PILAR Basic

Risk Analysis and Management

Help Files

version 2021.2

December, 2021

General

1 Edit / Options

You may modify the behaviour of PILAR in several aspects

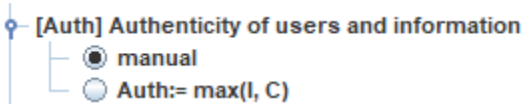
- *Options / Auth*
- *Options / Acc*
- *Options / Likelihood*
- *Options / Effects*
- *Options / Maturity*
- *Options / Special phases*

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.

1.1 Options - Authenticity

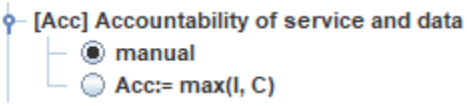
Authenticity is a valuation option in Magerit. You may valuate it explicitly or derive it automatically from other values.



The user may always enter an explicit value. This option only applies if the user leaves the valuation empty.

1.2 Options - Accountability

Authenticity is a valuation option in Magerit. You may valuate it explicitly or derive it automatically from other values.



The user may always enter an explicit value. This option only applies if the user leaves the valuation empty.

1.3 Options – Likelihood

How to describe the likelihood of a threat.

potential	likelihood	level	ease	frequency

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

1.4 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%

1.5 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

1.6 Options – Special phases

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

Select the ones you with to be shown.

2 Reports

2.1 From template

PILAR is able to 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.pilar-tools.com/doc/]

2.2 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.

Value model

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

Evaluation of safeguards

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

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

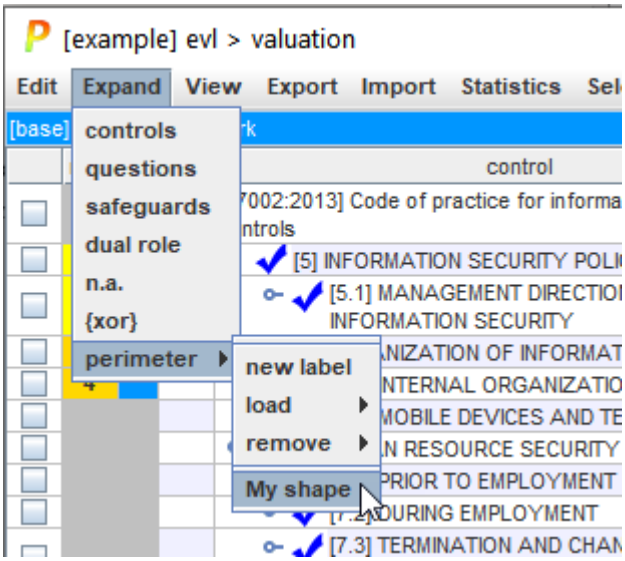
 To collapse the tree. Only first level of branching.

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

3 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`

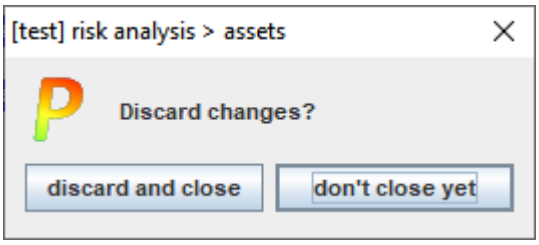
Screens

4 OK, Cancel, Help

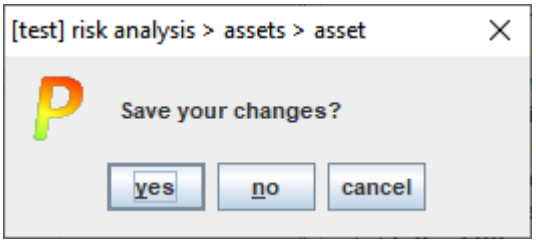
Most screens include buttons for:

	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:

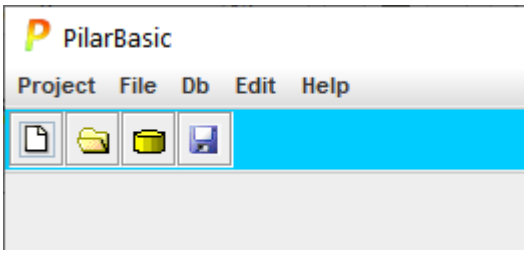


where you can

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

5 Main control panel

5.1 Basic controls



Top menu PROJECT

New	Starts a new project from scratch
Reopen	Returns to recent projects
Save	Saves current project either in a file, or in database (according to its source).
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
Save as ...	Saves a copy, where the user may select the file, and establish a password

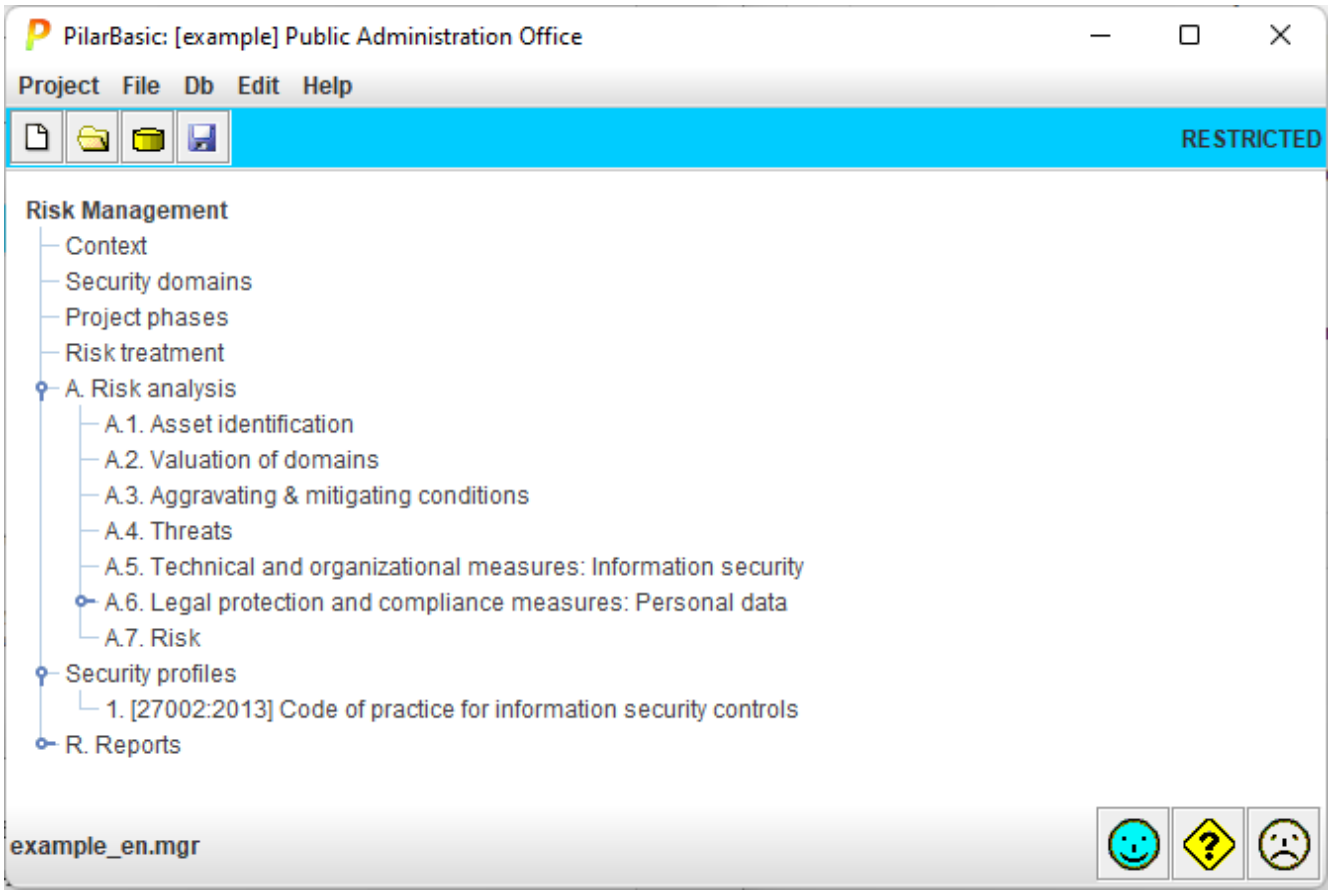
Top menu EDIT

Preferences	sets font size and family.
Options	see *Edit / Options*

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

5.2 Project controls



The bottom row presents the name of the project file.

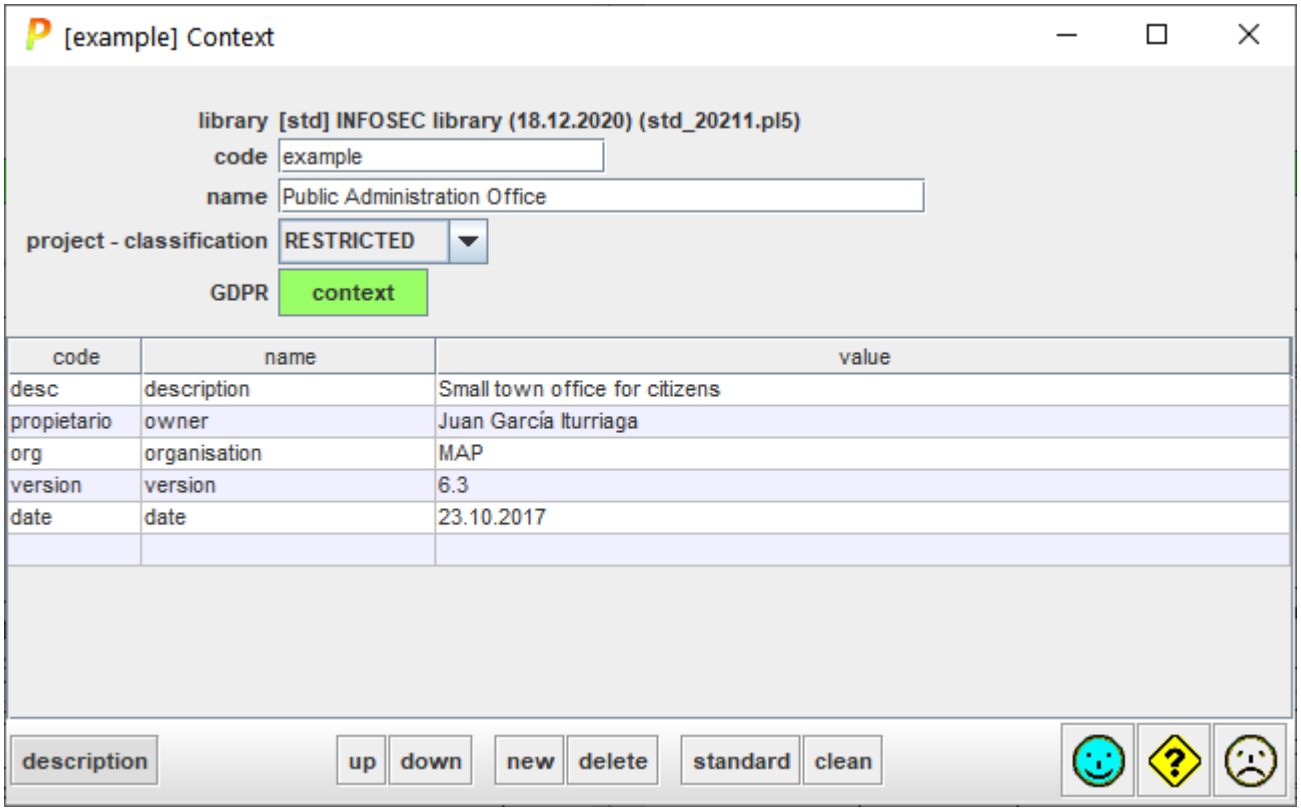
The inner tree presents the activities. Click to jump to the corresponding activity.

- *Context*
- *Security domains*
- *Project phases*
- *Risk treatment*
- Risk analysis
  - *Asset identification*
  - *Valuation of domains*
  - *Aggravating & mitigating conditions*
  - *Threats*
  - *Safeguards*
  - *Risk*
- *EVL – Security profiles*
- Reports
  - *Value model*
  - *Safeguards*
  - *Risk*
  - *From template*

6 Project

6.1 Project data

Quick start
Select a code and a descriptive name. Optionally, click **STANDARD** and add some descriptive information. 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.

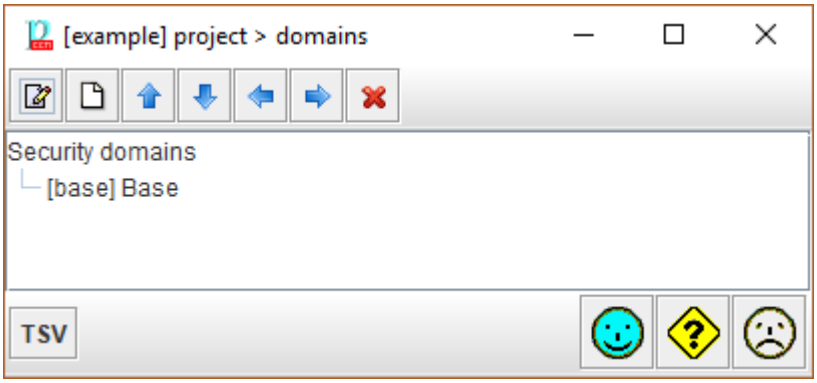
code	Key codes for key-value pairs. Useful for translations.

	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 

6.2 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.



	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.

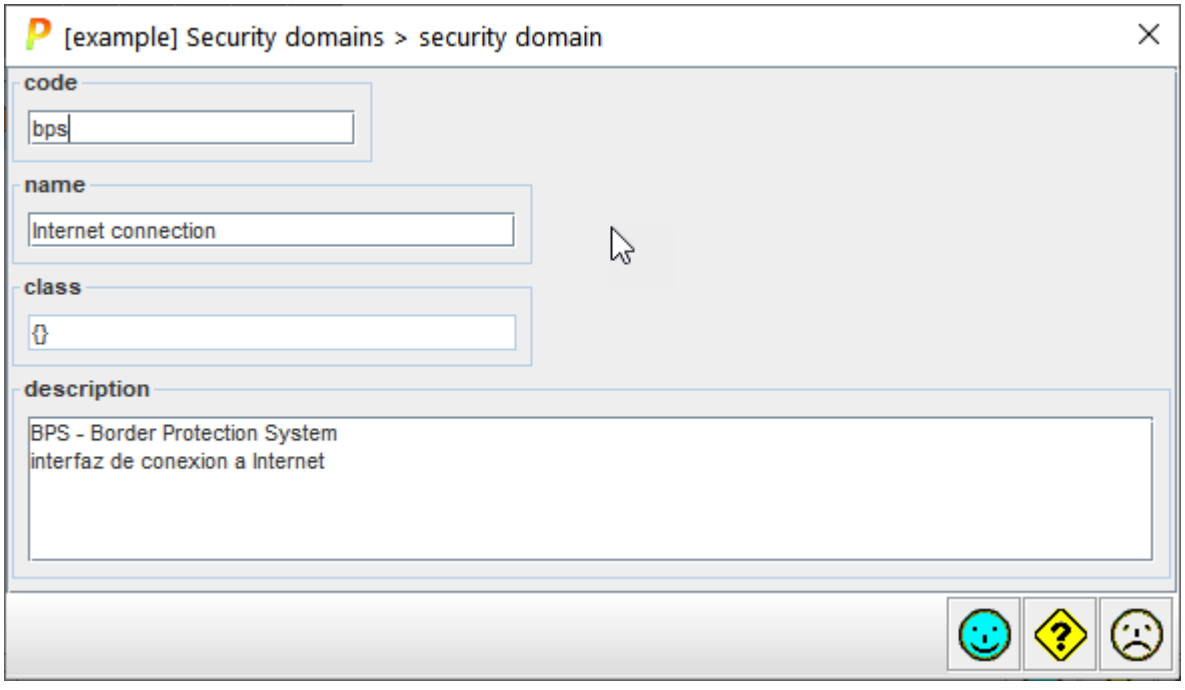
- See "*Threat Standard Values*".

6.2.1 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
— a longer description

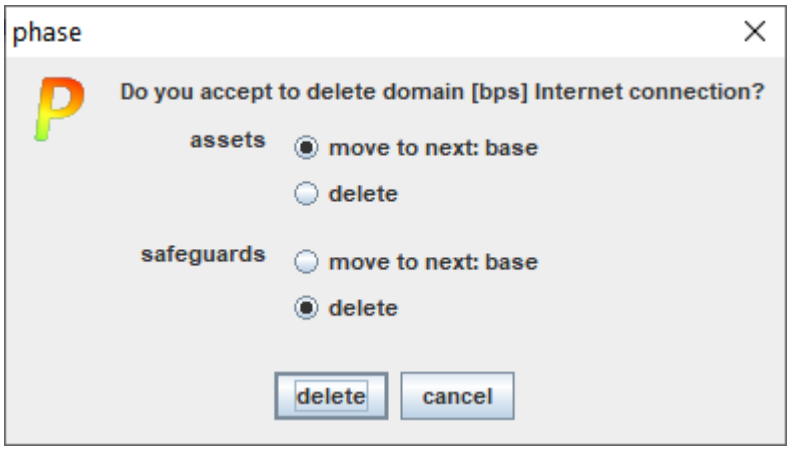
The description may include hyperlinks (URLs). To go to the linked page RIGHT-CLICK, then



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.

