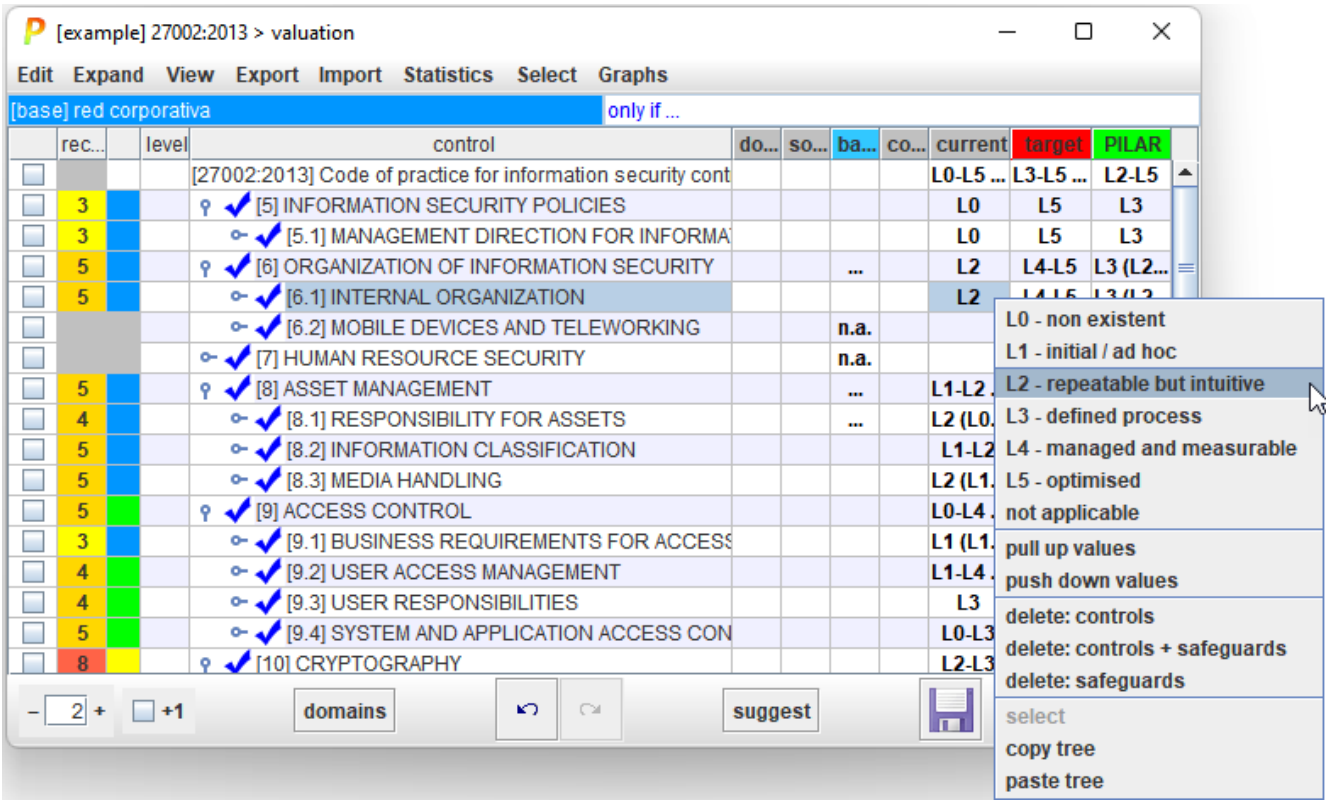


EVL trees have different types of nodes:

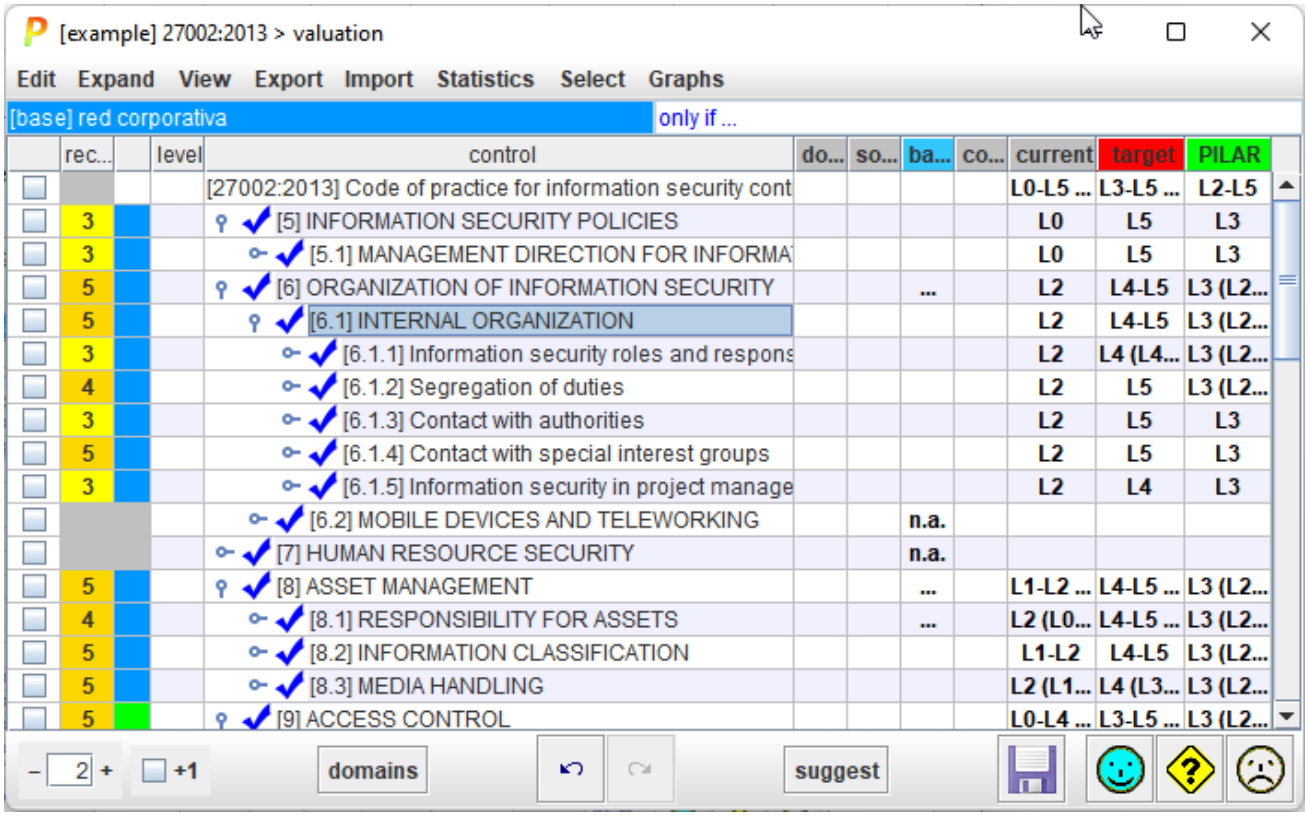
	Controls – main requirements from security profiles
	Questions – secondary requirements, or tree structuring nodes
	Links – when a control refers to another control
	Safeguards – countermeasures from the PILAR library
	See also – additional information

9.1 EVL - Basic usage

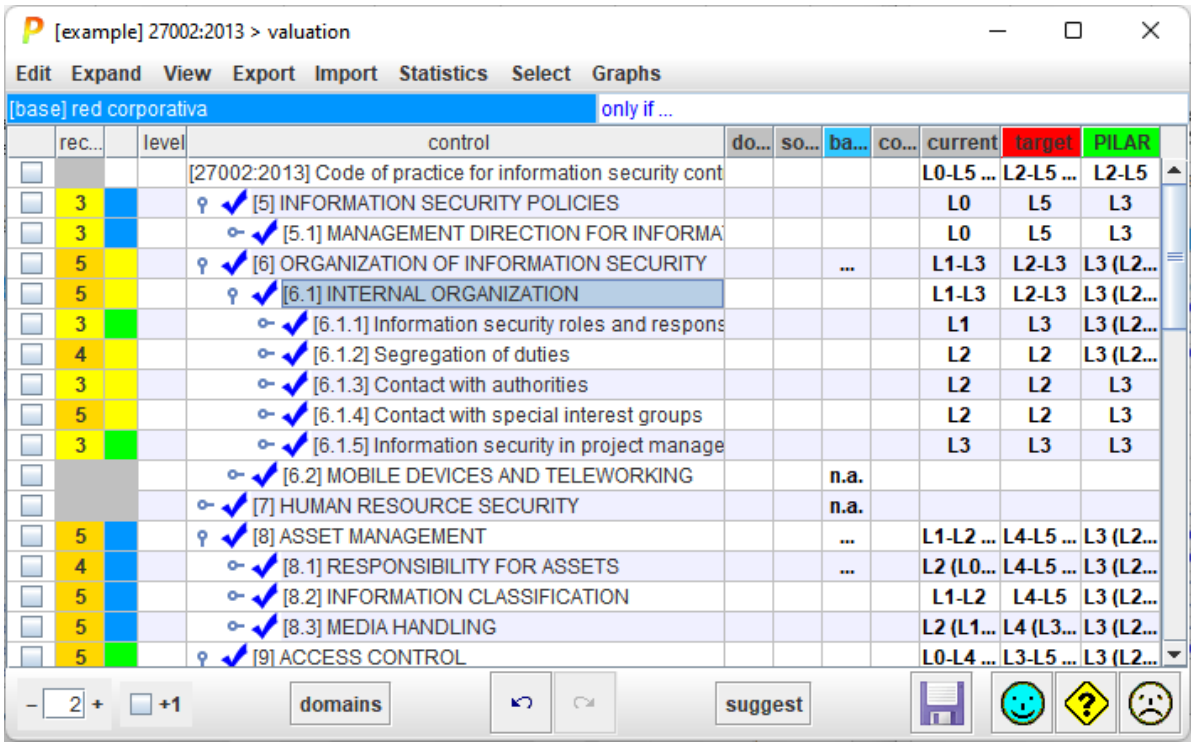
Basic usage is to introduce values for profile controls. Select the cell for a control, and a phase, then right click:



