

PILAR

Risk Analysis and Management

Help Files

version 5.1

March 15, 2011

1	ABOUT RISK MANAGEMENT	5
1.1	SUGGESTED READING	5
1.2	OTHER DOCUMENTATION ABOUT PILAR	5
2	USE CASES	6
2.1	NEW USER	6
2.2	ADVANCED USER	6
3	CONTROL PANELS	7
3.1	RISK ANALYSIS	7
3.2	BCM – BUSINESS CONTINUITY	8
4	INSTALLATION	10
4.1	JAVA ENVIRONMENT	10
4.2	PILAR (WINDOWS)	10
4.3	PILAR (UNIX, LINUX, ...)	10
4.4	PILAR (MAC OS X)	10
4.5	USAGE	10
5	1ST SCREEN	12
6	CONTROL BOARD	14
6.1	PROJECT MENU (PILAR STANDARD)	14
6.2	PROJECT MENU (PILAR BASIC)	14
6.3	FILE MENU (PILAR STANDARD)	14
6.4	DB MENU (PILAR / DATABASE ENABLED)	15
6.5	EDIT MENU	15
6.5.1	<i>Preferences</i>	15
6.5.2	<i>Options – Valuation of domains</i>	15
6.5.3	<i>Options – Frequency</i>	16
6.5.4	<i>Options – Degradation</i>	16
6.5.5	<i>Options – Threats</i>	16
6.5.6	<i>Options – Project phases</i>	16
6.5.7	<i>Options – Unevaluated safeguards</i>	16
6.5.8	<i>Options – Export: safeguards</i>	17
6.5.9	<i>Options – Residual risk</i>	17
6.5.10	<i>Options – Maturity</i>	17
6.6	DOMAINS AND PHASES	17
6.7	LEVEL MENU	18
6.8	HELP MENU	18
7	PROJECT DATA	19
8	INFORMATION SOURCES	21
9	SECURITY DOMAINS	22
10	SELECTION OF DIMENSIONS	23
11	SELECTION OF VALUATION CRITERIA	24
12	SELECTION OF THREATS	25
13	VALUE QUANTIFICATION	26
14	IDENTIFICATION OF ASSETS	27
14.1	LAYERS	27
14.2	ASSETS	28

14.3	SECURITY DOMAINS	31
14.4	STATISTICS	31
14.5	DESCRIPTION OF ONE ASSET	31
14.6	ASSET: IS IT SUBJECT TO THREATS?.....	32
14.7	ASSET: IS IT VISIBLE?	33
14.8	ASSET: DOES IT EXIST?.....	33
14.9	ASSET: IS IT AVAILABLE?	33
15	ASSOCIATION OF CLASSES TO ASSETS.....	34
16	ASSOCIATION OF CPE NAMES TO ASSETS.....	35
17	VALUATION OF SECURITY DOMAINS	36
18	DEPENDENCIES BETWEEN ASSETS.....	37
18.1	DEPENDENCIES PER DIMENSION OF SECURITY	38
18.2	MAP OF DEPENDENCIES BETWEEN LAYERS.....	39
18.3	GRAPH OF DEPENDENCIES BETWEEN ASSETS.....	40
18.4	BUSES: DEPENDENCIES BETWEEN ASSETS	40
18.5	BLOCKS: DEPENDENCIES BETWEEN ASSETS.....	41
18.6	MAP OF DEPENDENCIES BETWEEN ASSETS	41
19	VALUATION OF ASSETS	43
19.1	NULLIFY A VALUATION.....	44
19.2	AVAILABILITY VALUATION	46
20	DOMAIN VULNERABILITIES	48
21	IDENTIFICATION OF THREATS	49
22	VALUATION OF THREATS	52
23	TECHNICAL VULNERABILITIES (CVE).....	54
24	PROJECT PHASES.....	55
24.1	COMBINATION AND REMOVAL OF PHASES.....	55
25	IDENTIFICATION OF SAFEGUARDS.....	57
26	EVALUATION OF SAFEGUARDS PER DOMAIN	59
26.1	MATURITY TRAFFIC LIGHT	61
26.2	OPERATIONS	62
26.3	SEARCHES	63
27	EVALUATION OF SAFEGUARDS FOR ONE ASSET	64
28	ADDITIONAL PROTECTIONS.....	65
28.1	ADDITIONAL PROTECTIONS FOR ONE ASSET	65
29	EVALUATION OF SECURITY POLICIES.....	66
30	EVALUATION OF SECURITY PROCEDURES.....	67
31	IMPACT & RISK: ACCUMULATED VALUES	68
31.1	RESIDUAL VALUES.....	68
32	IMPACT & RISK: DEFLECTED VALUES.....	70
32.1	RESIDUAL VALUES.....	71
33	ACCUMULATED IMPACT AND RISK TABLES	72
33.1	RESIDUAL VALUES.....	73
34	DEFLECTED IMPACT AND RISK TABLES	74
34.1	RESIDUAL VALUES.....	75