6.2.2 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:



6.3 Project phases

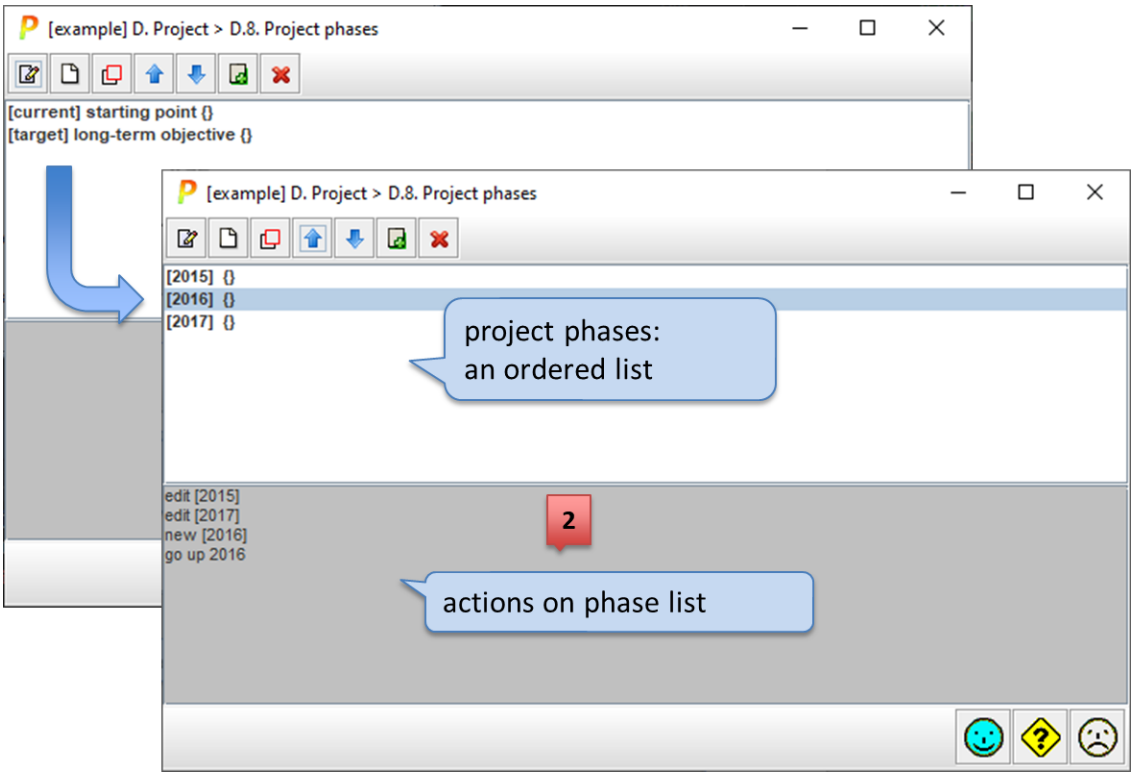
Quick start
Do nothing! The standard should be enough: • [current] the system as it is today • [target] the system you would love to have Click **OK** to continue.

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.

6.3.1 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	

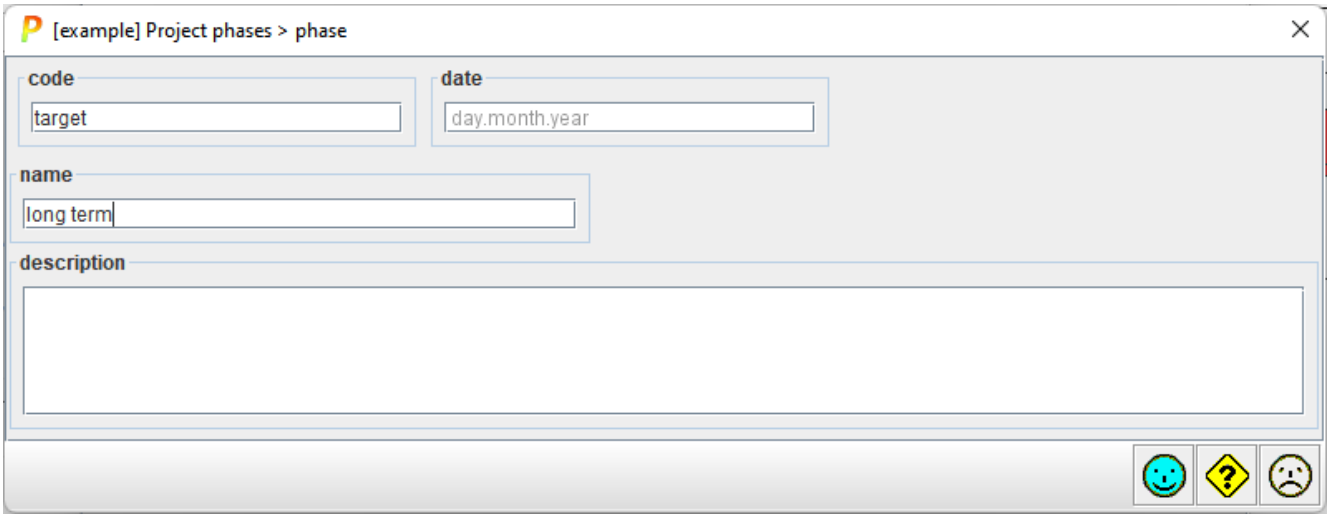
If we combine F2 + F3, the values in phase F2 that are not modified in phase F3, are copied in phase F3:

	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	

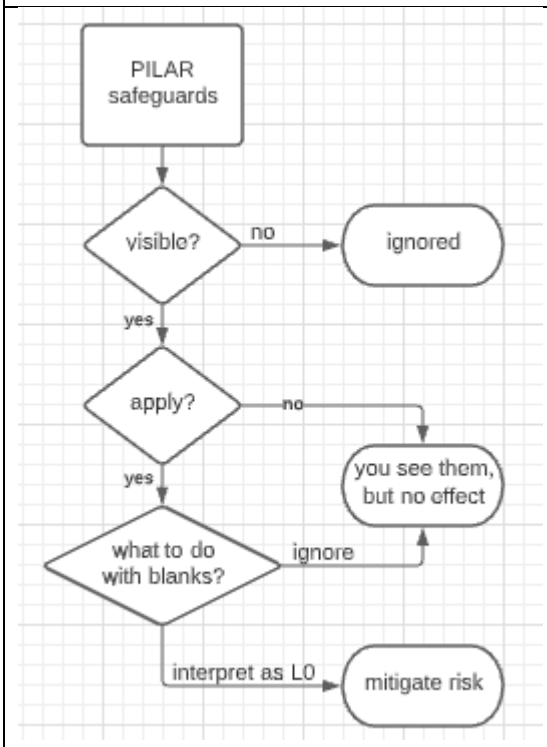
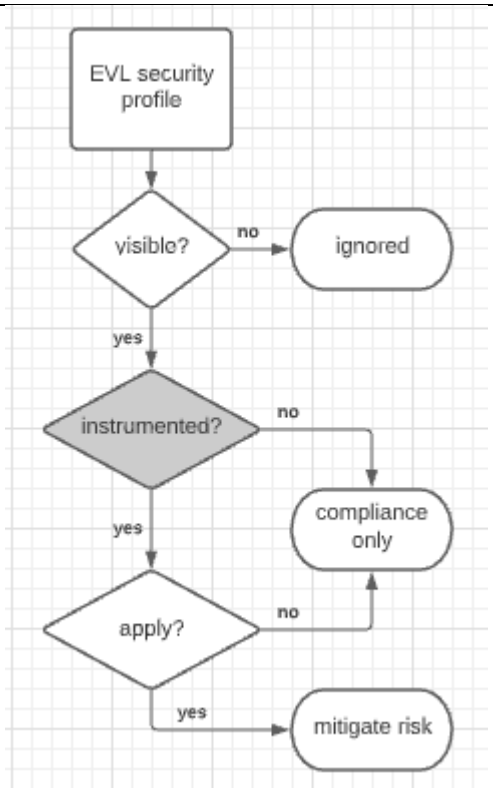
6.3.2 Edit one phase



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

6.4 Risk Treatment

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

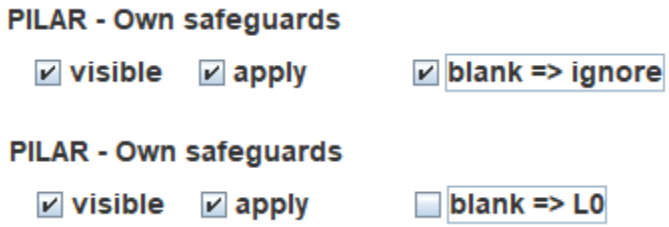
You may control how different security measures (safeguards and profile controls) are used.

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

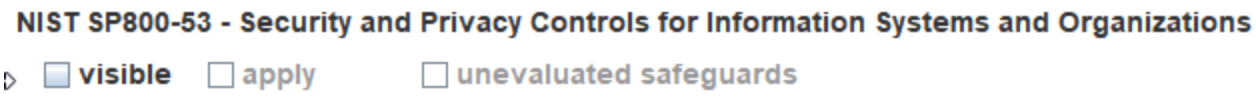
- If not visible, they are completely ignored in interface and in risk mitigation.

- 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.

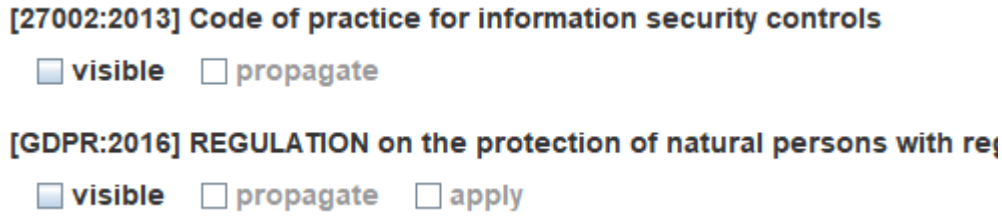


For NIST 800-53 rev.5 collection of safeguards, you have the same options:

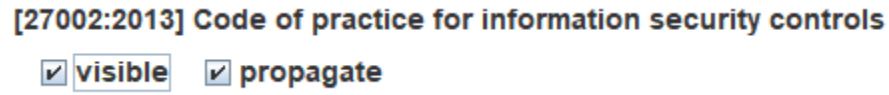


For security profiles, EVL, you may select whether they are visible o invisible.

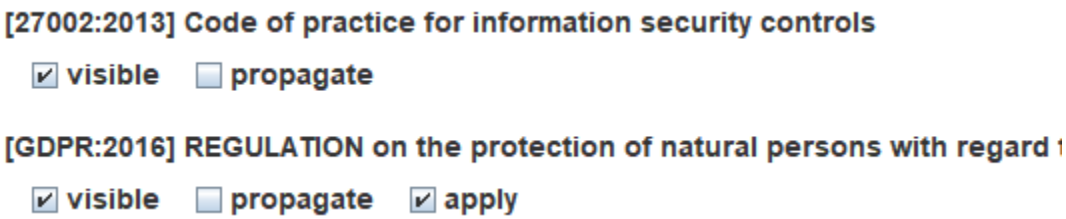
- If invisible, they are ignored.



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



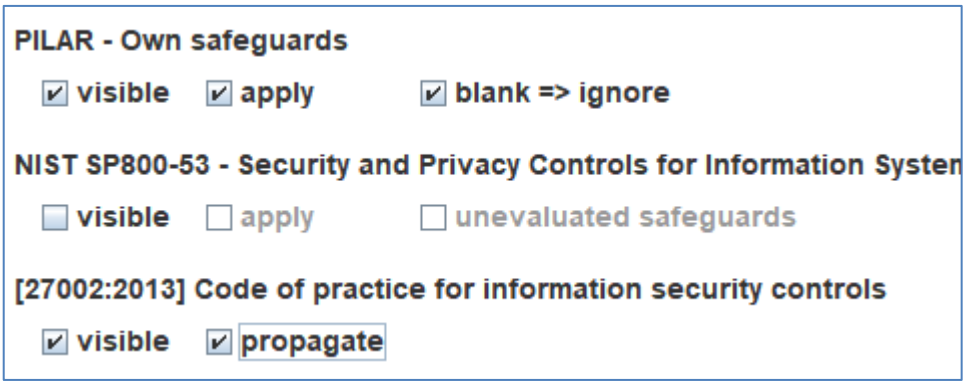
- For some security profiles, if visible, you may choose to apply their controls to mitigate risk. only some EVL are instrumented with the mitigation knowledge.



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 Risk analysis

7.1 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 only 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.

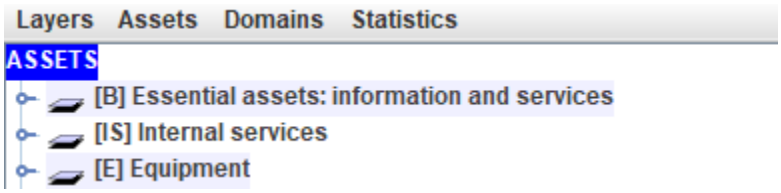
To move one layer, group or asset

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

To move one or more assets, you may select altogether 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

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.
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).

7.1.1 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

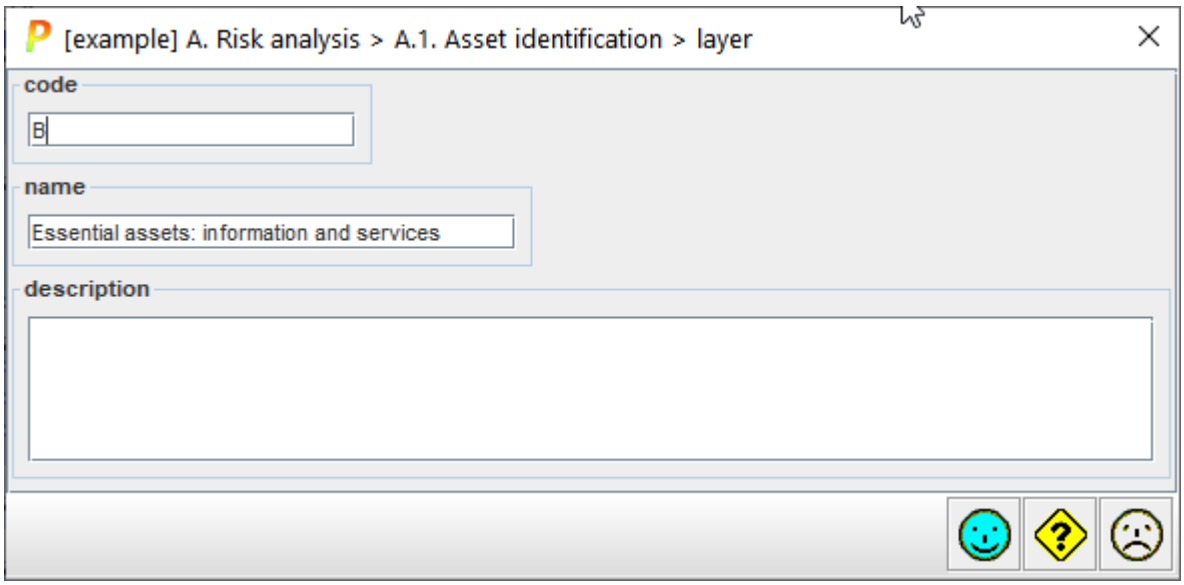
or

- 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.

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

7.1.2 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.
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.

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 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

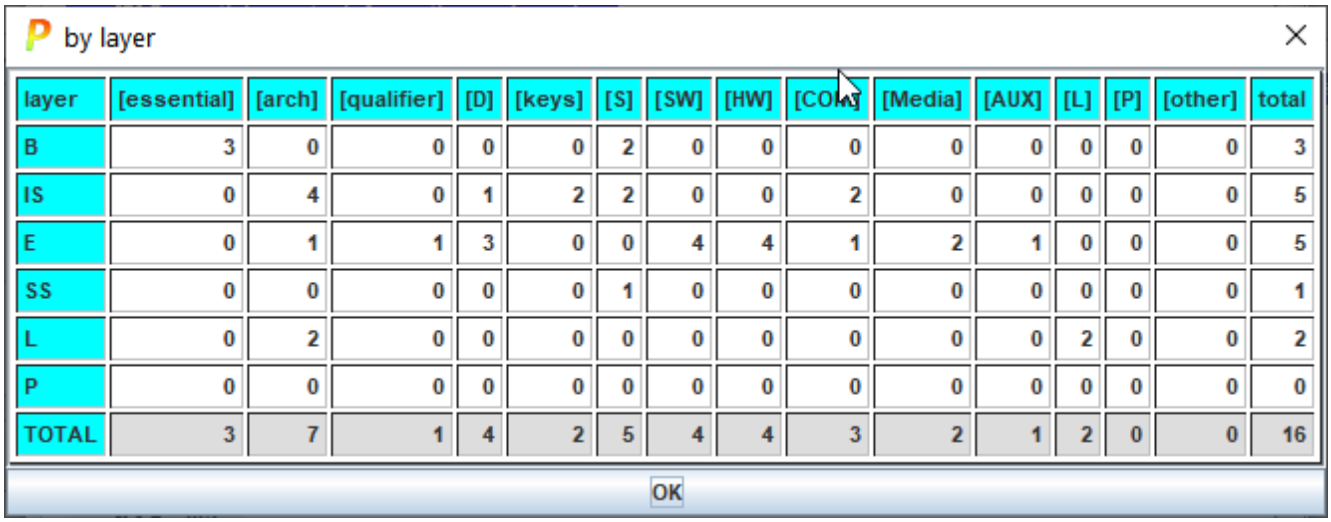
- drag & drop
- cut & paste

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

7.1.3 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 or by security domains. The outcome is like the following one:



layer	[essential]	[arch]	[qualifier]	[D]	[keys]	[S]	[SW]	[HW]	[COM]	[Media]	[AUX]	[L]	[P]	[other]	total
B	3	0	0	0	0	2	0	0	0	0	0	0	0	0	3
IS	0	4	0	1	2	2	0	0	2	0	0	0	0	0	5
E	0	1	1	3	0	0	4	4	1	2	1	0	0	0	5
SS	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1
L	0	2	0	0	0	0	0	0	0	0	0	2	0	0	2
P	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
TOTAL	3	7	1	4	2	5	4	4	3	2	1	2	0	0	16

Each column refers to a major class of assets. In column [SW] there are 4 assets with classes of this column, all of them in layer [E].