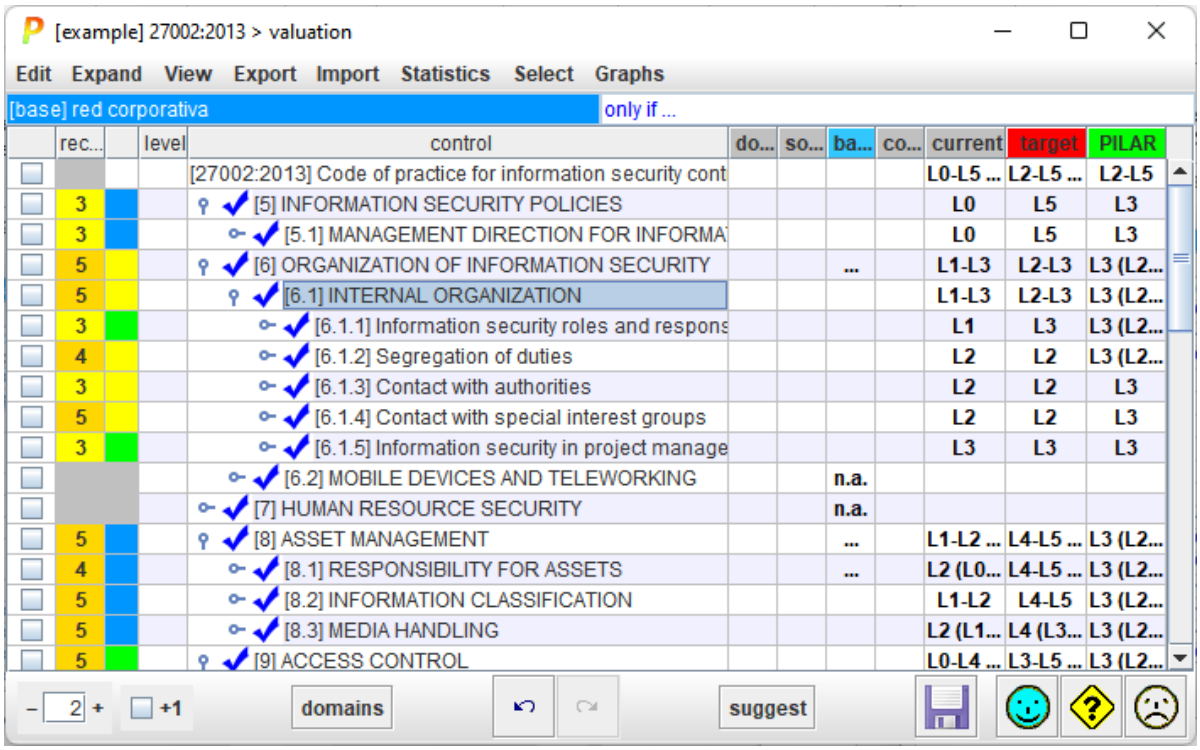
PILAR applies the selected maturity to the selected control. Then, it is copied onto every child.



So, you can set a general value for many controls, and refine the details later. When children have a range of values, the common father presents the maturity range:



The value in one phase is used in following phases, unless changed.

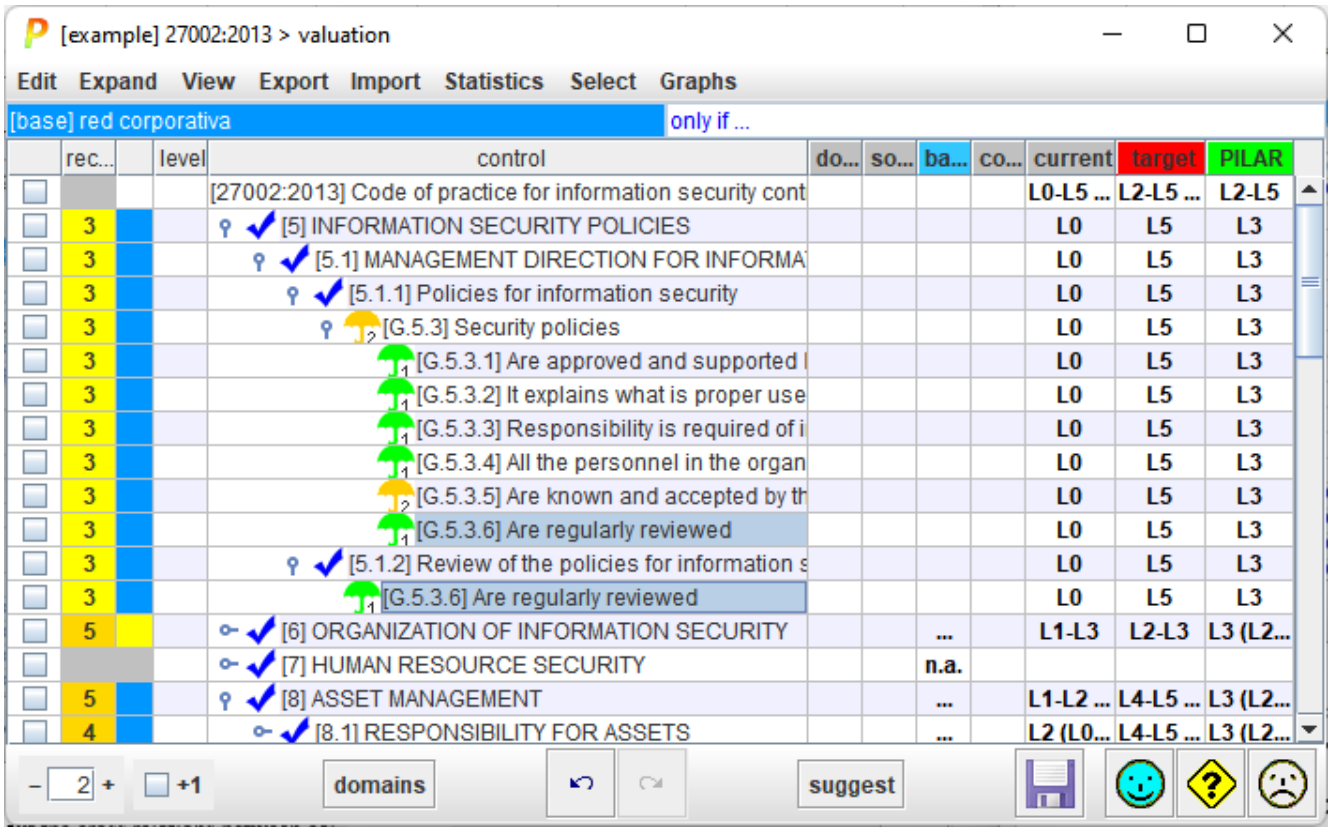


PILAR maps controls onto safeguards. This mapping is neither official, nor perfect. It is not official because security profiles are pieces of work from different sources, unrelated to PILAR. And it is not perfect for several reasons:

- there may be no appropriate safeguard in PILAR to meet the control requirements
- the same safeguard in PILAR may apply to more than one control
- as PILAR evolves, the set of safeguards evolve

PILAR tries to do something reasonable.