35	TEXTUAL REPORTS.....	76
35.1	REPORT TEMPLATES.....	76
36	GRAPHICAL REPORTS.....	78
36.1	VALUE / SECURITY DOMAIN.....	78
36.2	VALUE / ASSET.....	78
36.3	SAFEGUARDS / ASPECT.....	78
36.4	SAFEGUARDS / STRATEGY.....	78
36.5	SAFEGUARDS / TYPE OF PROTECTION.....	78
36.6	ACCUMULATED IMPACT / ASSET.....	79
36.7	ACCUMULATED IMPACT / DIMENSION.....	79
36.8	ACCUMULATED RISK / ASSET.....	79
36.9	ACCUMULATED RISK / DIMENSION.....	80
36.10	ACCUMULATED RISK / DIMENSION / PHASE.....	80
36.11	DEFLECTED IMPACT.....	80
36.12	DEFLECTED RISK.....	80
36.13	PARETO.....	81
37	SECURITY PROFILES.....	82
38	INTERRUPTION STEPS (BCM).....	84
38.1	FORMAT TO DESCRIBE DOWN TIME.....	84
39	DOMAIN VALUATION (BCM).....	86
40	ASSET VALUATION (BCM).....	87
41	VALUATION OF THREATS (BCM).....	89
42	EVALUATION OF BACKUP EQUIPMENT (BCM).....	91
43	IMPACT & RISK: ACCUMULATED VALUES (BCM).....	92
44	IMPACT & RISK: DEFLECTED VALUES (BCM).....	93
45	DRP - DISASTER RECOVERY PLAN(S) (BCM).....	94
45.1	THE MEANING OF ENABLED ASSETS.....	95
46	PROJECTS IN XML.....	97
46.1	FORMAT (IMPORT AND EXPORT).....	97
46.2	XML SCHEMA DEFINITION (W3C SCHEMA).....	99

1 About Risk Management

In order to know the security position of a system, we need to model it, identifying and valuing its assets, and identifying and valuing the threats on those assets. So, we can estimate the risk the system is subject to.

The risk may be mitigated by means of safeguards or countermeasures deployed for protecting the system. It is unusual that safeguards reduce risk to zero; it's rather more frequent that a residual risk remains, that the organization may accept, or try to reduce further, establishing a security plan oriented to push the risk down to acceptable levels.

Risk analysis is an activity that provides information for risk treatment activities. These activities are run once and again, so new assets are taken into account, new threats, new vulnerabilities, and new safeguards.

EAR is a toolkit that provides support for

- either a risk analysis project, over the traditional security dimensions (confidentiality, integrity, availability, ...)
- or a business continuity project, focussed on the availability of the system, in order to short down the interruption of the services when incidents or disasters occur.

In either case, the analysis may be qualitative or quantitative.

PILAR implements the methodology Magerit: [\[\[http://www.csi.map.es/csi/pg5m20.htm\]\]](http://www.csi.map.es/csi/pg5m20.htm)

1.1 Suggested reading

- Magerit: [\[\[http://www.csi.map.es/csi/pg5m20.htm\]\]](http://www.csi.map.es/csi/pg5m20.htm). Chapter 2, "Undertaking the Analysis and Management", of "Book I: The Method" , of "Magerit version 2: Methodology for Information Systems Risk Analysis and Management".
- [ISO/IEC 27005:2008](#) - Information technology - Security techniques - Information security risk management
- [NIST SP 800-30:2002](#) - Risk Management Guide for Information Technology Systems

1.2 Other documentation about PILAR

- Glossary of Terms: [\[\[http://www.ar-tools.com/en/glossary/index.html\]\]](http://www.ar-tools.com/en/glossary/index.html)
- PILAR: [\[\[http://www.ar-tools.com/en/tools/pilar/doc.htm\]\]](http://www.ar-tools.com/en/tools/pilar/doc.htm)

2 Use cases

2.1 New user

1. Install and start the application: see "[Installation](#)."
2. See "[first screen](#)"
3. Choose risk analysis / qualitative analysis
4. Create a new project
5. PILAR standard: In Edit / Options, select
 - [valuation of the domains](#): ON
 - [threats](#): Automatic
6. [Identify assets](#), at least
 - some essential information
 - any essential service
 - some equipment
7. [Value the security domain](#)
8. PILAR standard: [Identify the safeguards that apply](#)
9. [Evaluate safeguards](#)
10. Examine the [residual risk](#)
11. Repeat steps 8, 9 and 10 until satisfied
12. Verify that you meet the [security profile\(s\)](#) you are be interested on
13. Repeat steps 8, 9, 10 and 11 until satisfied

2.2 Advanced user

[If you want to value assets using dependencies.](#)

[To apply a different profile of threats.](#)

[To change a threat manually.](#)

[If you want to know the deflected risk.](#)

[If you need more phases.](#)

[If you want to evaluate the security policies separately.](#)

[If you want to evaluate the security procedures separately.](#)

[If you want to evaluate other security profiles.](#)

[If you want to make a quantitative analysis.](#)

3 Control panels

3.1 Risk analysis

[[basic = PILAR Basic]]