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

Table may be printed: right-click.

7.1.4 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

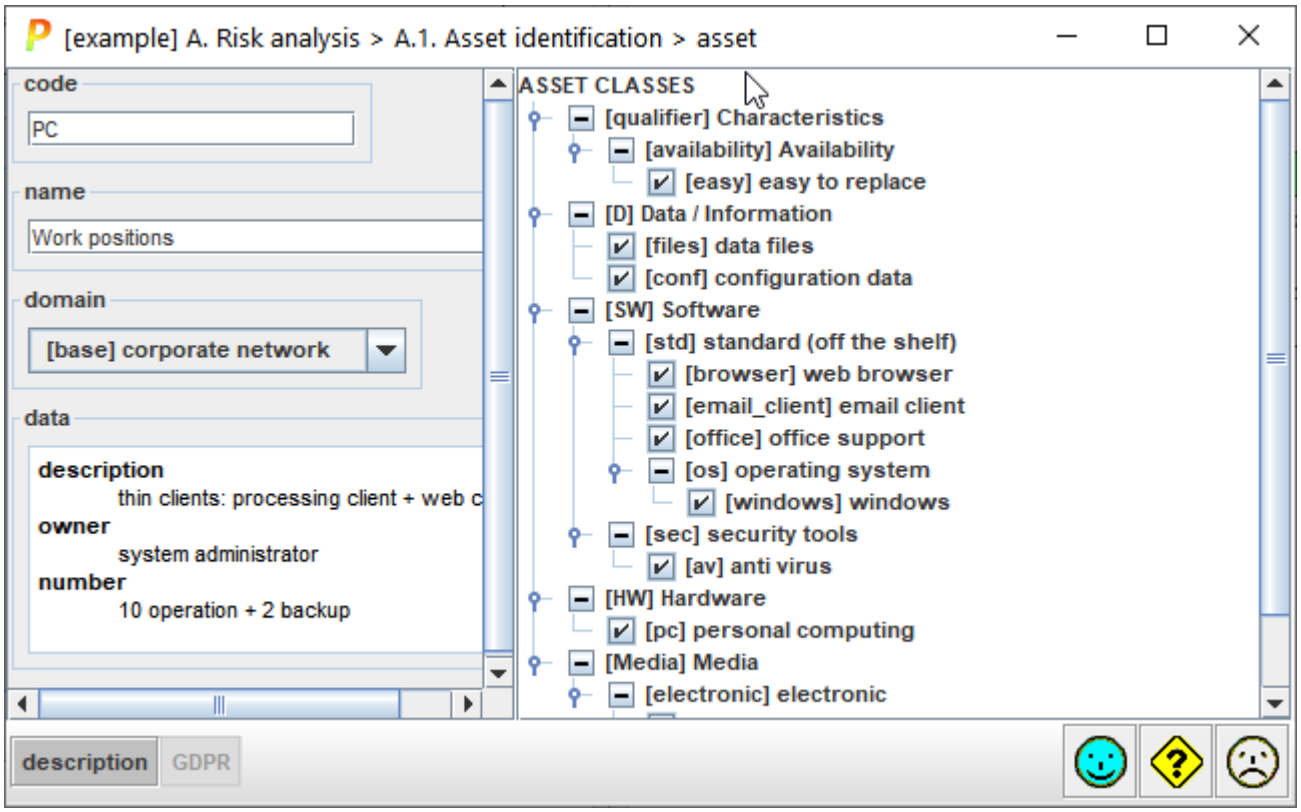
- drag & drop
- cut & paste

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

7.2 Assets / Edit one asset

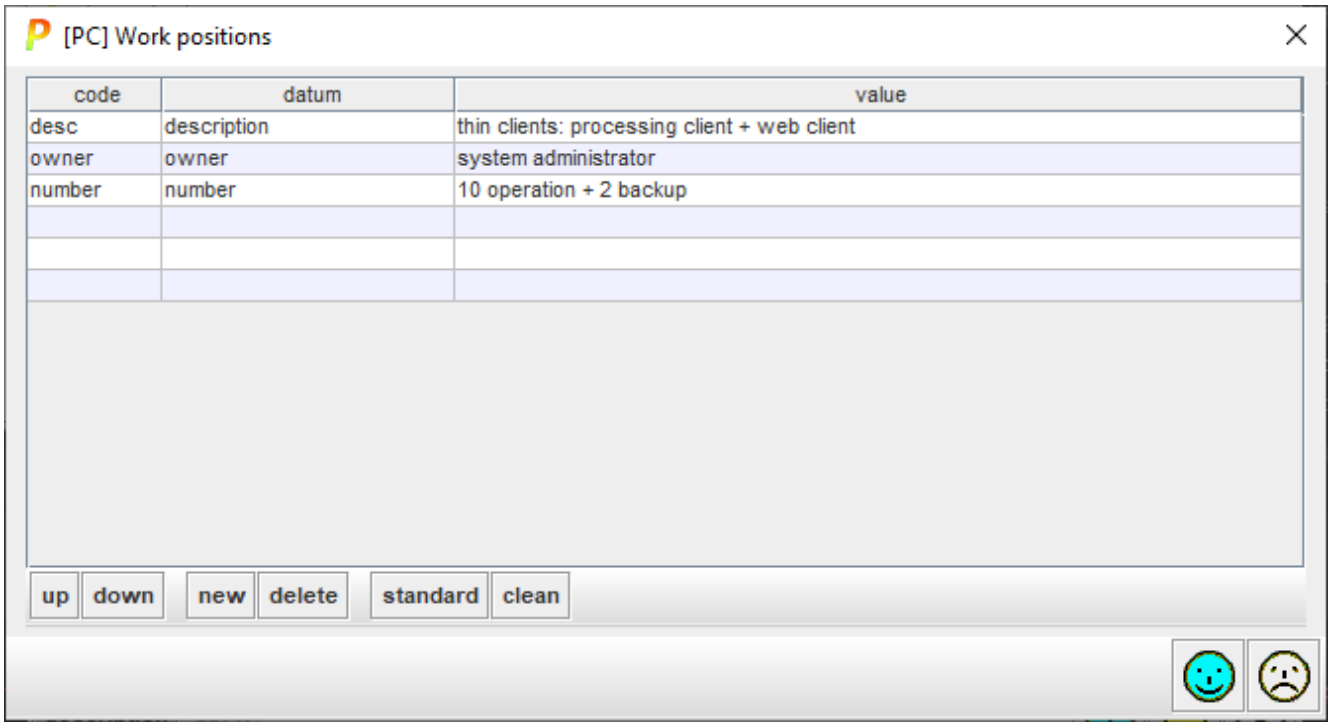
Quick start
Select a **unique code** and a descriptive name. Check on one or more classes on the right panel. Click **STANDARD** and add some descriptive information. Click **OK** to continue.



code	which shall be unique.
name	A short description: one line.
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

7.2.1 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

Classes with a mark (*) are those for which there is information on additional protections (kb).

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

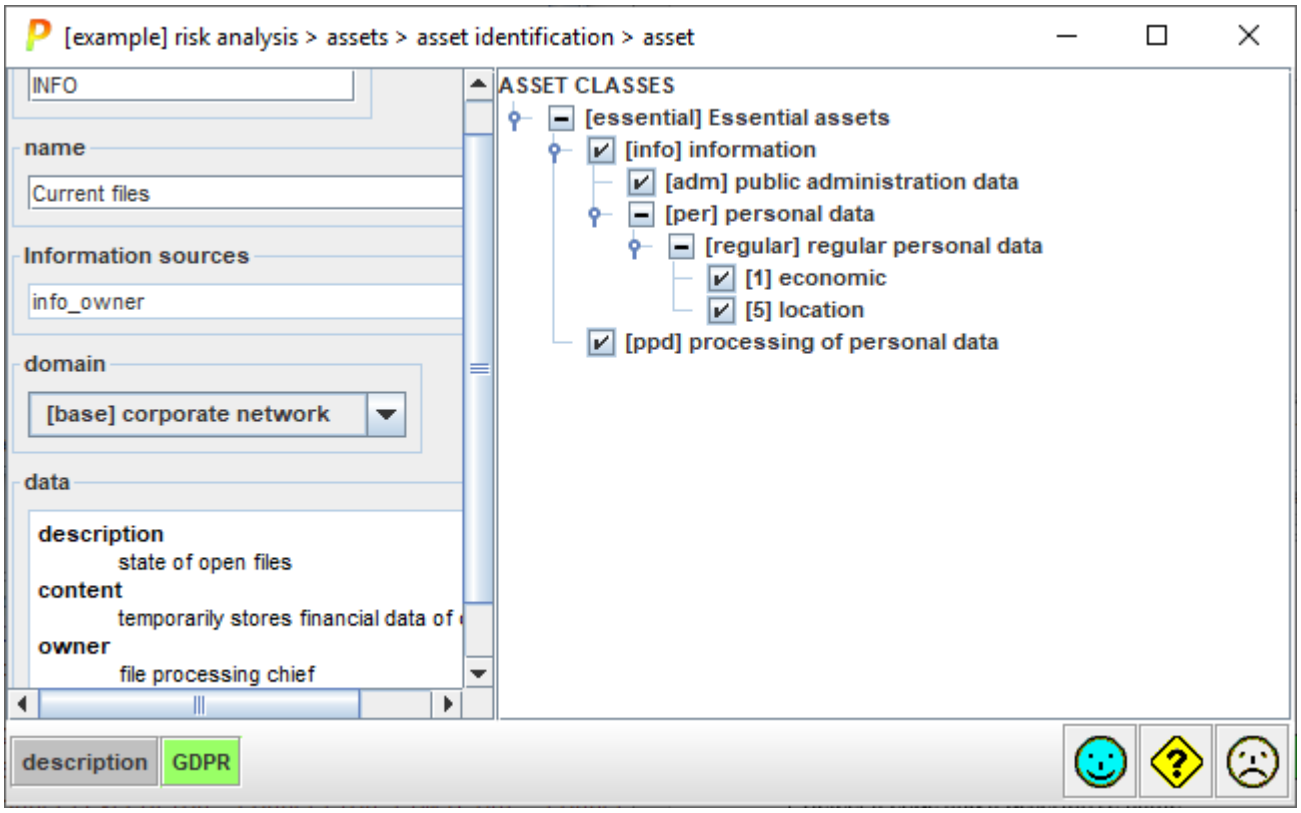
right click + CLEAN	right click + DELETE
	

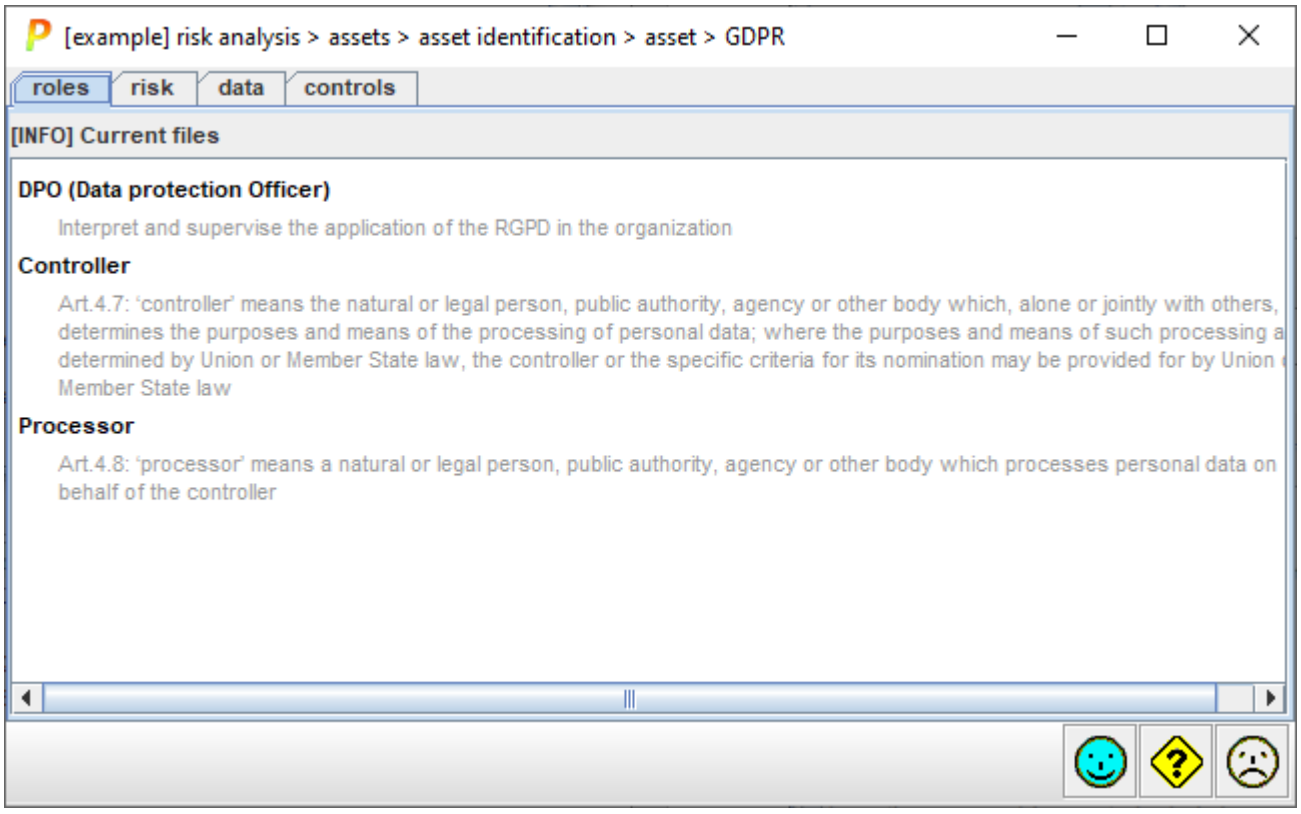
7.2.2 GDPR: privacy

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.

7.3 Assets / Valuation

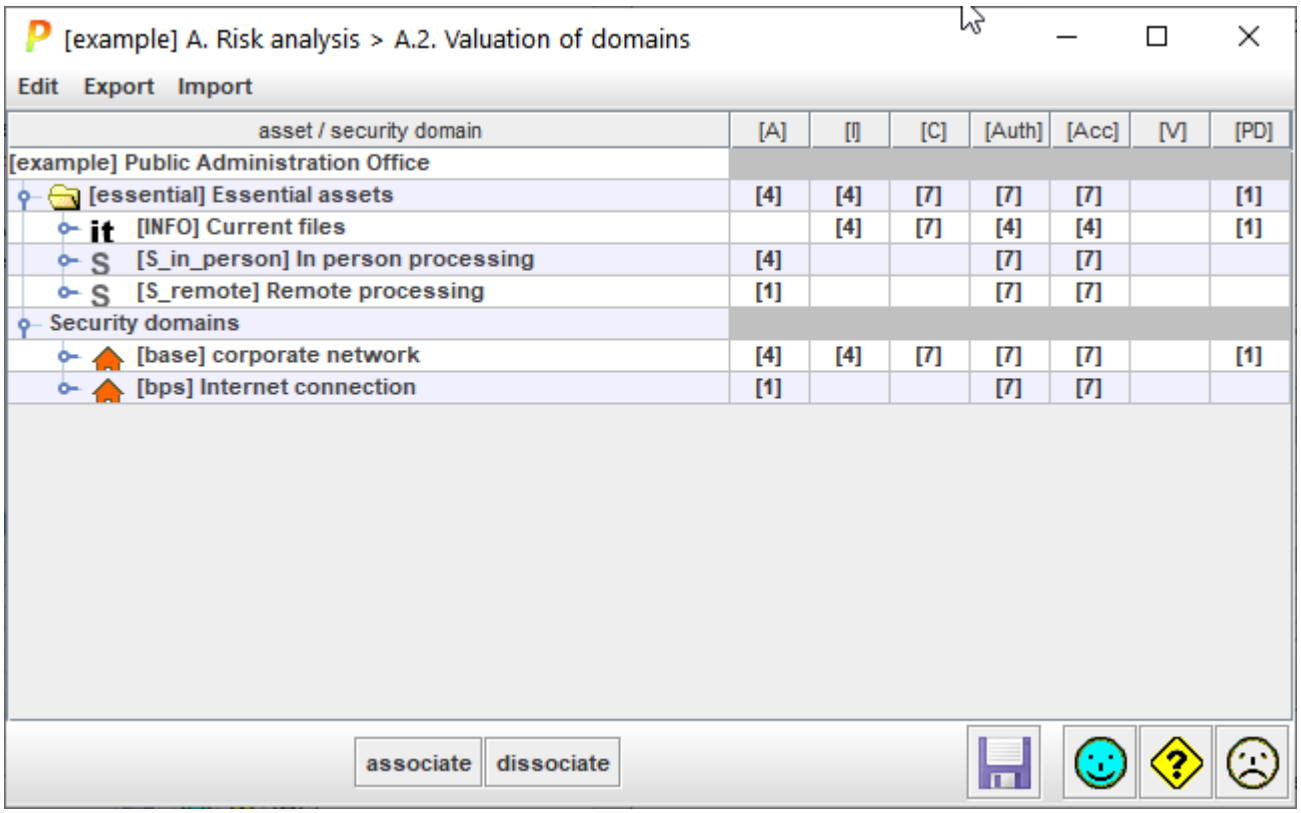
This approach provides a quick but imprecise assessment common for all the assets in each domain. It is faster than the evaluation by dependencies. Using this method, all assets in the domain receive the same values.