When a safeguard is found in several mappings, change the value in one place has a ripple effect:



We may find out the cross relations between controls by asking for the safeguards used in several places

EXPAND > dual role

9.2 EVL - View options

PILAR may present maturity of controls and safeguards in several ways

view >> maturity

PILAR presents the range of the controls, and the range of safeguards.

view >> ~ maturity

PILAR presents an approximation to the maturity, averaging components. For example, if most children are L3, but one is not, the average is slightly less than L3-

view >> percent

It averages the value of safeguards and presents the average between 0% and 100%. Although this mode forgets that safeguard mapping is not perfect, the numbers are useful for graphs.

view >> phase

It considers the maturity of the safeguards in the corresponding phase, compared to the recommended value in the extra phase. Using this mode, we have a picture of how far security if from recommended values. For example, with respect to PILAR

9.3 EVL - Control options

Right-click on any control for a collection of options:

edit

Presents a domain-phase view of the maturity values. See below.

copy

the name of the control to clipboard

copy path

the control, and its ancestors, to clipboard

full text

code and name of the control to clipboard

full path

all the stapes, from root to me, into clipboard

description

a more extensive description, if available

close father

compact tree: father is closed

close brothers

compact tree: brothers are closed

go to …

for links,  , jump to the link destination

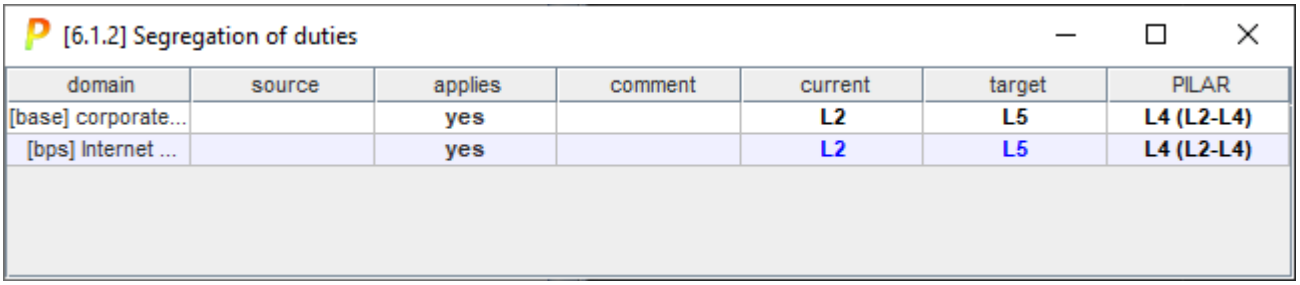
compensating control

adds or edits an alternative control

additional measures

adds or edits additional controls

Domain-phase view. Clicking on a control (right click > EDIT) you may have a one-control view of maturity values covering all the domains and all the phases



domain	source	applies	comment	current	target	PILAR
[base] corporate...		yes		L2	L5	L4 (L2-L4)
[bps] Internet ...		yes		L2	L5	L4 (L2-L4)

User values are in black over white; while calculated values are in cyan.

9.4 EVL - Hooks

Links may be associated to controls by means of hook-files. These are files in the library directory which name starts with the pattern “hooks-“. The content is formatted as JSON.

Let’s show an example:

bib_es/hooks-ccn.json

```
{
  "encoding": "áéíóú",
  "title" : "CCN-CERT",
  "defs" : [
    { "controls" : [ [ "ens:2015", "org.1" ],
                     [ "27002:2013", "5.1.1", "6.1.1" ] ],
      "classes" : [ ],
      "links" : [
        { "label" : "CCN-STIC-805 - Política de Seguridad de la Información",
          "url" : "https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-
esquema-nacional-de-seguridad.html"
        },
        { "label" : "CCN-STIC-801 - Responsabilidades y Funciones en el ENS",
          "url" : "https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-
esquema-nacional-de-seguridad.html"
        }
      ]
    },
    { "controls" : [ [ "ens:2015", "org.2" ],
                     [ "27002:2013", "5.1.1" ] ],
      "classes" : [ ],
      "links" : [
        { "label" : "CCN-STIC-821 - Normas de Seguridad en el ENS",
          "url" : "https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-
esquema-nacional-de-seguridad.html"
        }
      ]
    },
```

9.5 EVL – Applicability

For each one of the controls ( ), each one of the questions ( ), and each one of the safeguards ( ) you may say whether it applies or not by clicking on the column APPLIES:

For instance, if we have mobile computers, but no tele-working:

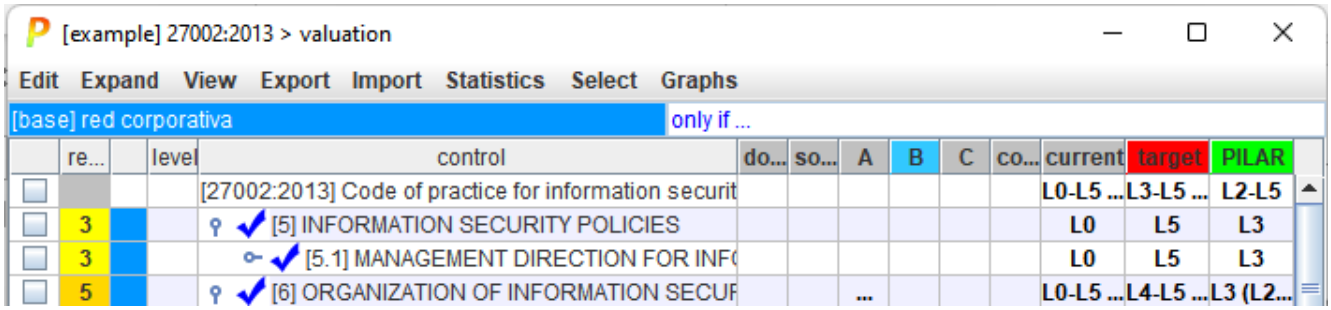
	rec...		control	do...	so...	ap...	co...	current	target	PILAR
☐			[27002:2013] Code of practice for information security controls					L0-L5	L2-L5 ...	L2-L5
☐	2		[5] INFORMATION SECURITY POLICIES					L0	L5	L2
☐	7		[6] ORGANIZATION OF INFORMATION SECURITY			...		L0-L5 ...	L2-L5 ...	L2-L4
☐	7		[6.1] INTERNAL ORGANIZATION					L0-L5 ...	L4-L5	L2-L4
☐	5		[6.2] MOBILE DEVICES AND TELEWORKING			...		L2	L2 (L4)	L3 (L2...
☐	5		[6.2.1] Mobile device policy					L2	L2 (L4)	L3 (L2...
☐			[6.2.2] Teleworking			n.a.				
☐			[7] HUMAN RESOURCE SECURITY			n.a.				
☐	7		[8] ASSET MANAGEMENT			...		L1-L2 ...	L4-L5 ...	L2-L4
☐	8		[9] ACCESS CONTROL					L0-L4 ...	L3-L5	L2-L5 ...

The “n.a.” means that the row does not apply. The dots mean that something below in the tree does not apply.

When you select a control row and click “n.a.”, every control under it becomes “n.a.”.

Applicability stages

When there are more than one applicability stages, the previous options apply independently to each one. You will have a column for each stage, while the current stage is highlighted in blue

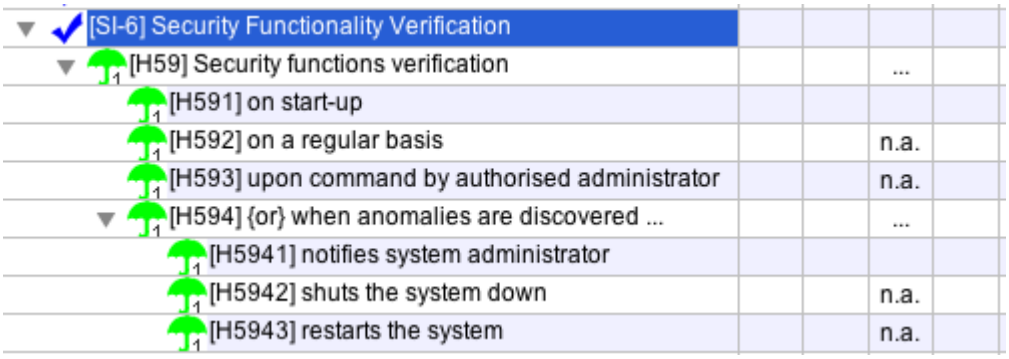


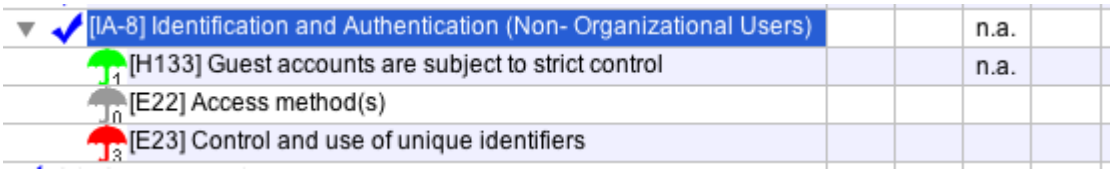
You may click on applicability stage headers to select the current one.

Safeguards

The applicability of safeguards is better stated in the specific screen for safeguards. 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.