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.

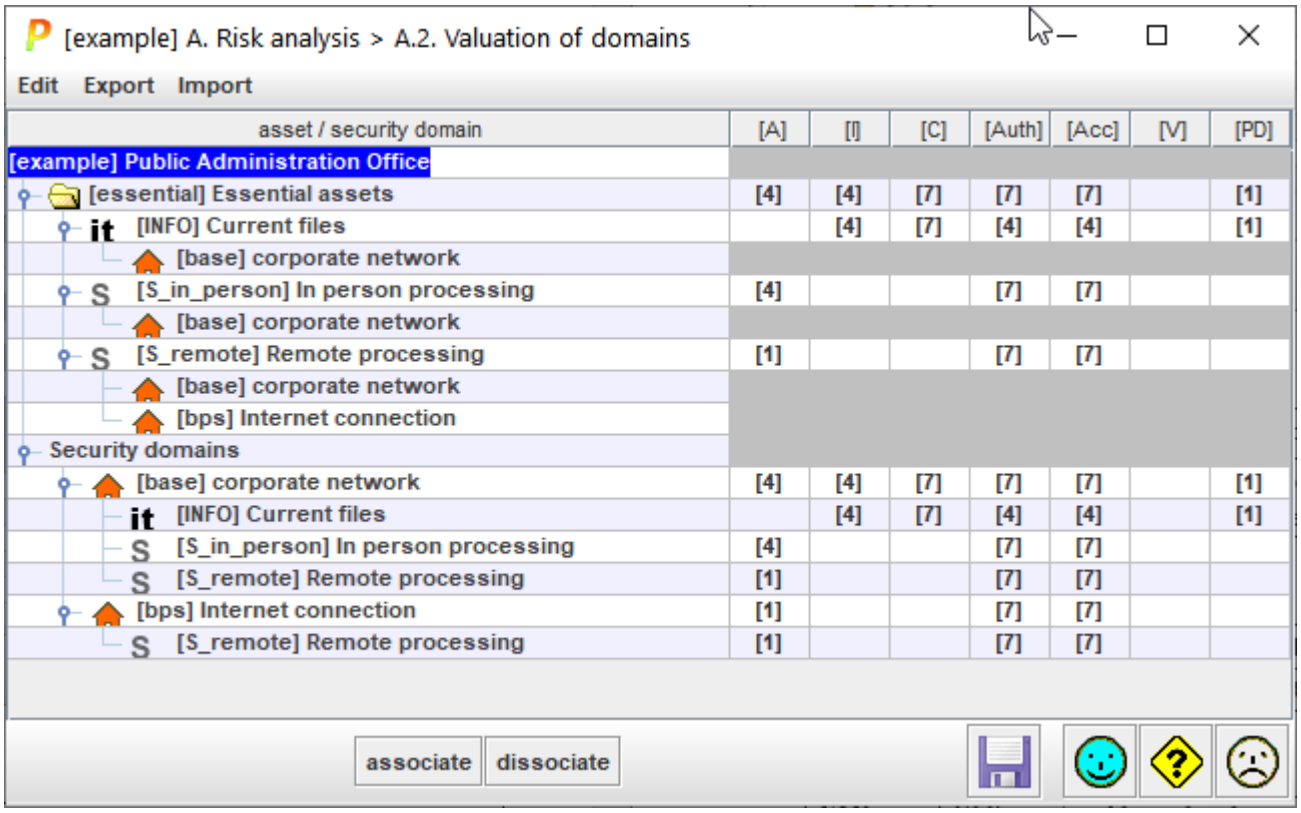
Let's suppose we have two security domains

— [base] Logical security

— [phys] Physical security



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*

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

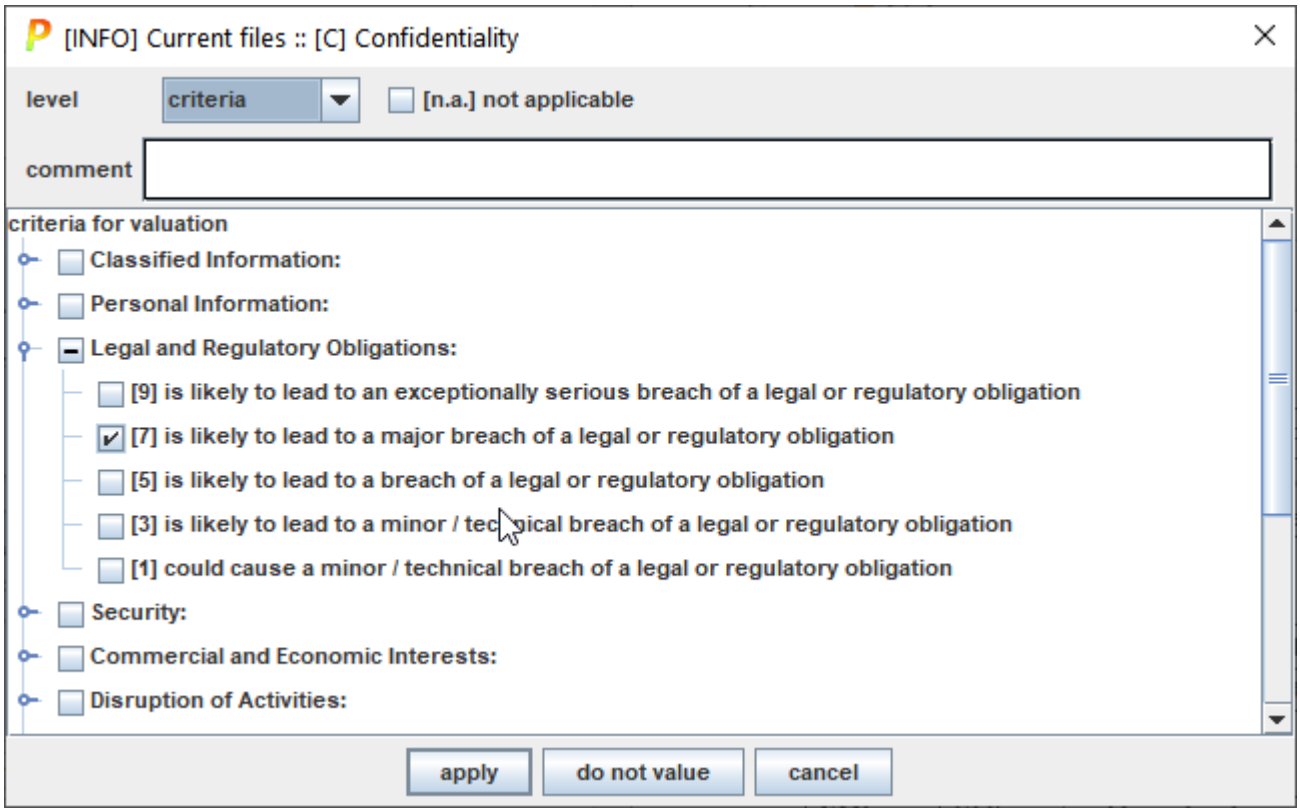
To disassociate an asset for a domain

- select the asset
- select the domain
- click DISSOCIATE

7.3.1 To set a qualitative valuation

To assign value to an asset

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

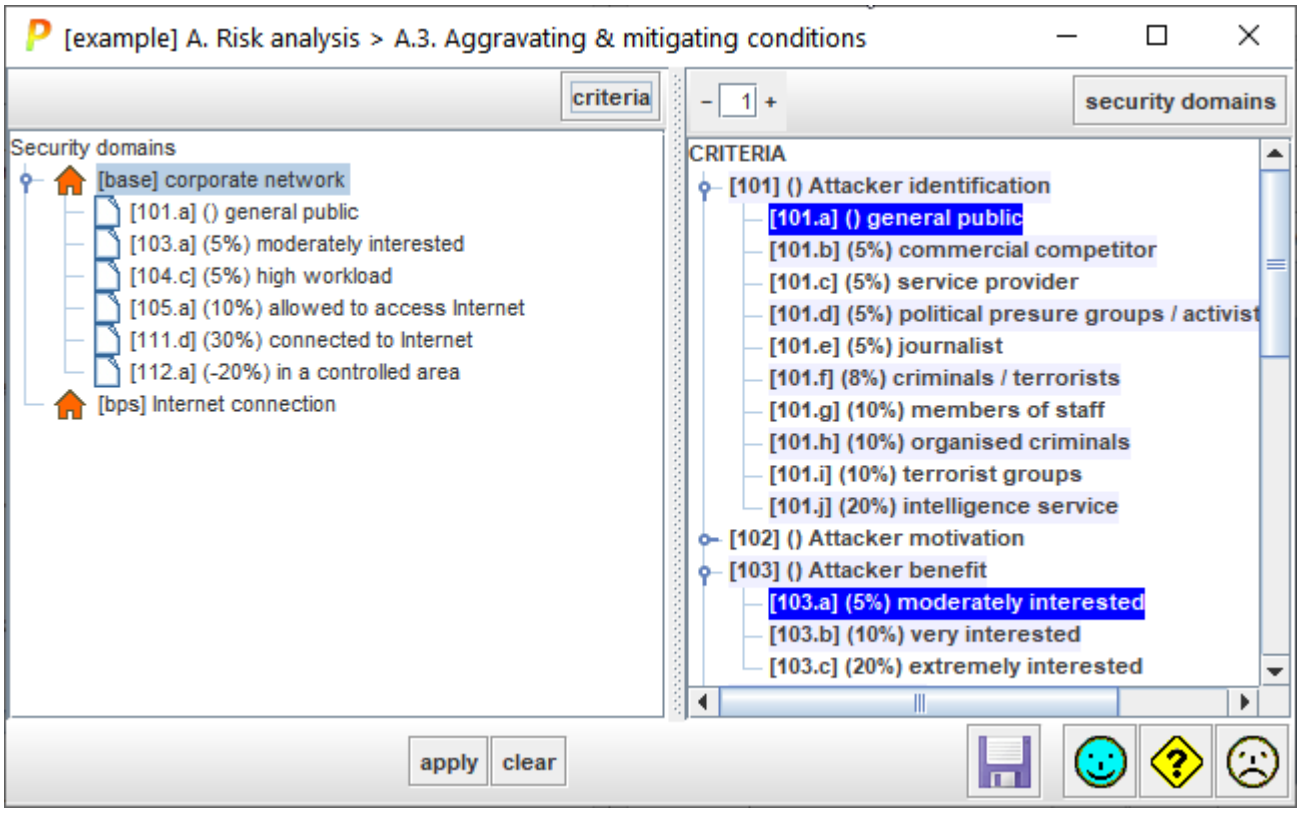


level combo	If you select “criteria” the value is decided by the highest-ranking criteria marked in panel. If you select any other value, that value is forced, ignoring the criteria (that are retained only for informative purposes).
[n.a.]	If the value has no sense for the asset, and its descendants, mark N.A.
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.

7.4 Threats

7.4.1 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.



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

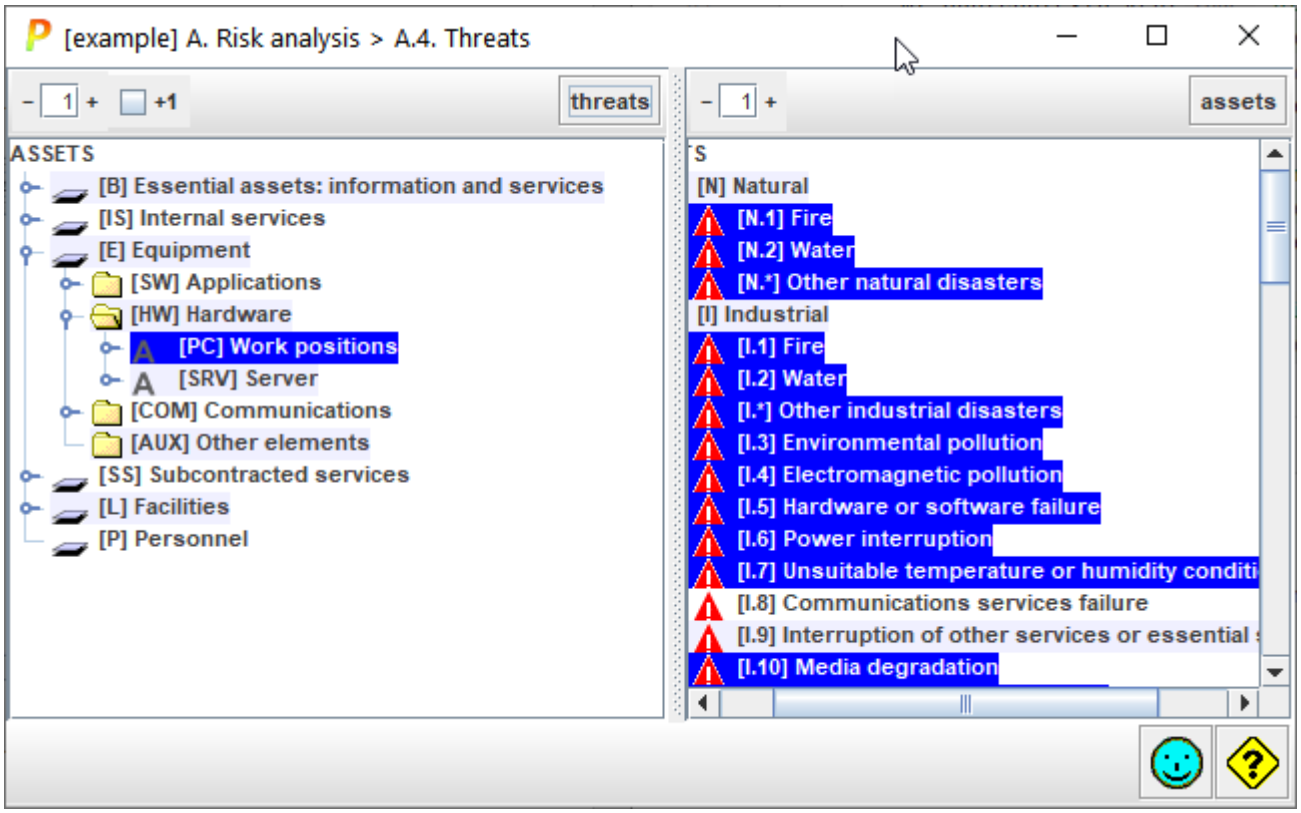
- select the domain (on the left panel)
- click criteria (left panel, top)

To discover the domains subject to a vulnerability

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

7.4.2 Identification

PILAR automatically applies the standard values from the *TSV file*.



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.
threats	— Select one or more assets in the left panel. — Click THREATS. PILAR selects on the right panel the threats that are associated to the selected assets.
	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.

Which threats are associated to an asset?

- select the asset on the left (one or more)
- click THREATS

Which assets are subject to a threat?

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

7.4.3 TSV – Threat Standard Values

TSV files are used to set threat values.

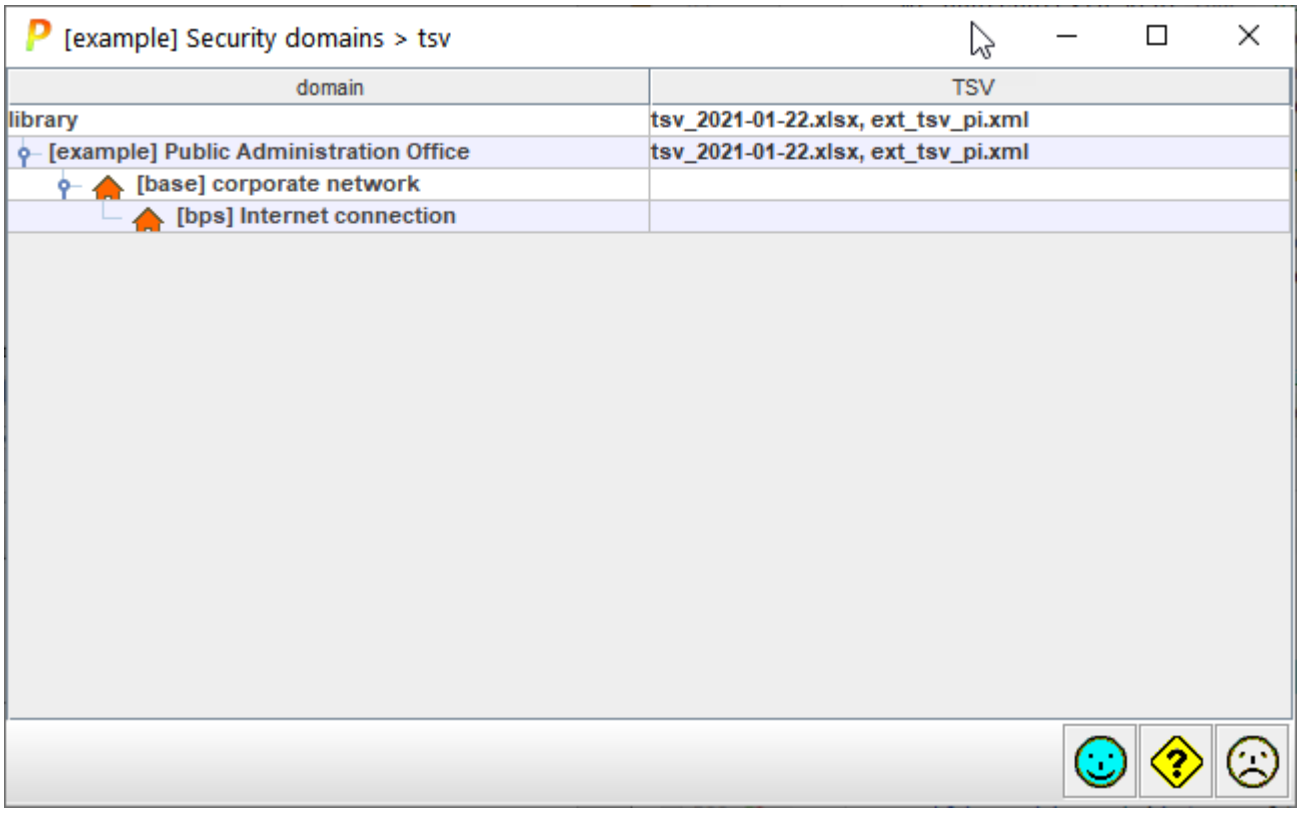
TSV files may be …

- an excel file
- an XML file

TSV files are explained in “personalization” at

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

When PILAR is going to load profiles for a security domain:



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.

7.5 Safeguards

7.5.1 Aspect

Aspect the safeguard deals with:

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

7.5.2 Type of protection

- PR – prevention
- DR – deterrence
- EL – elimination
- IM – impact minimization
- AD – administrative
- AW – awareness
- DC – detection
- MN – monitoring

— CR – correction
— RC – recovery

— std – policy
— proc – procedure
— cert – certification or accreditation

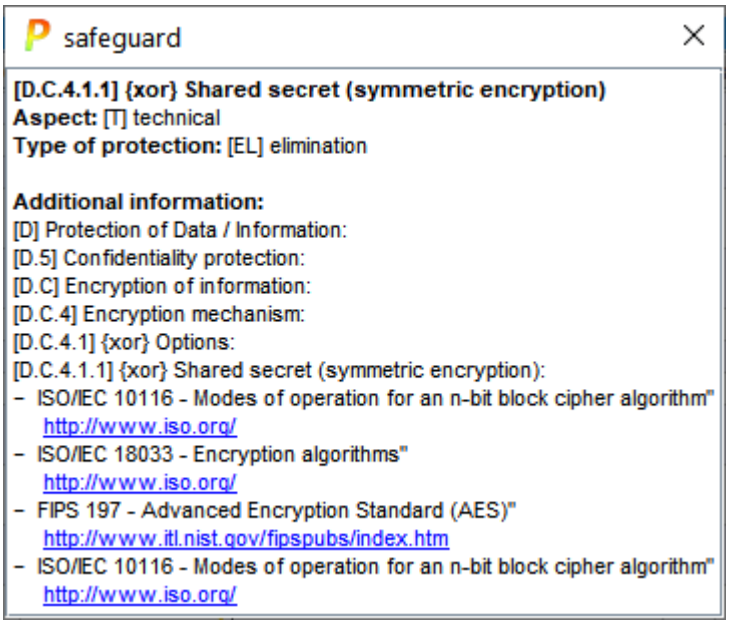
7.5.3 Relative weight

Not every safeguard is equally important:

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

7.5.4 Additional information

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



7.5.5 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

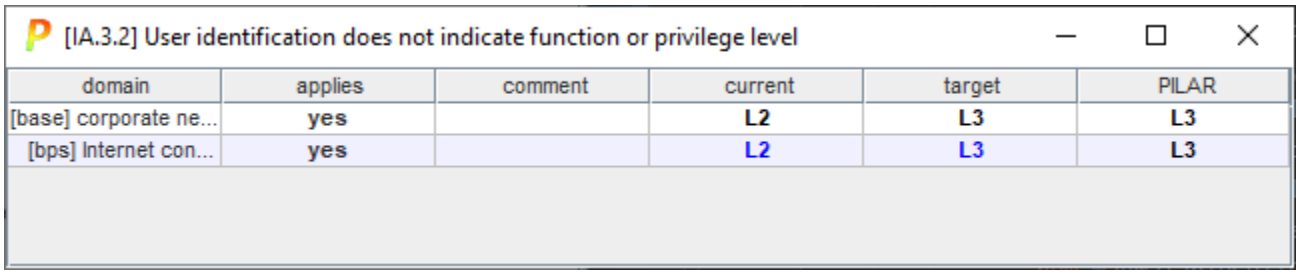
This node, and its brothers in the tree, are collapsed.

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 you may have a one-safeguard view of maturity values covering all the domains and all the phases



domain	applies	comment	current	target	PILAR
[base] corporate ne...	yes		L2	L3	L3
[bps] Internet con...	yes		L2	L3	L3

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

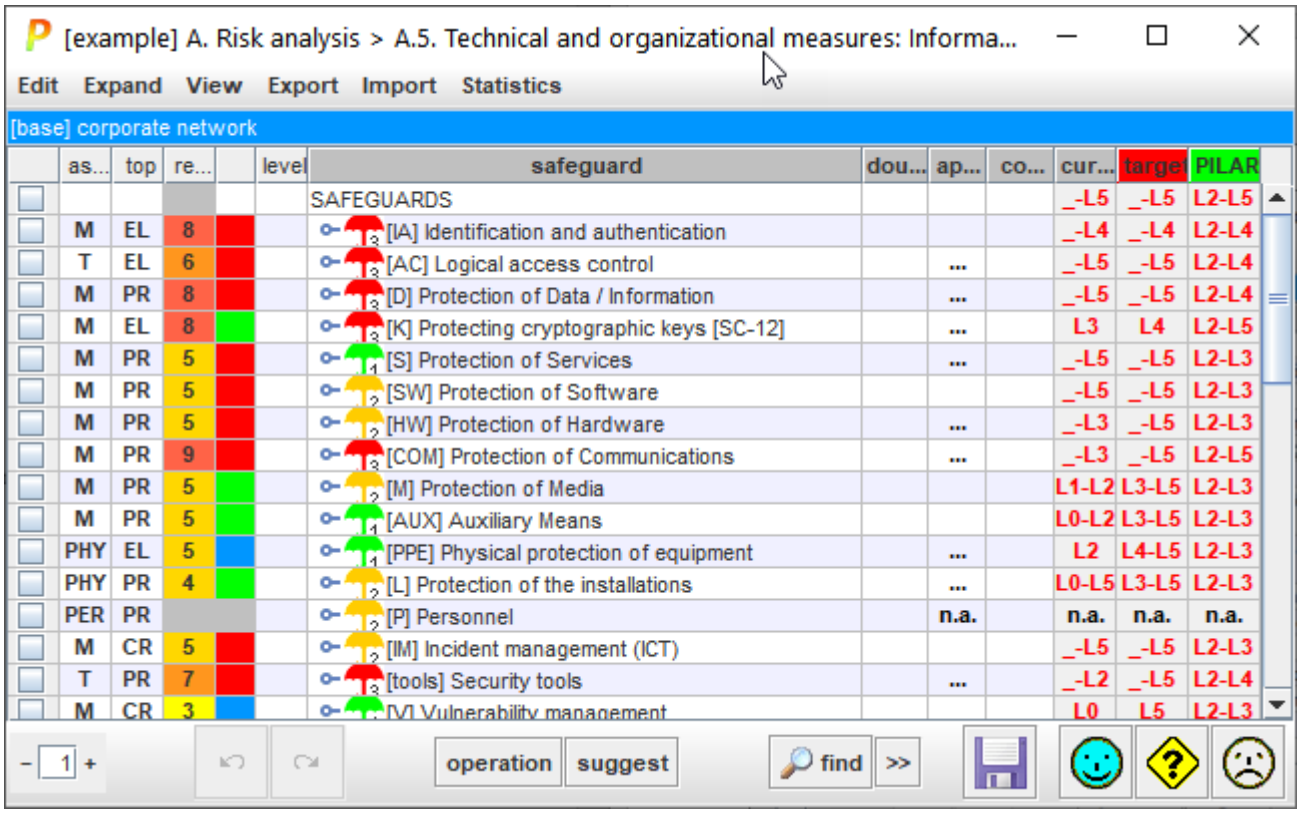
7.5.6 Valuation per domains

Quick start

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

If you have a plan in mind …

5. Go to the cell at row SAFEGUARDS, and column TARGET. Select it.
6. 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 VIEW

risks	Jumps to risk table, presenting only those that may be treated by this safeguard
one line	Safeguard text is truncate to use only one row
one paragraph	the full text of the safeguard is presented, expanding the cell if necessary

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)	

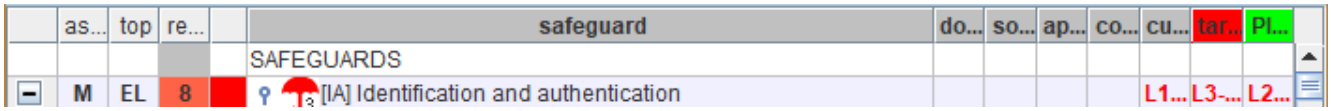
Top menu STATISTICS

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

Top band

security domain	There may be different safeguards for different domains. Click to select the domain you want to edit.

7.5.6.1 Central table



Selection	
aspect	See "*Safeguards / Aspect*".
top	See "*Safeguards / Type of protection*".
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.
traffic light	See "*Safeguards / Reference and target phases*" below.
safeguards	Safeguards tree. You double click to collapse / expand the tree. You may right-click to access to "*Safeguards / tree*".
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.
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.
comment	Click to associate comments to the safeguard.
	Project phases.

	See "*Safeguards / Maturity valuation*" below.

On applicability

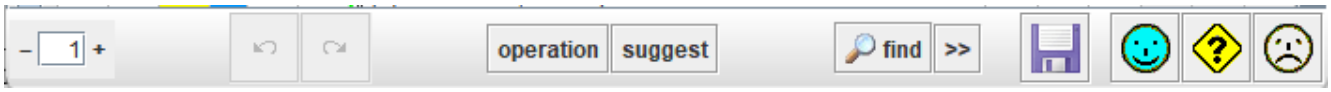
- left click
  - to select / unselect; if a countermeasure is marked as not applicable, all of its children become not applicable; if some children apply and some do not, the countermeasures above are marked as "…".
- right click

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 safeguads 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

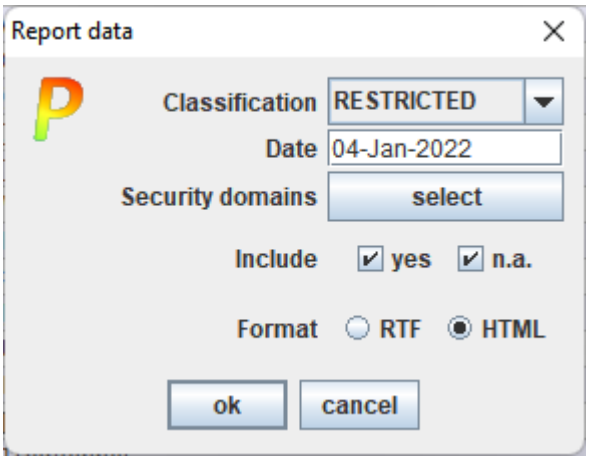
7.5.6.2 Bottom tool bar



	Spinner to control the expansion of the safeguards tree.
	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).

7.5.6.3 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.
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.

7.5.7 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

7.5.8 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. If after that search the cell is still empty, PILAR uses the value “L0”.

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

The selected safeguard is shown within square brackets.

7.5.9 Operation combo

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

APPLY

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

FILL

applies the selected value in the maturity combo 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

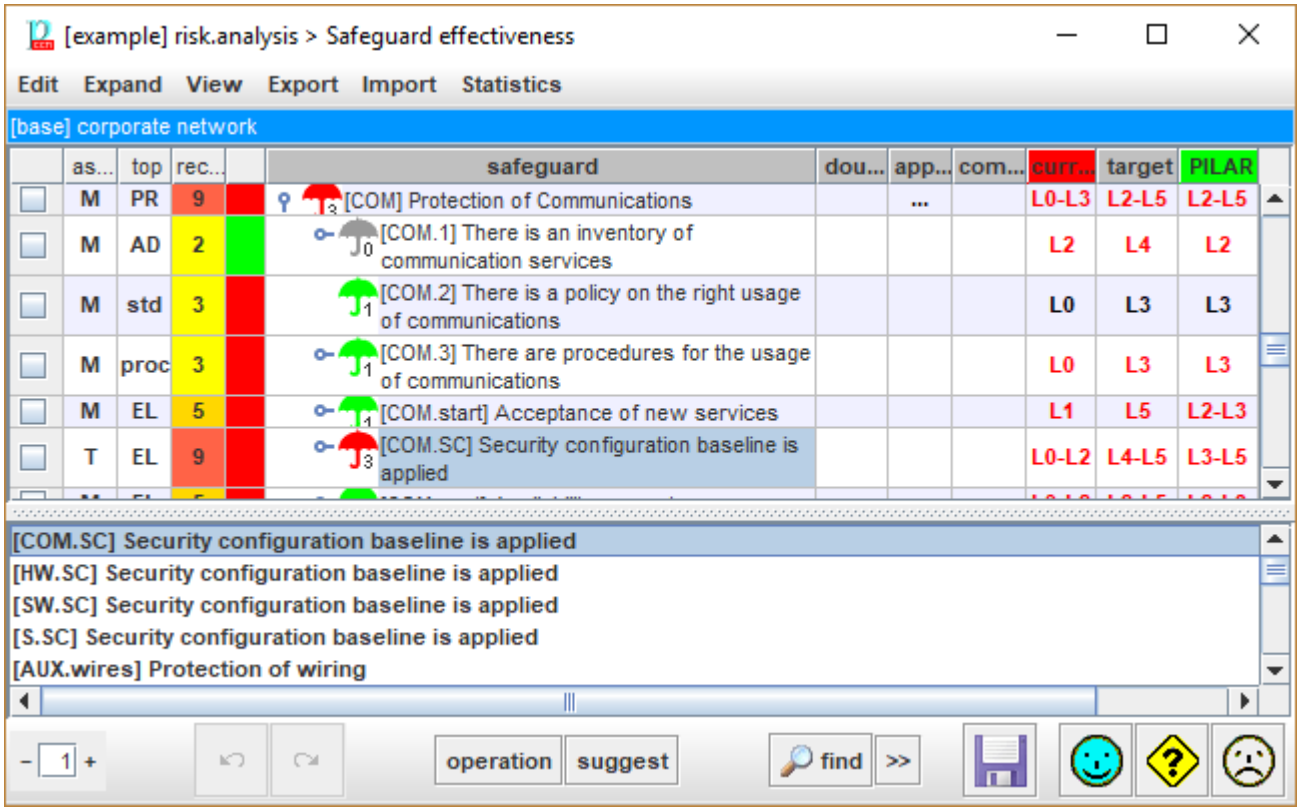
taking into account the recommendation, PILAR suggests that maturity values considered minimum to meet the needs of the system. Merely heuristic, with the intention of making a reference below which should not operate the system

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

7.5.10 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.