Altogether, you may have any combination of controls and safeguards that apply or not. For instance

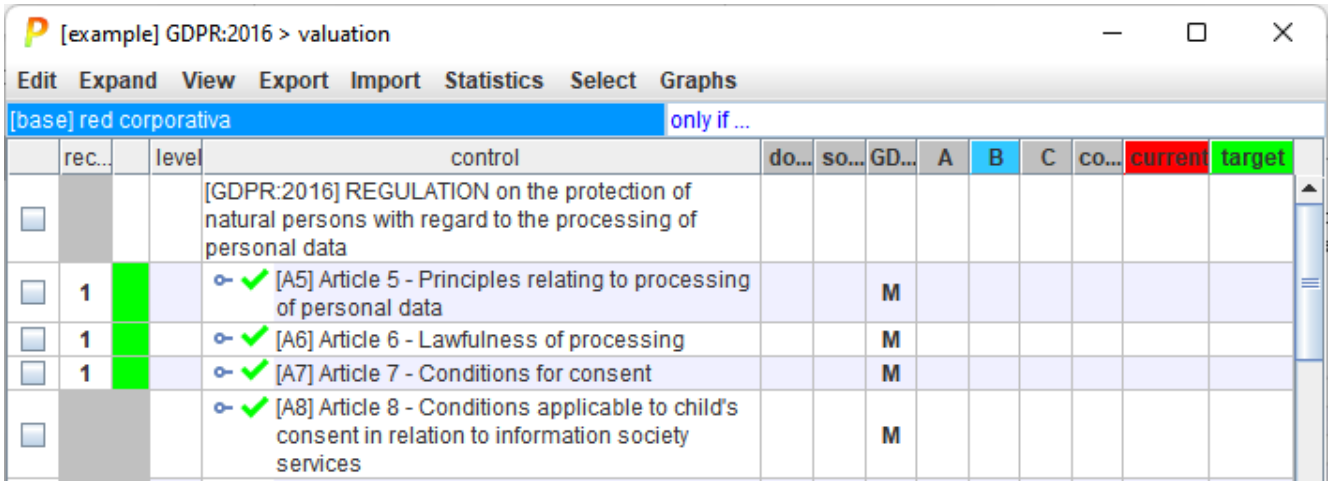




9.6 EVL – Mandatory controls

Some security profiles impose the obligation to meet some controls. It is a matter of compliance, and it may be conditional (e.g., if you have external communications, you shall …). When these compliance requirements are known, PILAR adds an applicability column

For instance, for GDPR:



9.7 EVL - Valuation

For the controls and safeguards that apply, you may specify a valuation in each project phase.

For elements without sub elements, a simple value is presented; e.g. L3.

For elements with sub elements (expandable), a range is presented.

[AC.1.1] There is a policy on access control					_-L3	L0-L3	L2
[AC.1.1.1] Security and business requirements are taken into account						L0	L2
[AC.1.1.2] Types of access and reasons for changing access rights					L2	L3	L2
[AC.1.1.3] The grounds for changing access rights are defined					L2	L3	L2
[AC.1.1.4] Review of the policy					L3	L3	L2

When the element is a control or safety measure, PILAR distinguishes between a technical assessment and an official assessment. The technical evaluation is calculated by PILAR from the associated safeguards and is presented within parentheses. The official evaluation is introduced by the user and is presented outside the parentheses. Each of these ratings can be a simple value or a range. When the official assessment and technique are the same, only the official one is presented. For example

L3 (L3) is simplified to L3

For example:

[9.1.1] Access control policy					L1 (_-L3)	L4 (L0-L5)	L3 (L2-L3)
[AC.1.1] There is a policy on access control					_-L3	L0-L3	L2
[AC.1.1.1] Security and business requirements are taken into account						L0	L2
[AC.1.1.2] Types of access and reasons for changing access rights					L2	L3	L2
[AC.1.1.3] The grounds for changing access rights are defined					L2	L3	L2
[AC.1.1.4] Review of the policy					L3	L3	L2
[H.ST.3] Segregation of tasks into roles			...		L2	L5	L2-L3
[9.1.2] Access to networks and network services					L1	L5 (L4)	L2

PILAR offers some shortcuts to quickly evaluate a set of measures and safeguards:

- when a safeguard with sub elements is valued, the value is propagated to the sub elements
- when a measure with sub elements is valued, the value is propagated to the sub elements, in a controlled manner
    - if the sub-element is another measure, it propagates
    - if the sub-element is a reference to a safeguard, it depends on the configuration option *Risk treatment*
- the values of the measures can be manually "pushed down" to the sub-elements
- the values of the safeguards can be manually "pulled up" to the measures.

The simplest way to proceed is to let the PILAR itself propagate the maturity values from the controls to the safeguards and vice versa. This automation can be selected in the *Risk treatment* panel.

In XOR type elements, we must indicate which option is selected within the possible ones.

On the valuation cells, you may move maturity value from one phase, security domain, or project, to another:

copy tree

PILAR copies the maturity of the cells in the current row, and in the corresponding sub-tree, to be pasted later

paste tree

PILAR pastes the values copied before

Note that the values can go from one phase to another phase, from one domain to another, and even from one project to another project; but they always apply to the same sub-tree.

Please, note as well that copy-paste only works within the application. You may not copy in PILAR and paste in another application.

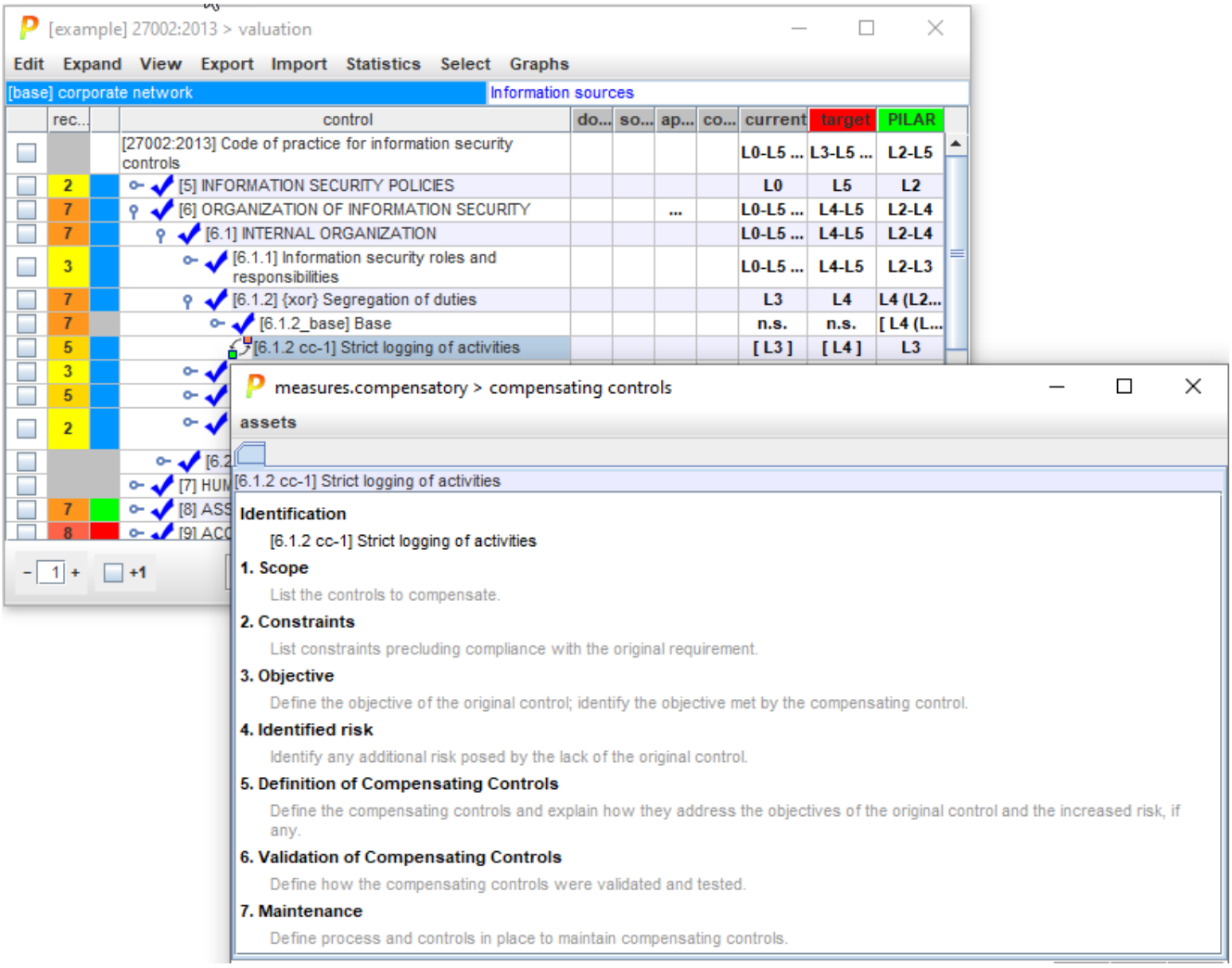
9.8 EVL – Compensating controls

The purpose or security objective of a control may be achieved by different means than those stated in PILAR. In PCI-DSS standard, there is a notion of “compensating controls”, described as

> *“Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of compensating control.”*

The core concept is that the purpose is achieved by alternative means.