7.5.11 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

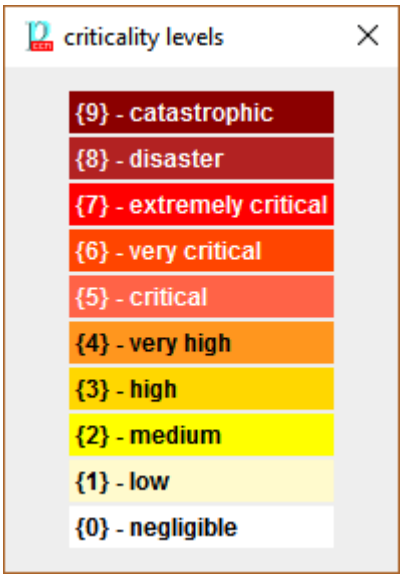
>>

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

7.6 Impact & risk

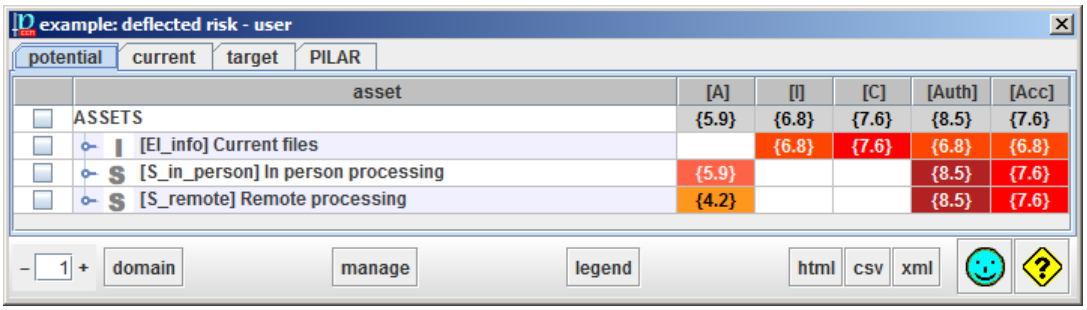
7.6.1 Criticality levels – Colour encoding

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

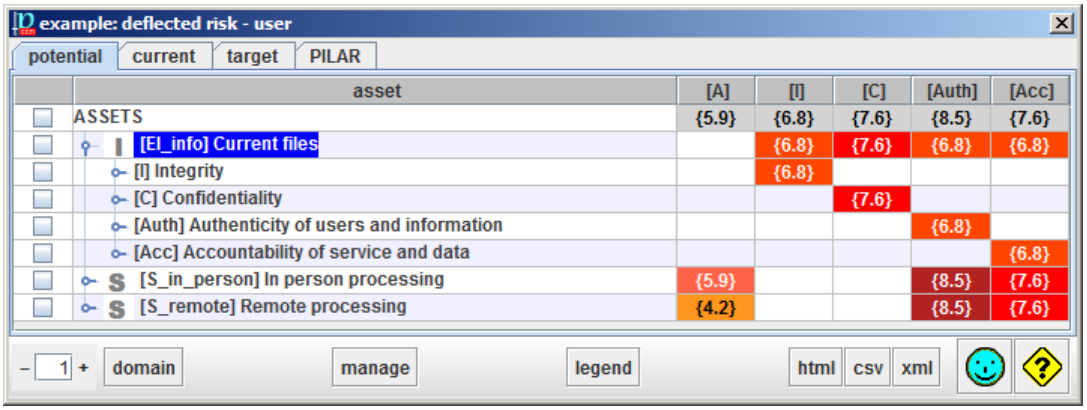


7.6.2 Indirect risk

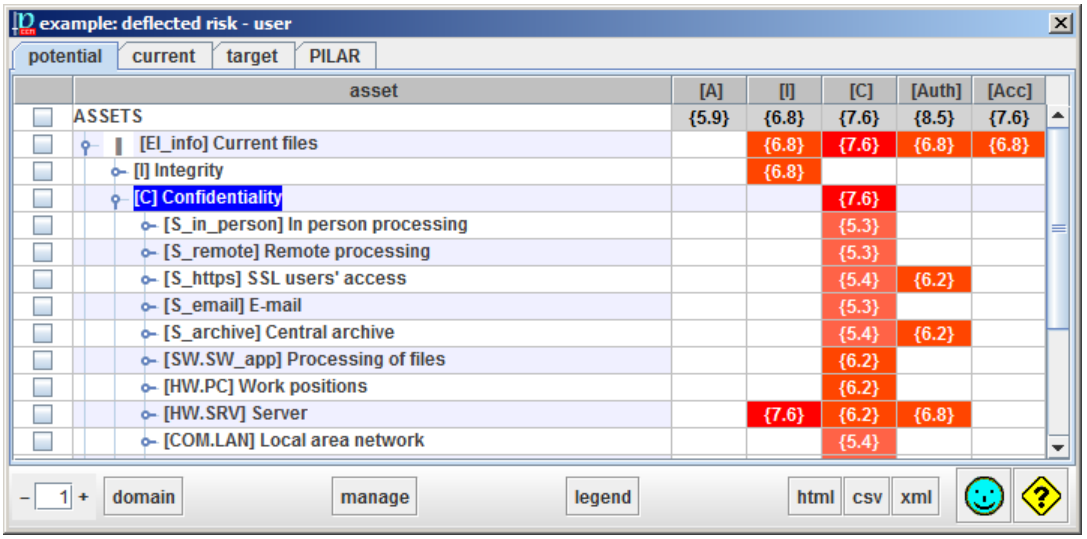
PILAR presents the indirect risk on essential assets with an explicit value:



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:



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

Phase tabs

One tab per project phase. Click to switch.

Pseudo phase “potential” shows inherent risk without safeguards.

Columns

selection	Click on checkboxes to check / uncheck.

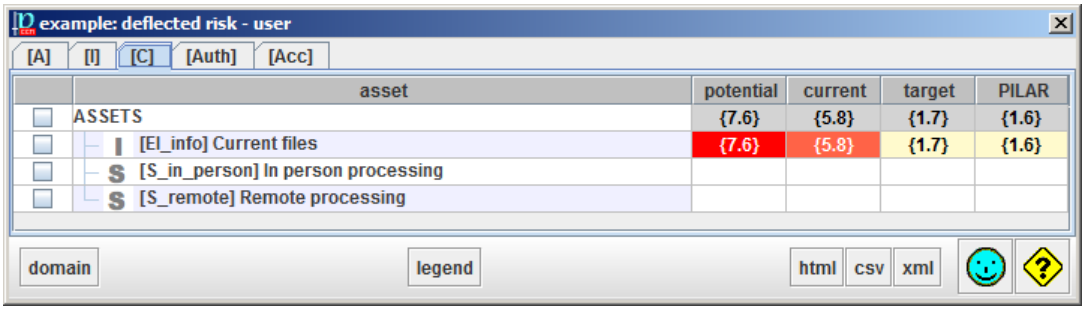
	SHIFT-click to check a range. Click on column header to clear current selection. Selects rows to manage (see below)
assets	Assets tree.
dimensions	One column per security dimension. Click on header to switch to alternate view. Risk value. Risk is evaluated on threats and summarised for assets.

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	See *Risks / Criticality levels & color encoding*

7.6.2.1 Alternate view

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



You may click on the header of a project phase column to return to the alternate view.

8 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

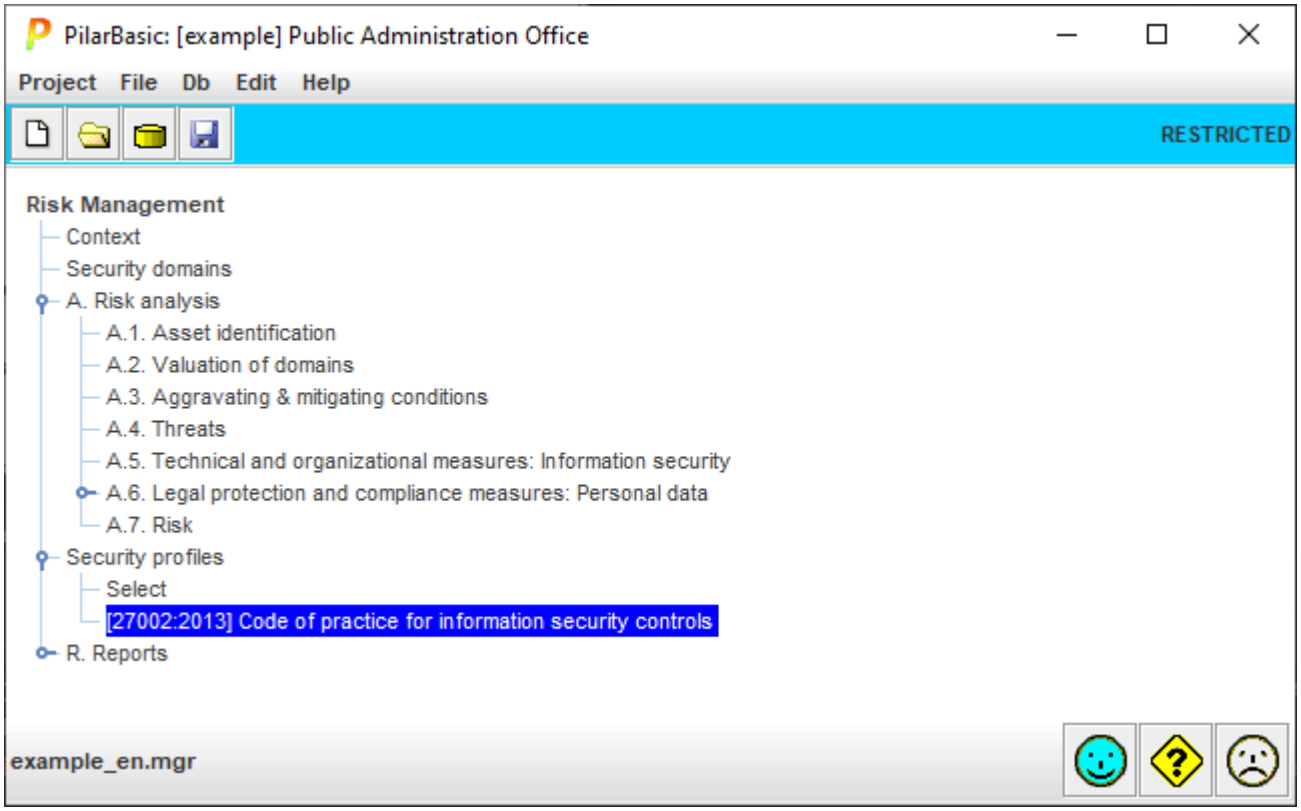
```
bib_en/27002_2013_*_en.evl
```

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

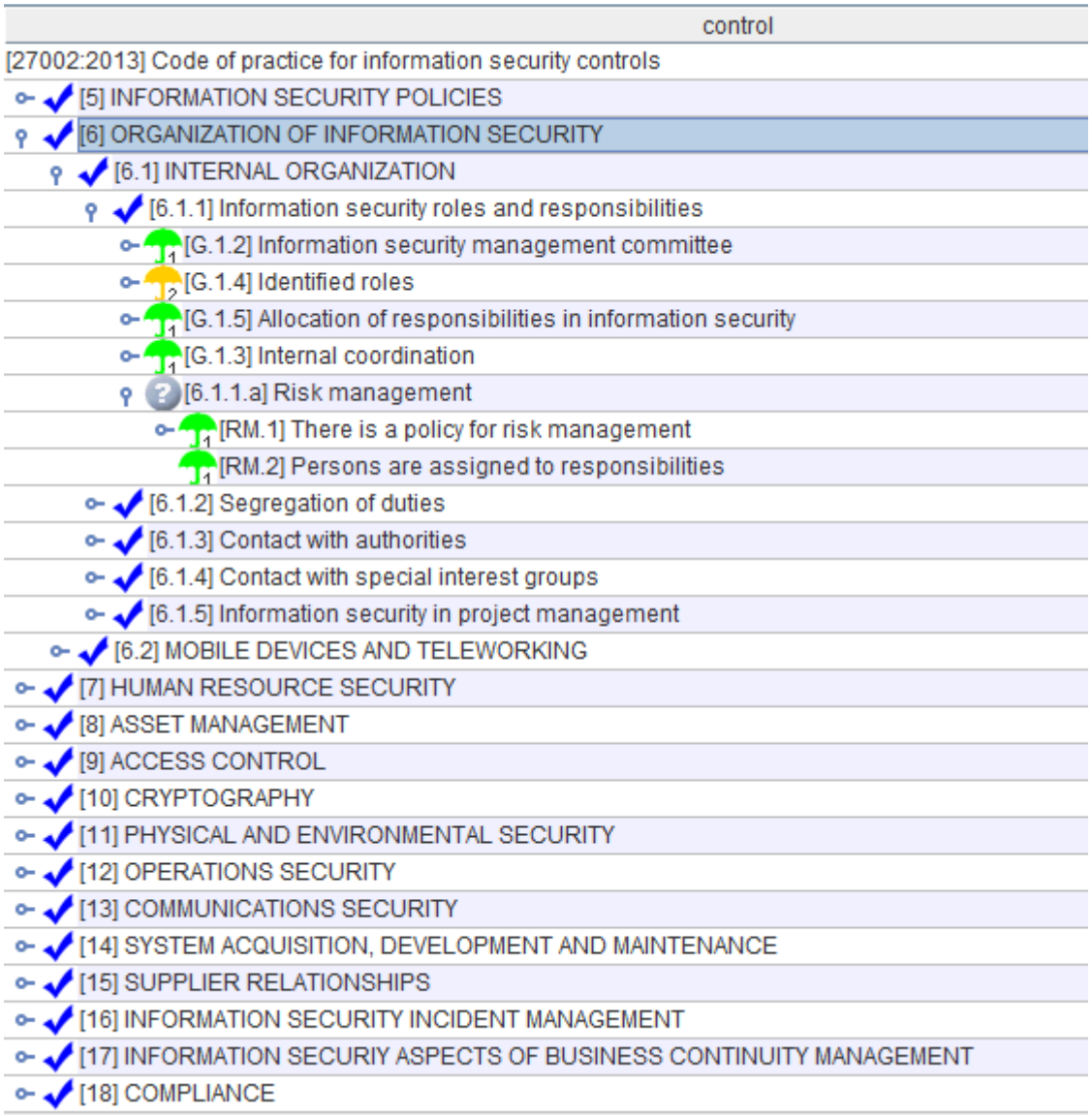
STIC_en.car

```
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:

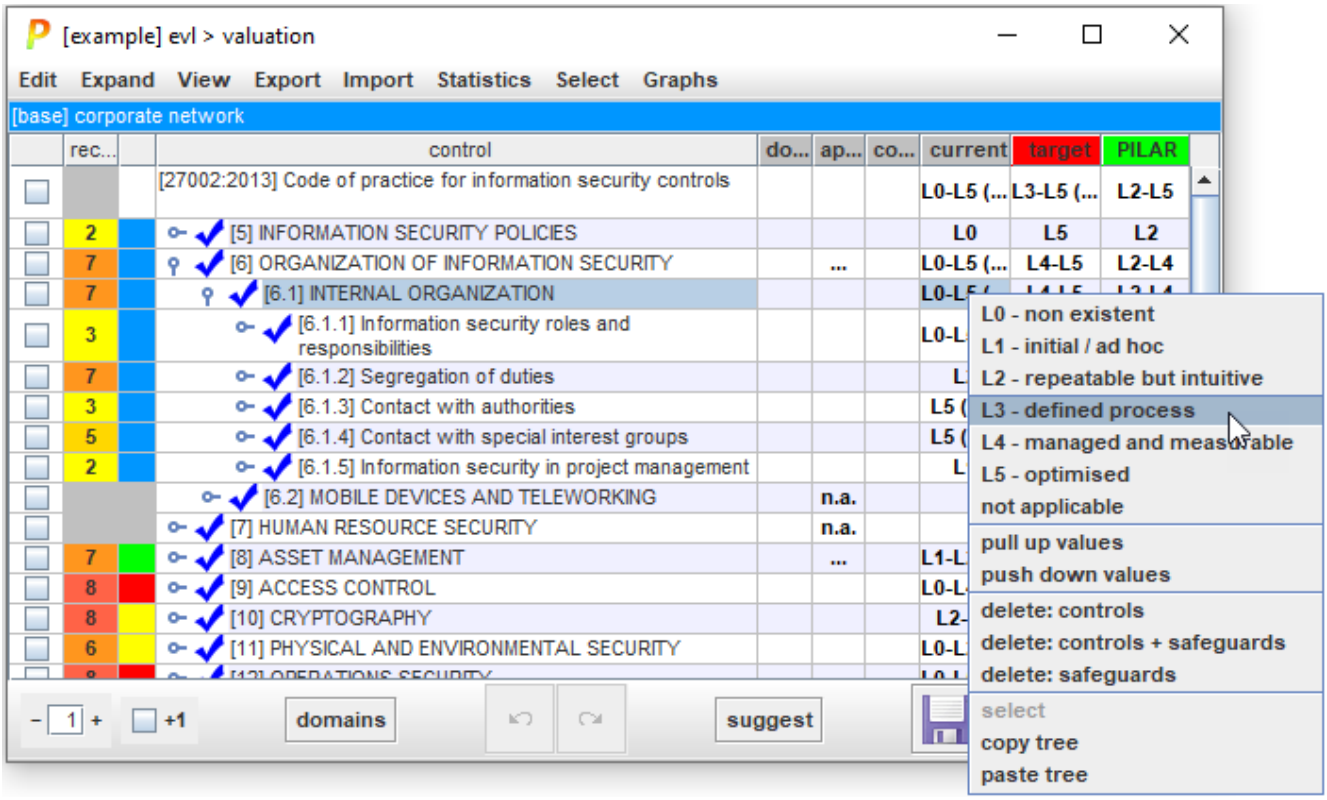


EVL trees have different types of nodes:

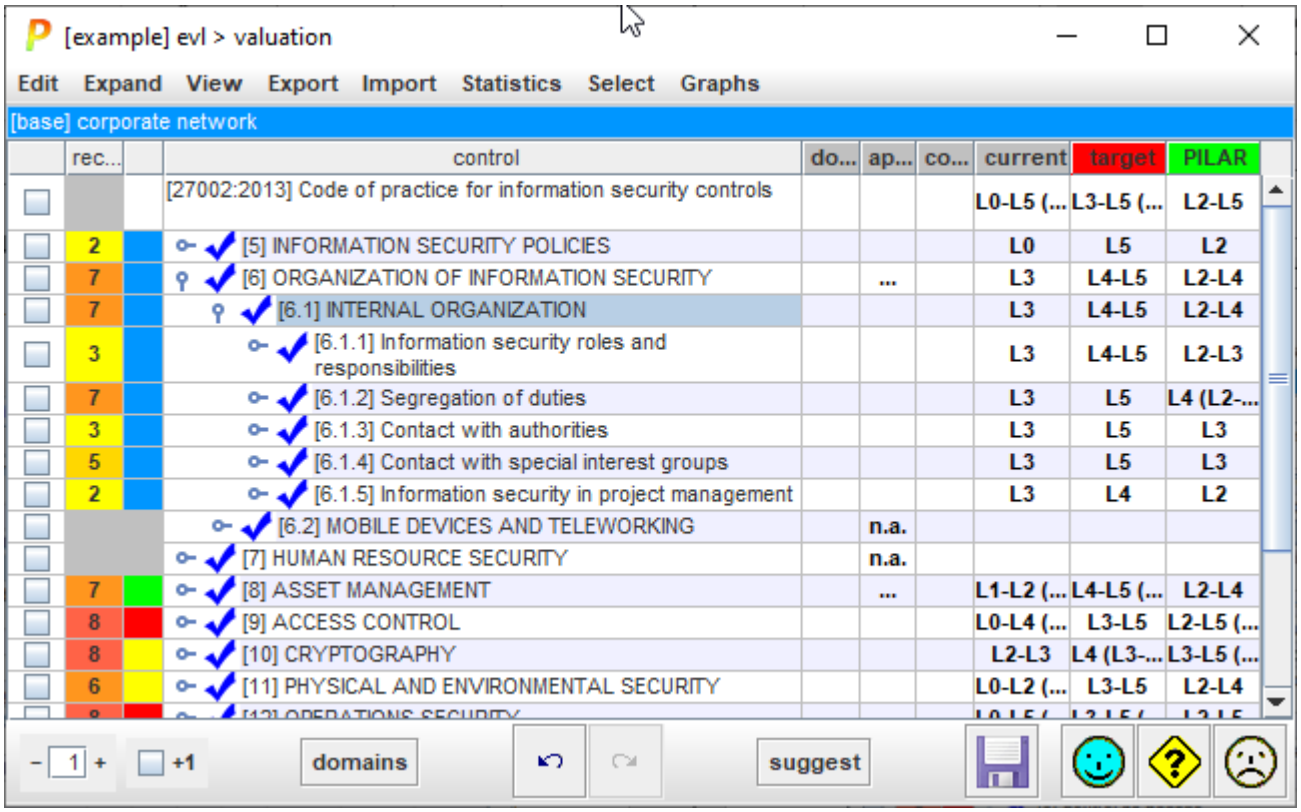
	Controls – main requirements from security profiles
	Questions – secondary requirements, or tree structuring nodes
	Links – when a control refers to another control
	Safeguards – countermeasures from the PILAR library
	See also – additional information

8.1 EVL - Basic usage

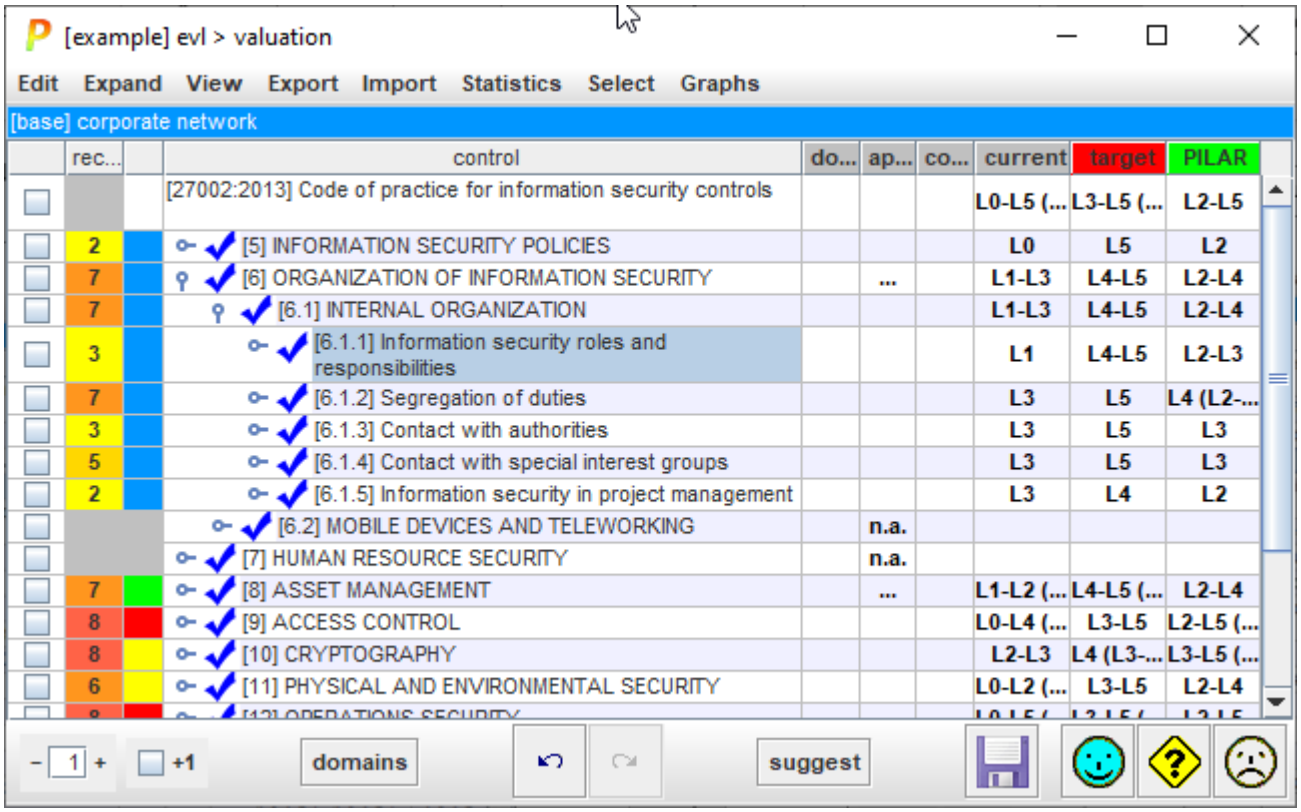
Basic usage is to introduce values for profile controls. Select the cell for a control, and a phase, then right click:



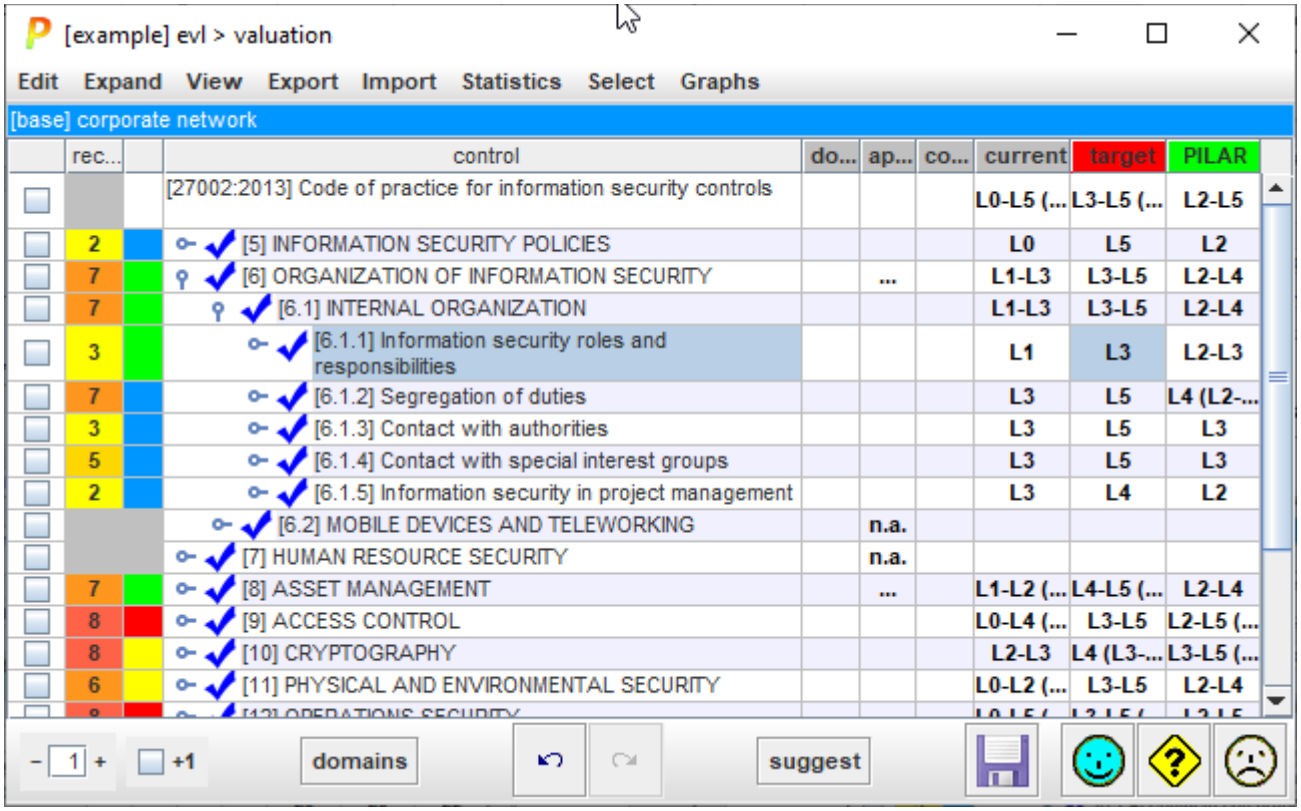
PILAR applies the selected maturity to the selected control. Then, it is copied onto every child.



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.

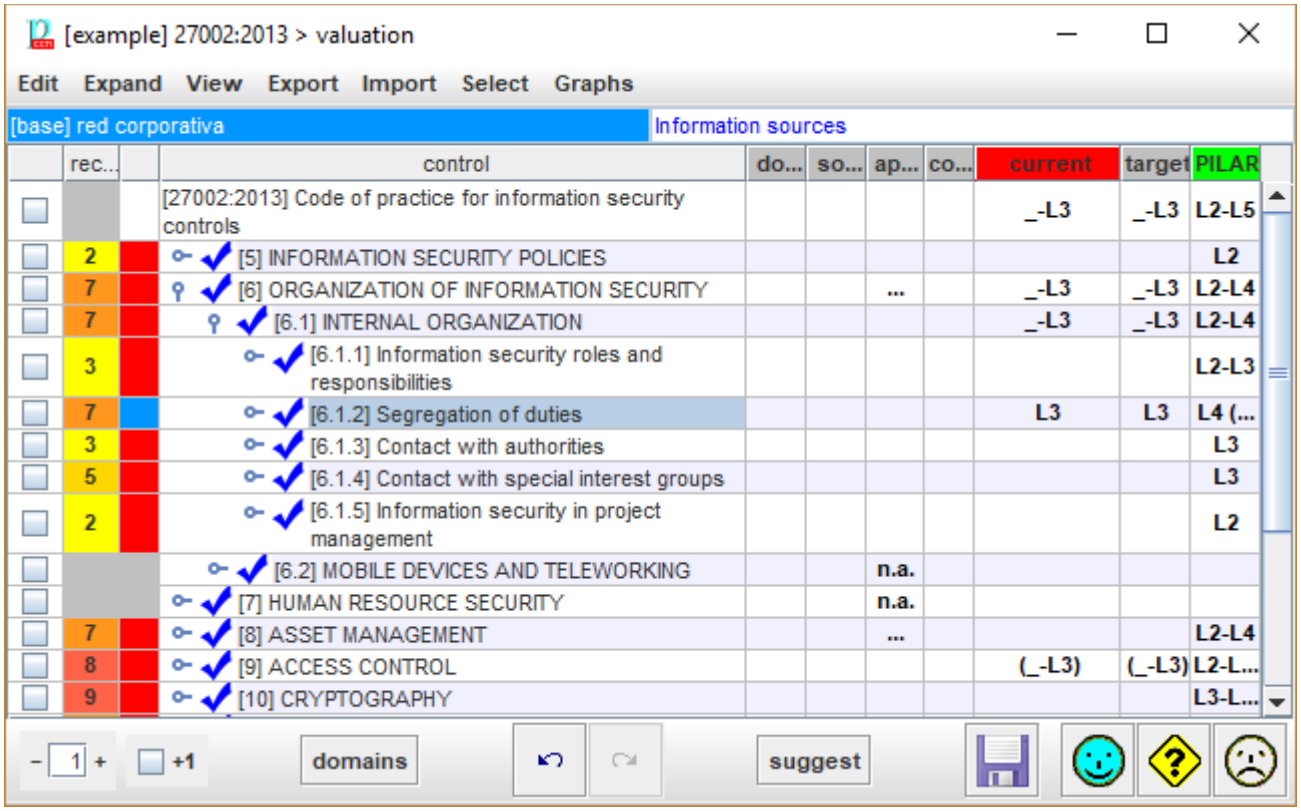


PILAR maps controls onto safeguards. This mapping is neither official, nor perfect. It is not official because security profiles are pieces of work from different sources, unrelated to PILAR. And it is not perfect for several reasons:

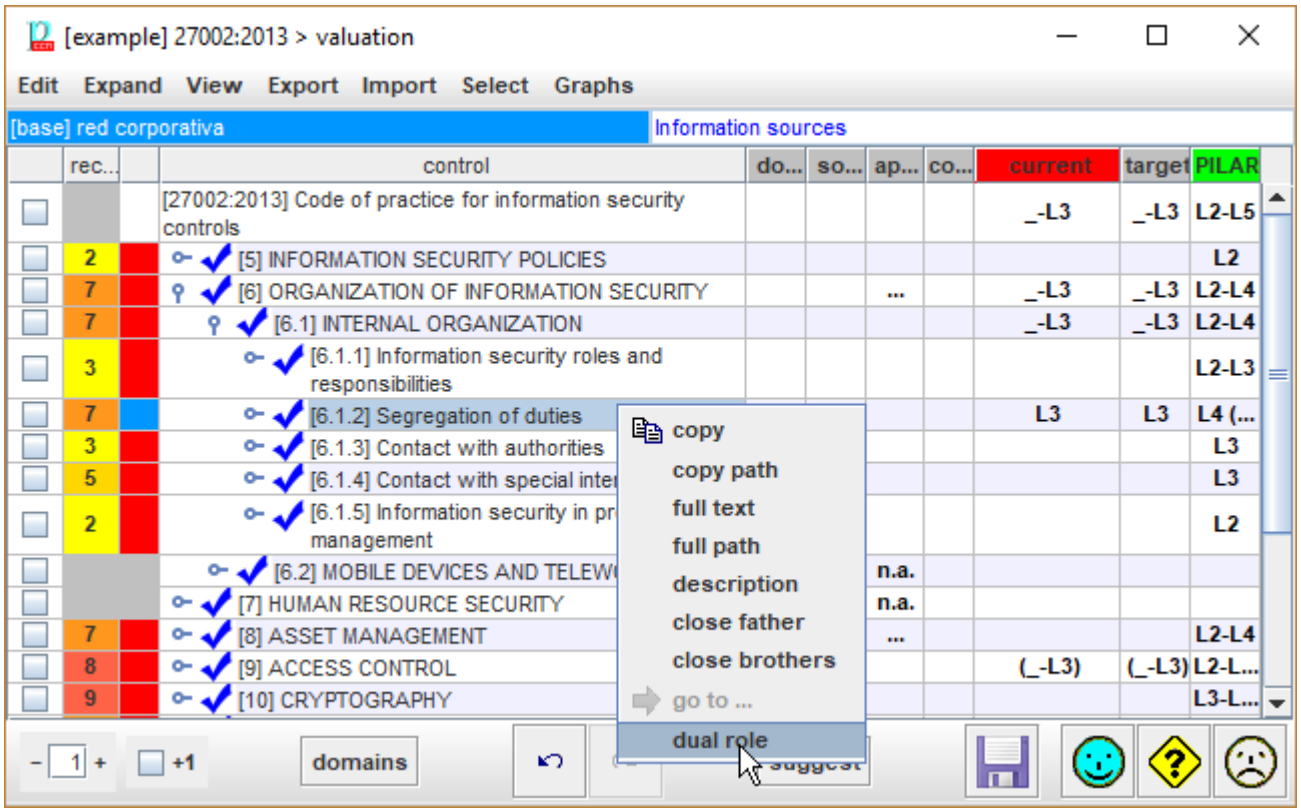
- there may be no appropriate safeguard in PILAR to meet the control requirements
- the same safeguard in PILAR may apply to more than one control
- as PILAR evolves, the set of safeguards evolve

PILAR tries to do something reasonable.

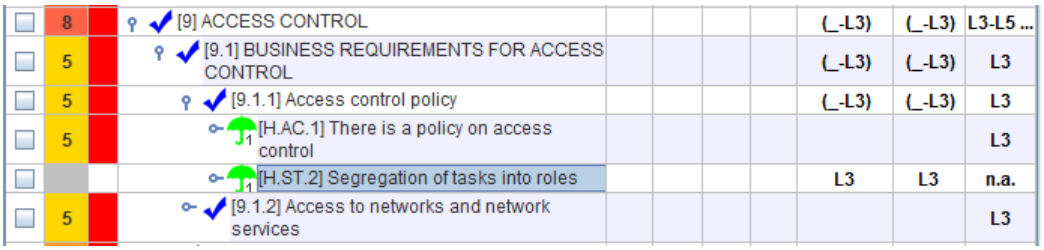
When a safeguard is found in several mappings, change the value in one place has a ripple effect:



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



and PILAR selects all the references in the profile; for example:



8.2 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

8.3 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

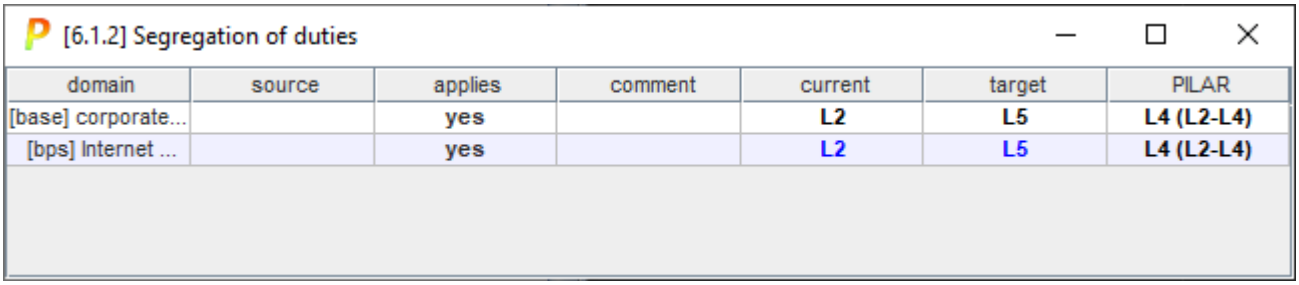
close brothers

compact tree: brothers are closed

go to …

for links, , jump to the link destination

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.

8.4 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:

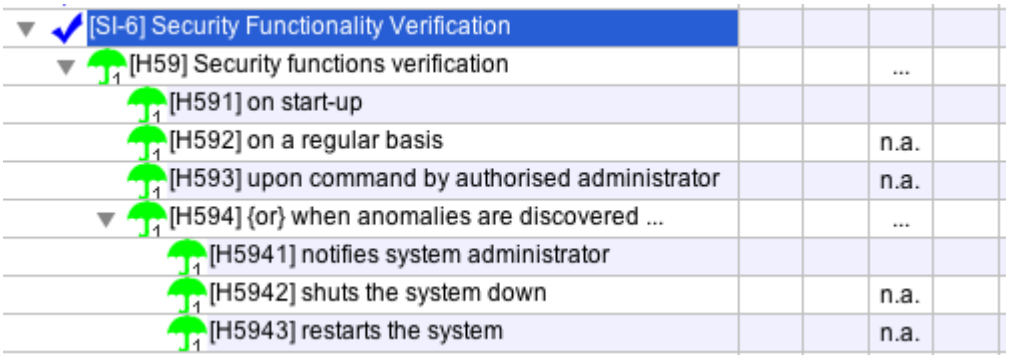
	rec...		control	do...	so...	ap...	co...	current	target	PILAR