In PILAR, the user has the option to disconnect a control from its children. Right click on the control for which you plan a compensating approach, and describe it:

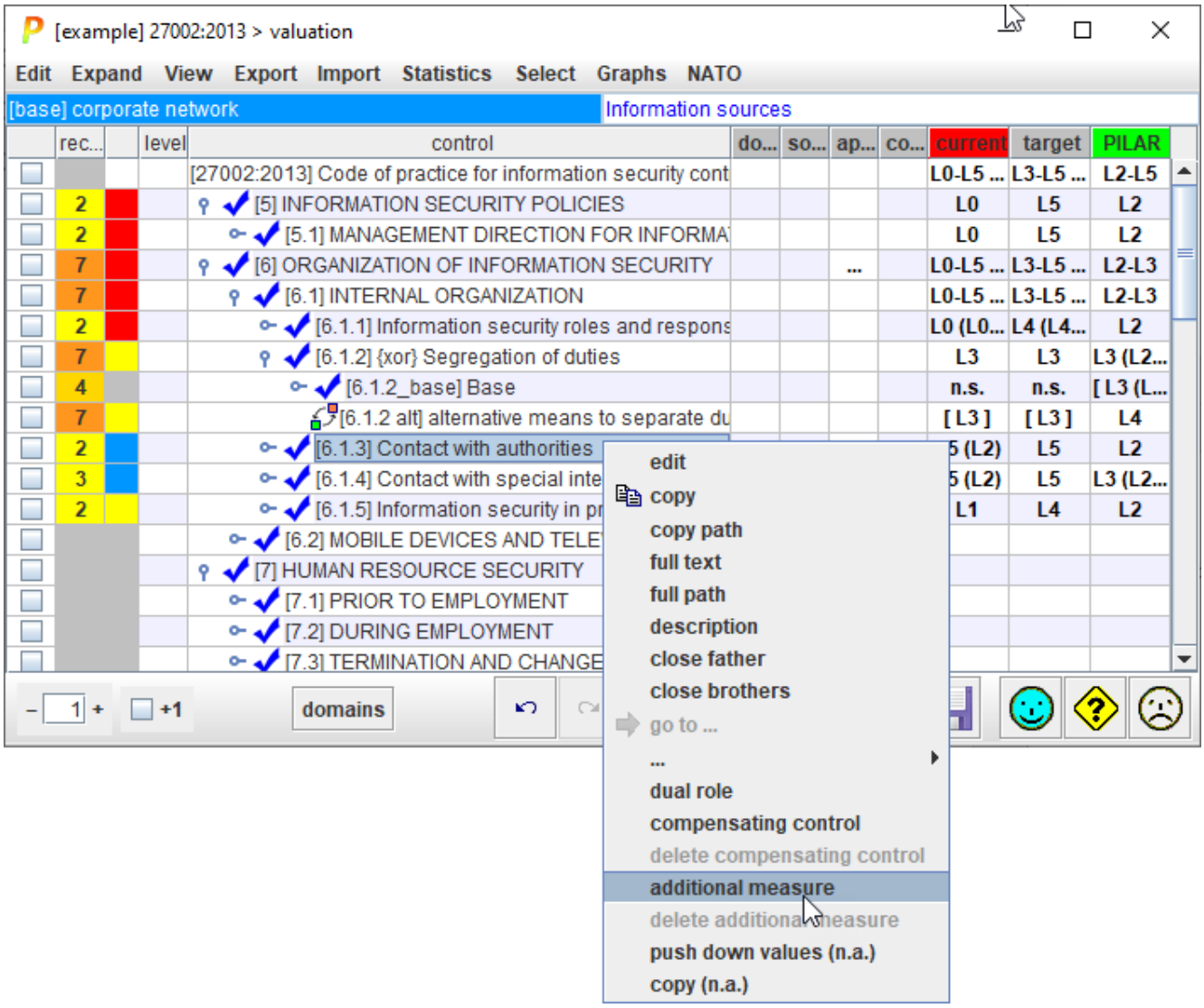


The selected control is marked as “compensated” and it can be selected and evaluated independently of its children.

Please note that the risk analysis, using PILAR safeguards still applies, to evaluate the residual risk achieved with the actual protection system.

9.9 EVL – Additional measures

You may extend the collection of controls with additional ones. These new controls may consider additional safeguards to be applied for risk treatment. The new controls may be narrowed to be applicable to some asset classes and threats.



For the new control you may specify

code (mandatory)

a unique code to identify the new control

name

a short 1-line description

asset classes (optional)

zero or more asset classes; the new control will be applied only to risks involving an asset of any of the enumerated classes

threats (optional)

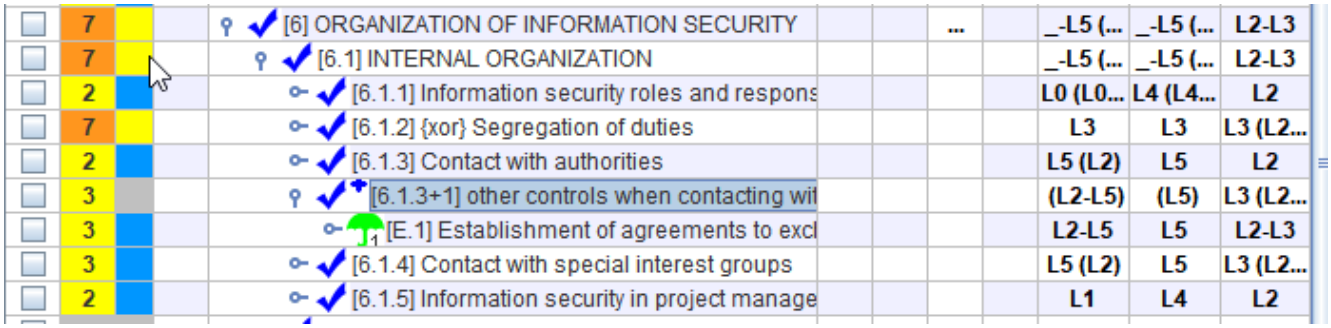
zero or more threats; the new control will be applied only to risks involving any of the enumerated threats

safeguards (optional)

zero or more safeguards from the catalogue (either PILAR or NIST); the new control may pull-up, push-down, or just compare its valuation with that of the enumerated safeguards

description

a longer description of the control



9.10 EVL - Reference and target phases

The traffic light gives a fast indication on whether the level of maturity is enough or not.

To calculate the colour of the light, PILAR uses 2 references:

GREEN: target maturity

- click the right button at the header of the phase to use as target

RED: assessed maturity

- click on the header of the phase you want to use as assessed

Using the above information, PILAR chooses a colour:

traffic light colour code	
BLUE	if the maturity at the RED phase is higher than the maturity at the target (GREEN) phase
GREEN	RED maturity is aligned with target
YELLOW	the RED maturity is poor: should be enhanced
RED	the RED maturity is too poor: must be enhanced
GREY	if the safeguard does not apply

9.11 EVL – Valuation by phases

Top menu EDIT

find	search text in tree
question	jumps to next question in tree
options	See *Edit_options*

Top menu EXPAND

controls	Expands tree to show controls

questions	Expands tree to show questions
safeguards	Expands tree to show safeguards
dual role	Selects those safeguards that contribute to two or more controls
n.a.	Expands tree to show not applicable controls
{xor}	Expands tree to show alternative options, to select
perimeter	See *Perimeters*

Top menu VIEW

maturity	Show maturity levels; either simple values, or a rank when children are of different maturity.
~maturity	Show maturity levels; when children have different maturities, an average is shown.
percent	A percent, between 0% and 100%, taking safeguards as source.
PILAR	A percent, relative to column PILAR.
one line	For tree entries that require more than one line, show only first line.
one paragraph	For tree entries that require more than one line, show full text

Top menu EXPORT

CSV	The visible rows are copied to a CSV file
XML	The values are copied to an XML file
database	The values are copied to an external database (if license allows database access)
SoA	A report is generated with the controls that apply (Statement of Applicability)
report	The values are copied to a textual file (RTF or HTML)
report (< Lx)	A report is generated with the safeguards below a given threshold
report (< target)	A report is generated with the safeguards below target phase.See "*Safeguards / Reference and target phases*" below.
report (suggest)	Generates a report with suggested improvements. It compares selected phase with extra phase and prints both maturity values. Results are grouped by controls, and sorted.

Top menu IMPORT

from CSV	Read maturity values from a CSV file
from XML	Read maturity values from an XML file
from EVL	from other profile (evl)

import (mgr)	
import (db)	

To import from another project, PILAR presents a list of possible sources and destinations. Sources are security profiles in the project to import. Destinations are security profiles in this project. Sources and destinations are linked by profile code, and by association files.

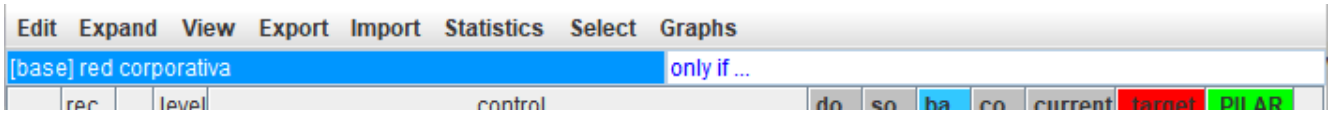
Top menu SELECT

clear	clear selection
level 1	select controls on tree level 1
level 2	select controls on tree level 2
level 3	select controls on tree level 3
current situation	select controls currently visible
mandatory	select controls that are mandatory
project phases	select phases for graph

Top menu GRAPHS

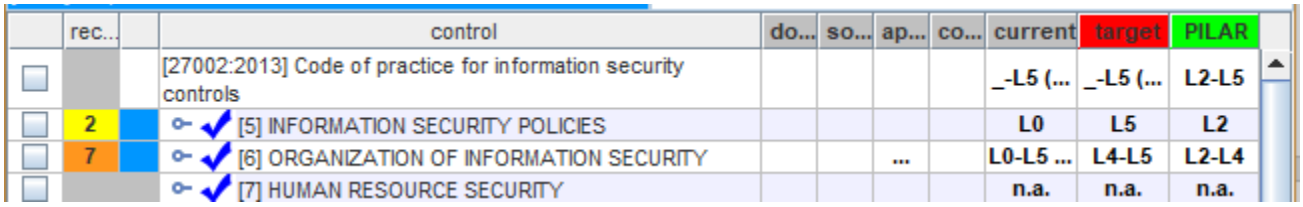
draw	Drawing with the current selection of rows and phases.

Top bands



security domain	There may be different controls for different domains. Click to select the domain you want to edit.
only if …	Click to select some controls based on attributes. After that, PILAR will prune the tree to show only the parts of the tree related to the selected items. You may select different criteria to match • controls that apply or that do not apply • information sources • applicability level

Table columns



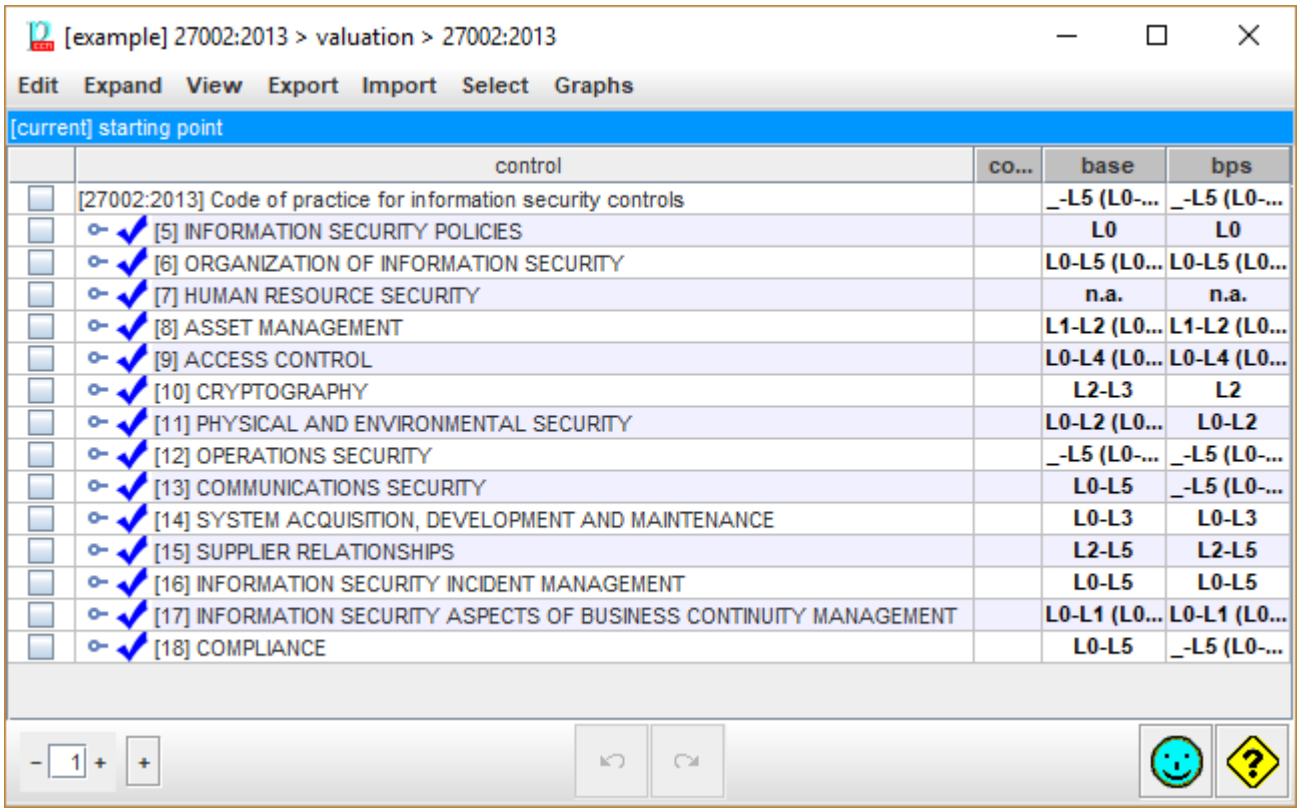
1	select	Selects rows for graphs. Click on checkboxes to check / uncheck. SHIFT-click to check a range. Click on column header to clear current selection.
2	recommendation	It is a rank in the range [null .. 10], estimated by PILAR taking into account the assets, the security dimensions, and the level 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").
3	traffic light	Compares valuation in reference phase (RED) with valuation in target phase (GREEN), and shows a colour: 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 See "*EVL / Reference and target phases*" below.
4	controls	Presents hierarchically the controls in the security profile, and the mapping onto safeguards. You double click to collapse / expand the tree. You may right-click to access to tree menu.
5	doubts	Click to mark / unmark the row. The mark is typically used to remember that there are issues waiting for an answer. The mark "floats" to the top level to highlight the problem.
6	sources	Click to associate information sources to the row and its children.
7	applies	See *EVL / Applicability*
8	comment	Click to associate comments to the row.

9 …		Project phases. Left-click to select reference phase (RED). Right-click to select target phase (GREEN). • See "*EVL / Reference and target phases*" • See "*EVL / Valuation*

Bottom toolbar

	Spinner to control the expansion of the tree
	Modifies the behaviour of spinner. If selected, the expansion includes mapped safeguards. If unselected, expansion stops before presenting safeguards.
domains	See *EVL / domain*
	Undo last changes.
	Redo last undone changes.
suggest	Presents a sorted list of controls that deserve improvements. In order to sort, PILAR takes into account the relative importance if the control and the maturity gap between current phase and target phase.
	Saves current project either in a file, or in database (according to its source).

9.12 EVL - Valuation by security domains

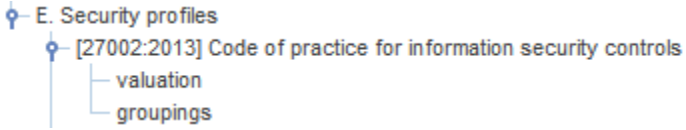


control	co...	base	bps
[27002:2013] Code of practice for information security controls		_-L5 (L0-...	_-L5 (L0-...
[5] INFORMATION SECURITY POLICIES		L0	L0
[6] ORGANIZATION OF INFORMATION SECURITY		L0-L5 (L0...	L0-L5 (L0...
[7] HUMAN RESOURCE SECURITY		n.a.	n.a.
[8] ASSET MANAGEMENT		L1-L2 (L0...	L1-L2 (L0...
[9] ACCESS CONTROL		L0-L4 (L0...	L0-L4 (L0...
[10] CRYPTOGRAPHY		L2-L3	L2
[11] PHYSICAL AND ENVIRONMENTAL SECURITY		L0-L2 (L0...	L0-L2
[12] OPERATIONS SECURITY		_-L5 (L0-...	_-L5 (L0-...
[13] COMMUNICATIONS SECURITY		L0-L5	_-L5 (L0-...
[14] SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE		L0-L3	L0-L3
[15] SUPPLIER RELATIONSHIPS		L2-L5	L2-L5
[16] INFORMATION SECURITY INCIDENT MANAGEMENT		L0-L5	L0-L5
[17] INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT		L0-L1 (L0...	L0-L1 (L0...
[18] COMPLIANCE		L0-L5	_-L5 (L0-...