			[27002:2013] Code of practice for information security controls					L0-L5	L2-L5 ...	L2-L5
	2		[5] INFORMATION SECURITY POLICIES					L0	L5	L2
	7		[6] ORGANIZATION OF INFORMATION SECURITY			...		L0-L5 ...	L2-L5 ...	L2-L4
	7		[6.1] INTERNAL 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 ...

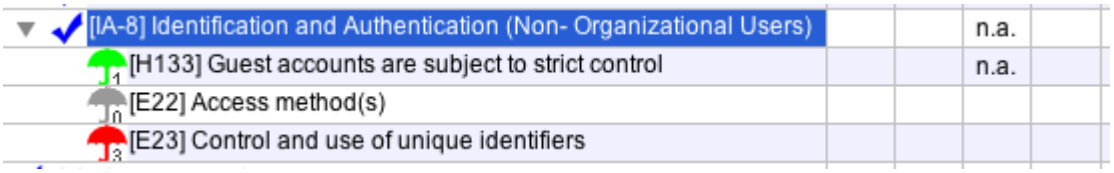
The “n.a.” means that the row does not apply. The dots mean that something below in the tree does not apply.

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

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

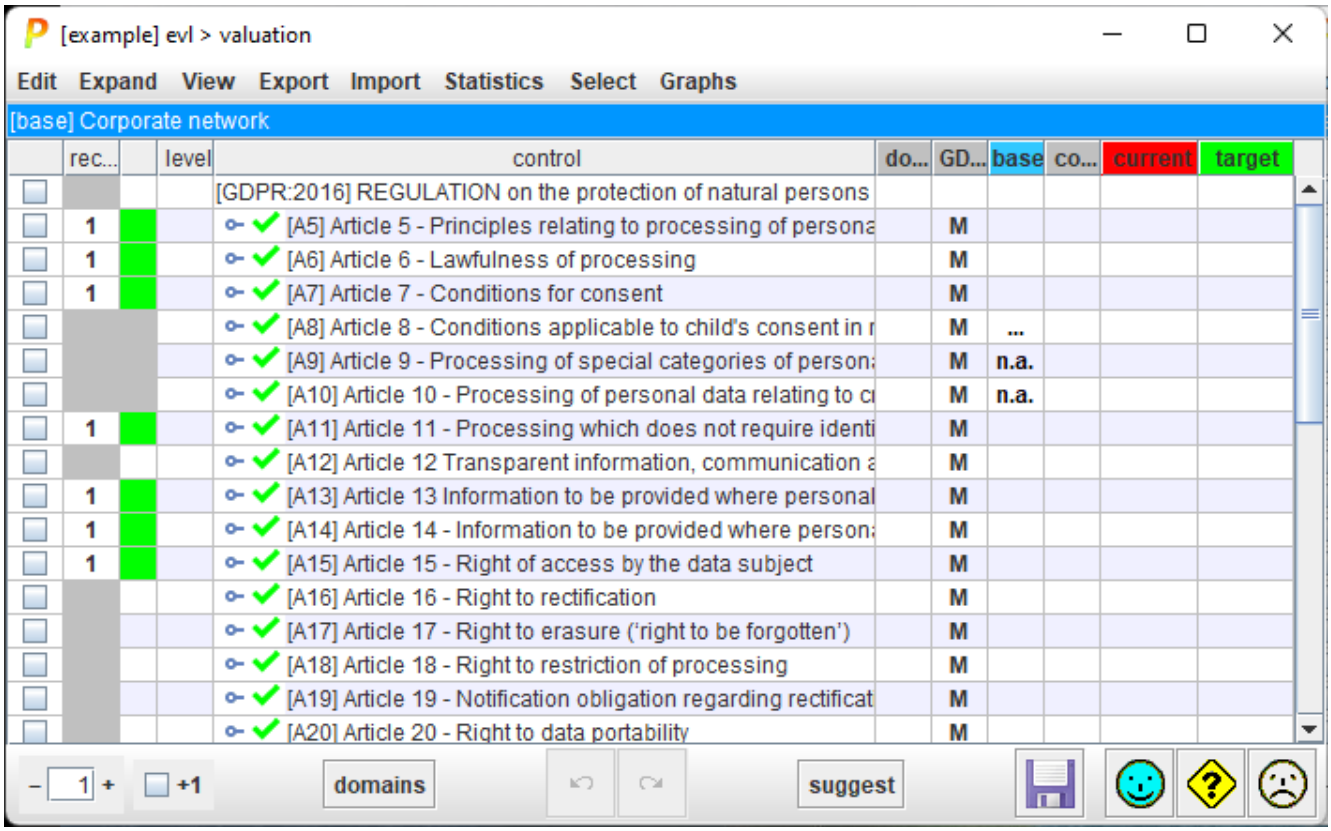




8.5 EVL – Mandatory controls

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:



8.6 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.

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.

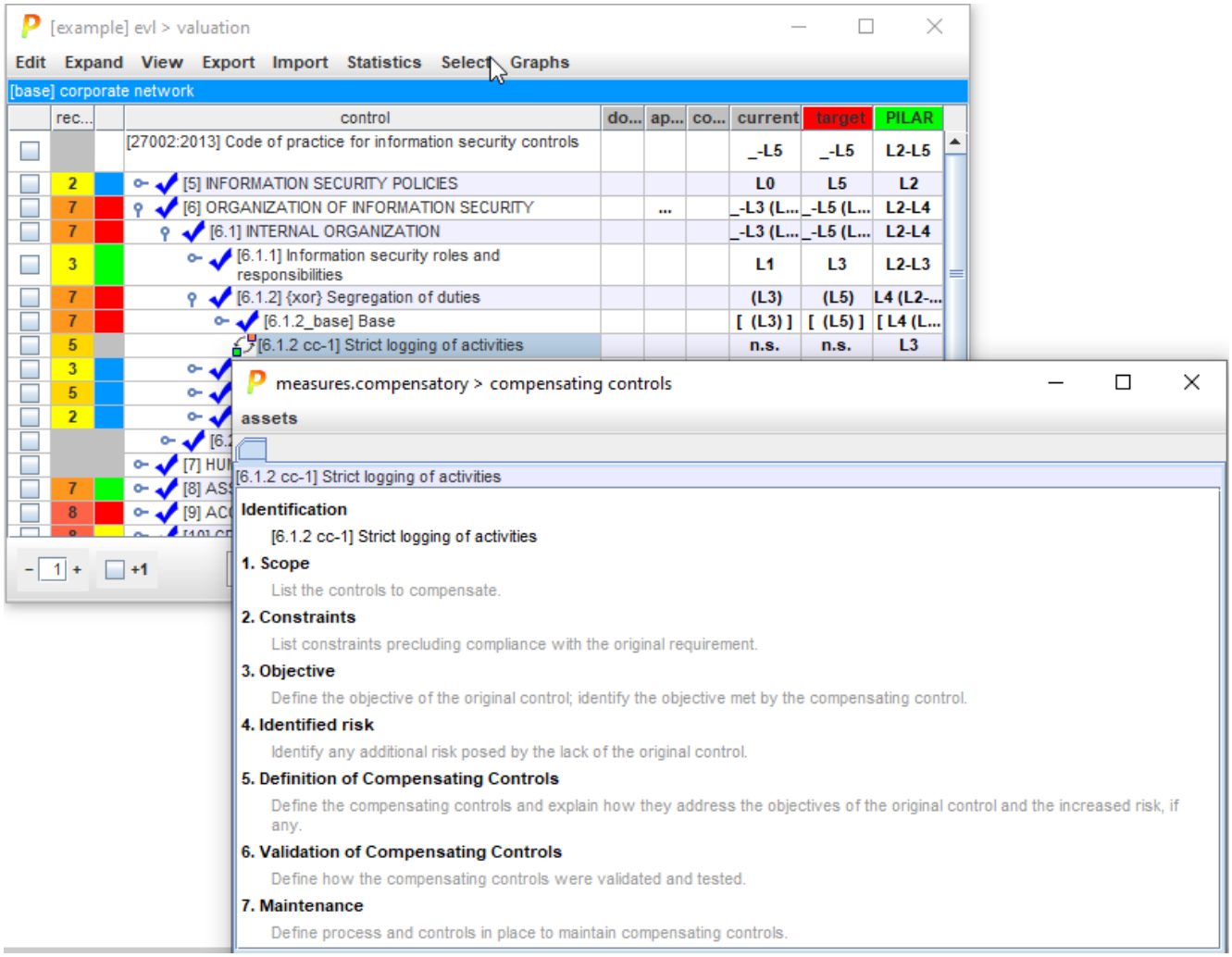
8.7 EVL – Compensating controls

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, in order to evaluate the residual risk achieved with the actual protection system.

8.8 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

8.9 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)	

For 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.

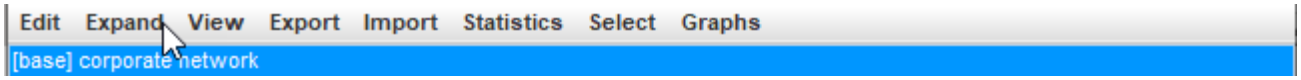
Top menu SELECT

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

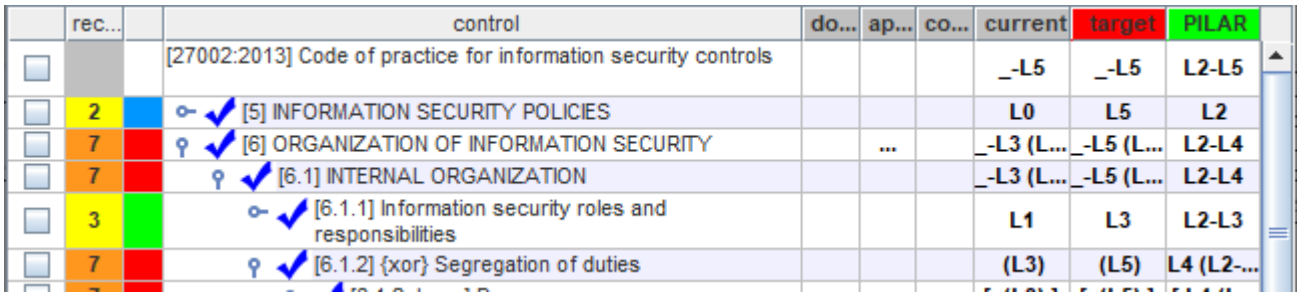
draw	Drawing with the current selection of rows and phases.

Top bands



security domain	There may be different controls for different domains. Click to select the domain you want to edit.

Table columns



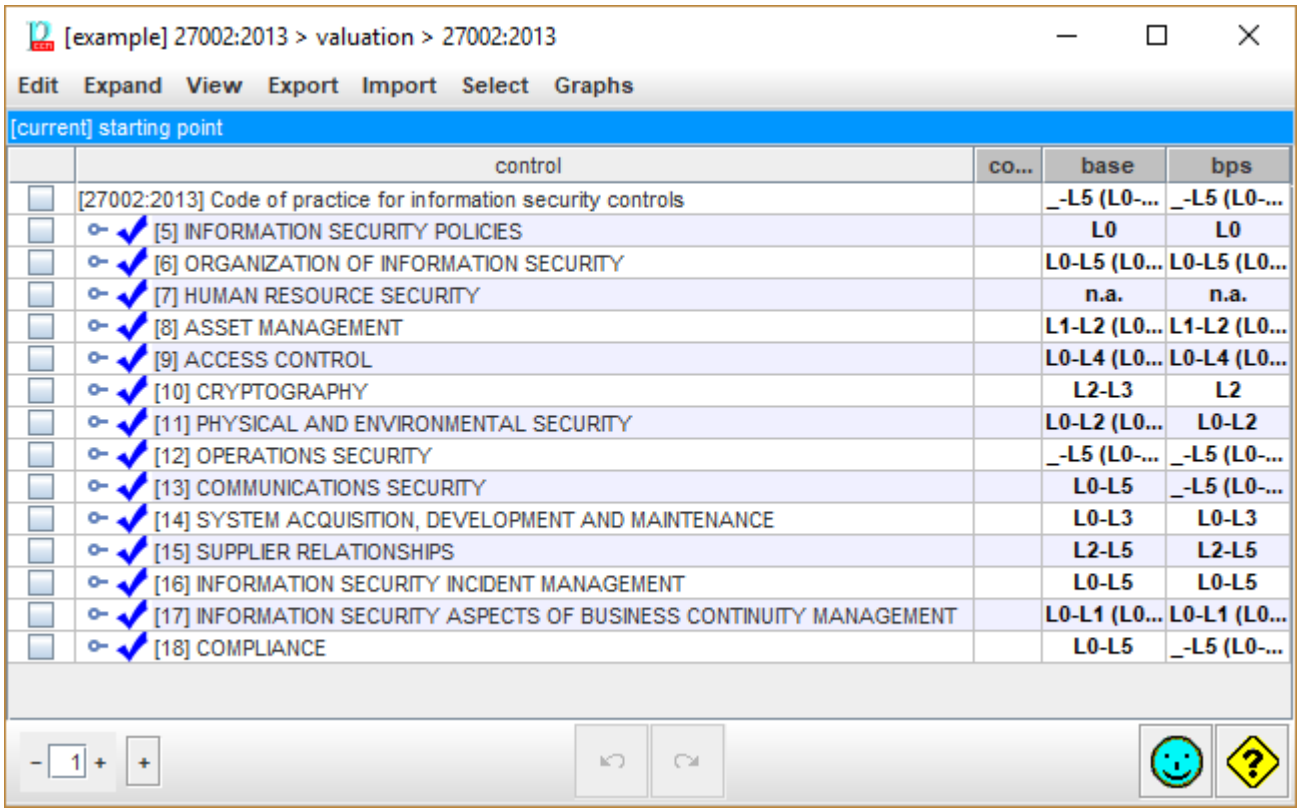
select	Selects rows for graphs. Click on checkboxes to check / uncheck. SHIFT-click to check a range. Click on column header to clear current selection.
recommendation	It is a rank in the range [null .. 10], estimated by PILAR taking into account the assets, the security dimensions, and the level of 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").
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.
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 options menu.
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.
applies	See *EVL / Applicability*
comment	Click to associate comments to the row.
	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).

8.10 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-...