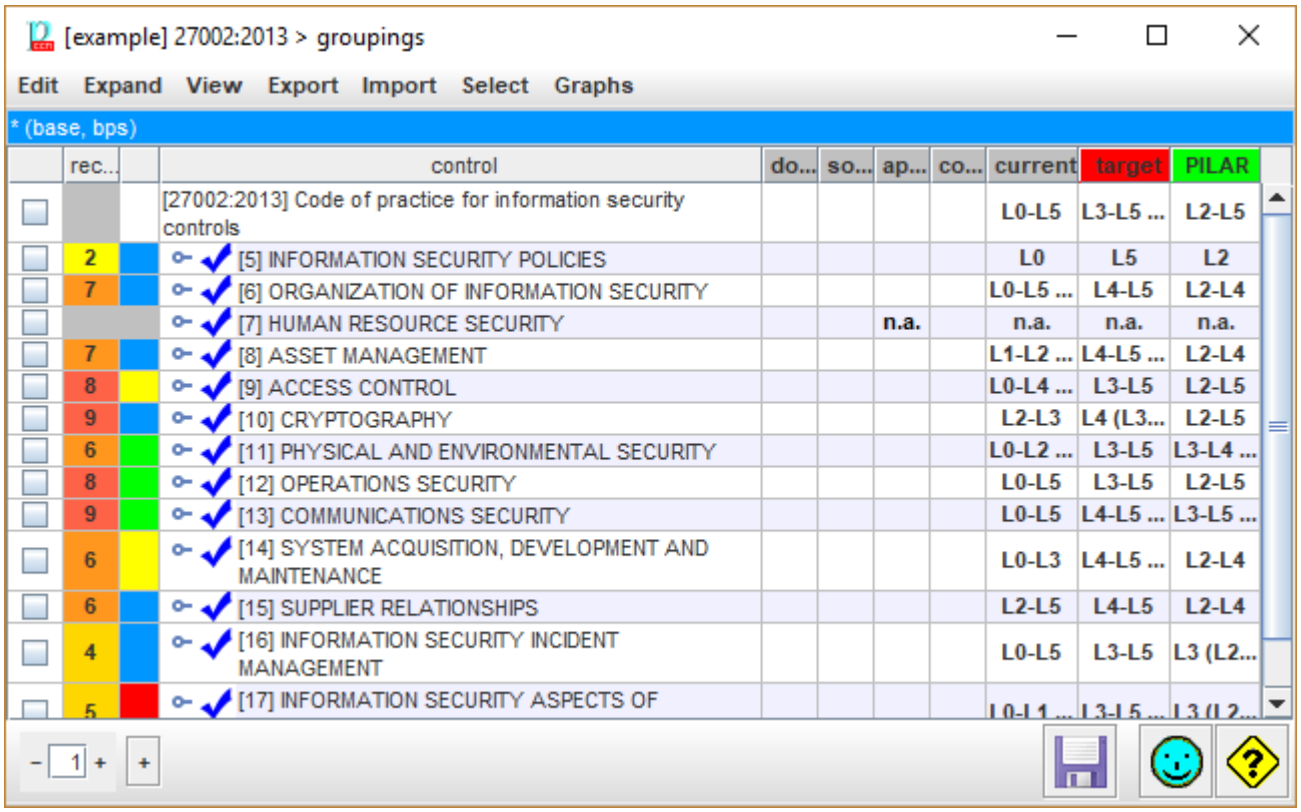
9.13 Groups of security domains

Valuation by security domains is good for details but prevents a global view of the system.

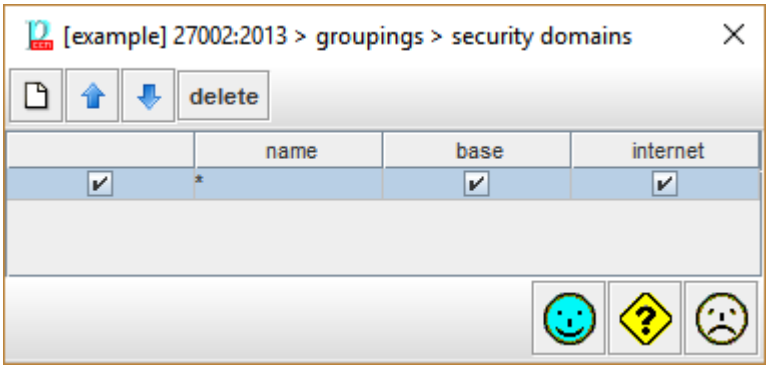
For a global view, go to groupings:



Groupings screen is quite like screens for rating, but it is view-only:

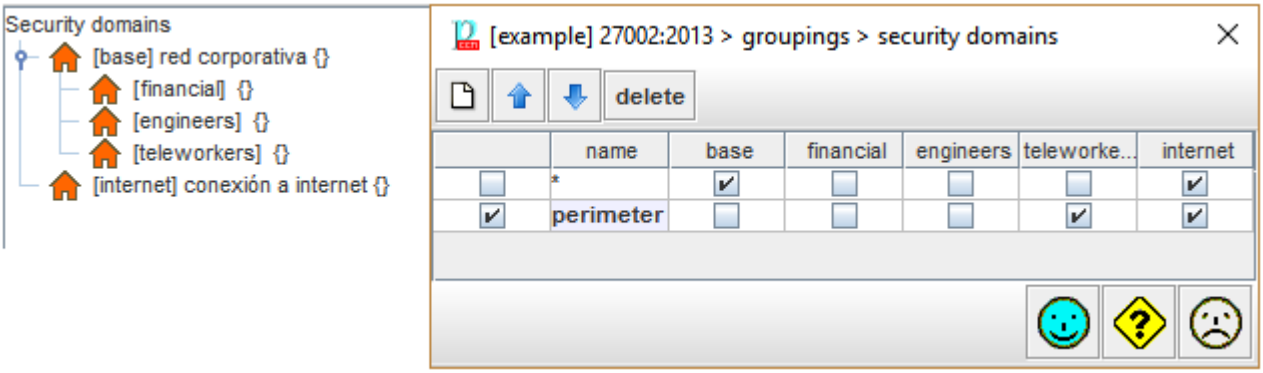


On the top blue band, you may edit and select groupings. By default, there is always a group made up of every security domain:

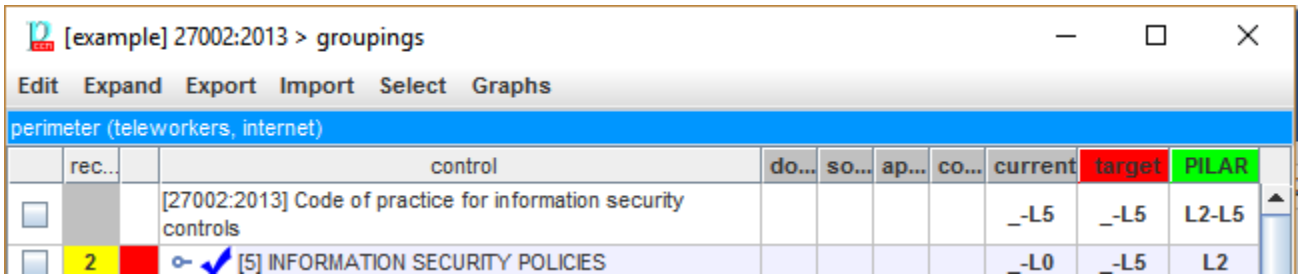


On that group, little can be done.

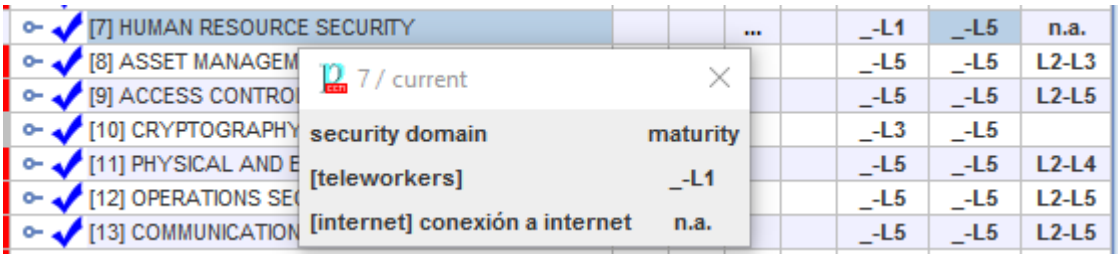
The real interest is on your own groupings when you have many domains:



Now, users may select their groupings:



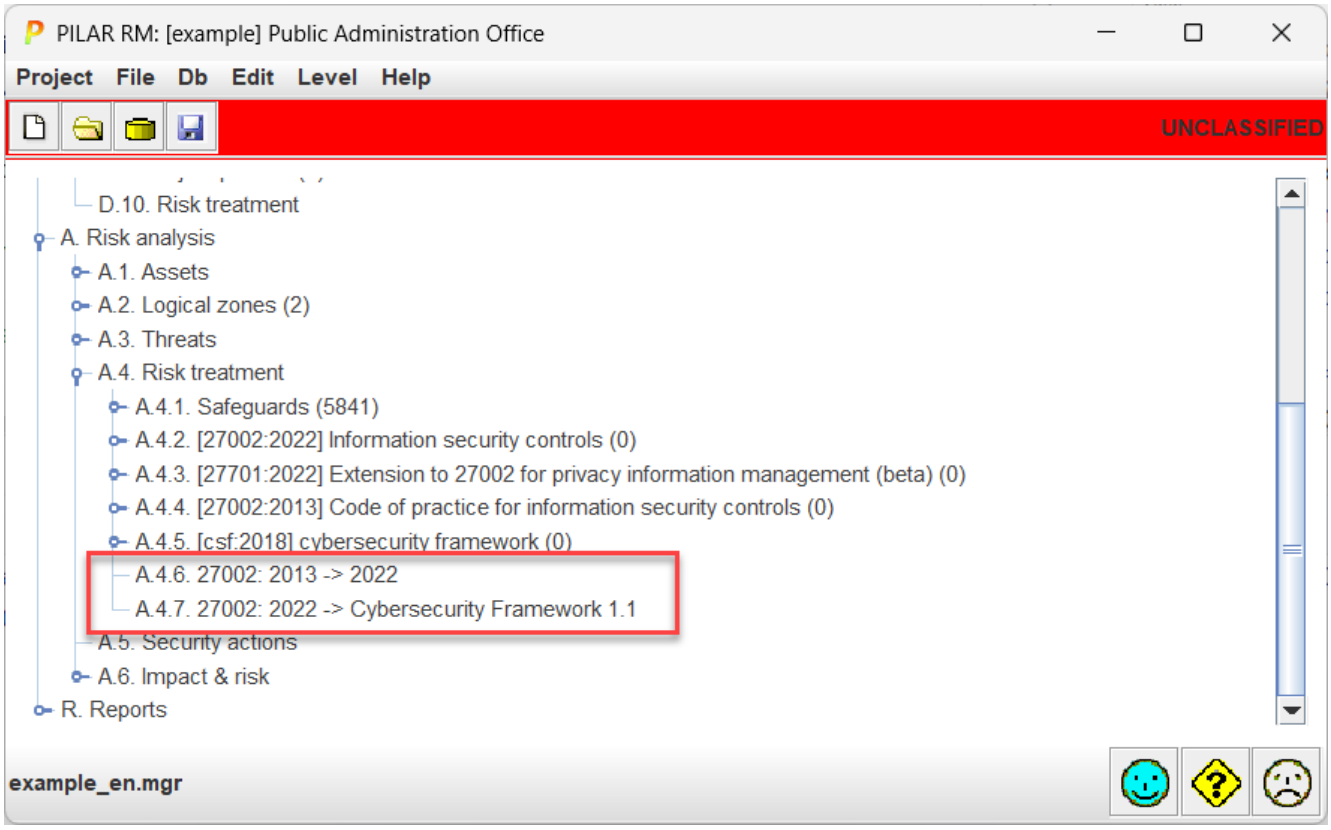
In the columns for maturity, doubts, etc., you may click to get a summary of the value on each domain. For instance:



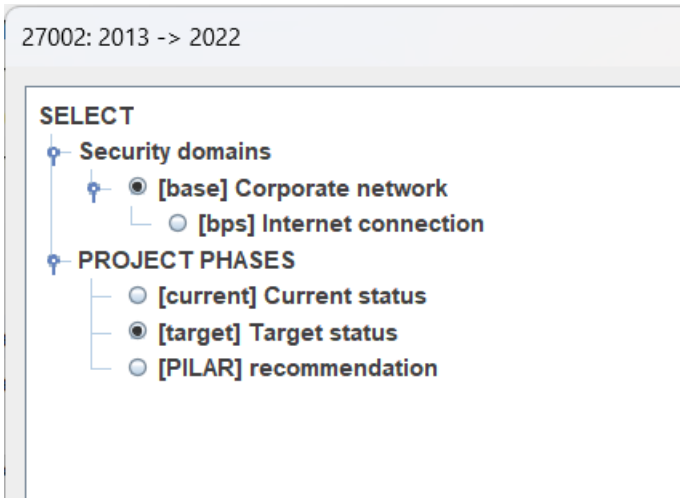
9.14 Mapping (EVL → EVL)

PILAR aligns the controls in one security profile with controls in another security profile. This functionality is useful, for instance, to estimate ISO 27002:2022 values out of already known ISO 27001:2015 values.

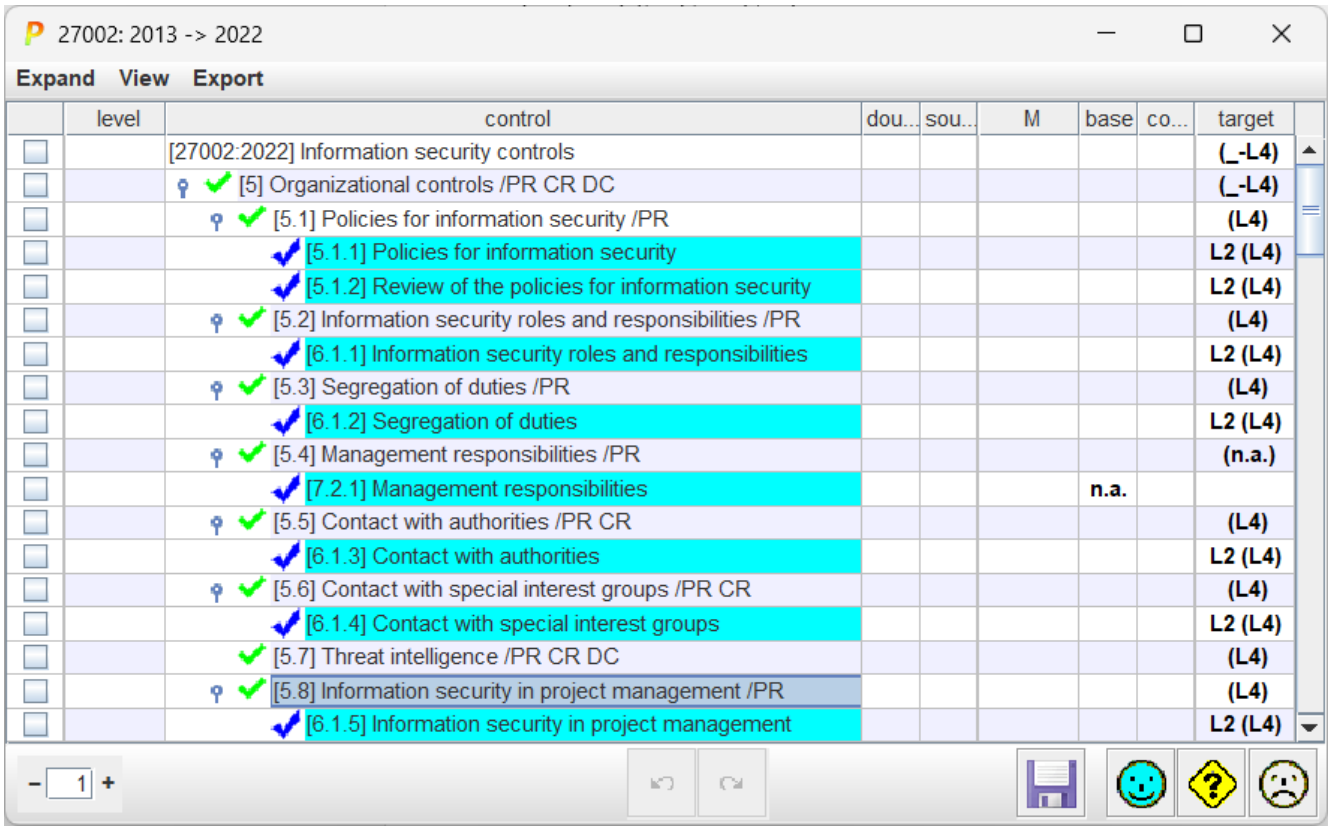
There may be several mappings available in your installation. For instance:



When you clic on one mapping, you have to select one security domain, and one phase for translating values from left evl to right evl



And then a panel shows up to transfer values:



Rows presented as black letters on cyan background are valuations of the (old) source evl.

Black on white rows are valuation os the (new) target evl.

Values between parenthesis display the valuation of the associated safeguards.

You may set maturity levels, and comments on the (new) target evl. The propagation of this values to safeguards depends on propagation setting for the corresponding profile.

You may ask PILAR to suggest a value for target taking source into account