[[std = standard]]

	micro	basic	standar /basic	standar /medium	standar /expert
Project	yes	yes	yes	yes	yes
Information sources	no	no	no	yes	yes
Security domains	1	yes	yes	yes	yes
Subset of dimensions	no	no	no	no	yes
Subset of criteria	no	no	no	yes	yes
Subset of threats	no	no	no	no	yes
Risk analysis					
- qualitative	yes	yes	yes	yes	yes
- quantitative	no	no	yes	yes	yes
Assets					
- identification	essential	yes	yes	yes	yes
- asset classes	yes	yes	yes	yes	yes
- CPE names	no	no	no	no	yes
- domain valuation	yes	yes	yes	yes	yes
- asset valuation	no	no	yes	yes	yes
Threats					
- identification	auto	auto	yes	yes	yes
- domain vulnerabilities	yes	yes	yes	yes	yes
- valuation	auto	auto	yes	yes	yes
- technical vulnerabilities (CVE)	no	no	no	no	yes
Risk treatment					
- Project phases	2	2	yes	yes	yes
- Safeguards					
- - identification	no	yes	yes	yes	yes
- - valuation	no	yes	yes	yes	yes
- policies	no	no	no	yes	yes
- procedures	no	no	no	yes	yes

- additional protections	no	no	no	yes	yes
Impact & risk					
- accumulated impact	no	no	yes	yes	yes
- accumulated risk	no	yes	yes	yes	yes
- deflected impact	no	no	no	no	yes
- deflected risk	yes	no	no	no	yes
Reports					
- text	specific	yes	yes	yes	yes
- + templates	yes	yes	yes	yes	yes
- graphical	specific	yes	yes	yes	yes
- DB	no	no	opt	opt	opt
Security profiles	1	yes	yes	yes	yes

3.2 BCM – Business Continuity

[[bcm = business continuity]]

	micro	basic	standar /basic	standar /medium	standar /expert
Project	no	no	yes	yes	yes
Information sources	no	no	no	yes	yes
Security domains	no	no	yes	yes	yes
Interruption steps	no	no	yes	yes	yes
Subset of criteria	no	no	no	yes	yes
Subset of threats	no	no	no	no	yes
Risk analysis					
- qualitative	no	no	yes	yes	yes
- quantitative	no	no	yes	yes	yes
Assets					
- identification	no	no	yes	yes	yes
- asset classes	no	no	yes	yes	yes
- domain valuation	no	no	yes	yes	yes
- asset valuation	no	no	yes	yes	yes
Threats					
- identification	no	no	yes	yes	yes
- domain vulnerabilities	no	no	yes	yes	yes
- valuation	no	no	yes	yes	yes

Risk treatment					
- Project phases	no	no	yes	yes	yes
- Backup equipment	no	no	yes	yes	yes
- Safeguards	no	no			
- - identification	no	no	yes	yes	yes
- - valuation	no	no	yes	yes	yes
- policies	no	no	no	yes	yes
- procedures	no	no	no	yes	yes
- DRP: disaster recovery plan	no	no	no	yes	yes
Impact & Risk					
- accumulated impact	no	no	yes	yes	yes
- accumulated risk	no	no	yes	yes	yes
- deflected impact	no	no	no	no	yes
- deflected risk	no	no	no	no	yes
Reports					
- text	no	no	yes	yes	yes
- + templates	no	no	yes	yes	yes
- graphical	no	no	yes	yes	yes
- DB	no	no	opt	opt	opt

4 Installation

4.1 Java environment

You need a

JRE - Java Runtime Environment

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

4.2 PILAR (Windows)

When java is installed ...

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

4.3 PILAR (UNIX, Linux, ...)

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

When java is installed ...

- uncompress `pilar_<version>_<lang>.tar.gz` where appropriate (several languages may share the same installation directory)
- when the installation completes, there will be a file `pilar.jar` where you decided to install the software.

4.4 PILAR (Mac OS X)

Java is already installed as part of the system software.

- open `pilar_<version>_<lang>.dmg`
- execute INSTALL, selecting the destination of the files as convenient for you
- when the installation completes, there will be a file `... / pilar_51.app`

4.5 Usage

Run `pilar.exe` or `pilar.jar`:

- it will ask for a configuration file:
`STIC_en.car`

- then go to the “[first screen](#)”

The .car file specifies a directory. If there are more than one library (.bgr file) in the directory, PILAR asks the user to select one, and only one, to load. You may have several libraries in the same directory; but you may use only one in an analysis.

See “First time” screens on the web: [[http://www.ar-tools.com/en/tools/pilar/first_time/index.html]]

5 1st Screen

[[s1 = first screen]]

Quick start

To see a risk analysis (read only):

- click **mode / presentation**
- click **Qualitative analysis**

To work in a new or existing project:

- click **mode / working**
- go to the directory where you saved the licence (.lic file) and select it
- click **Qualitative analysis**

This first screen determines the working mode.

configuration

Choose a working configuration for the tools; that is, working language and library.

Usually, you will choose

`STIC_en.car`

at the installation directory.

mode

There are two modes to use PILAR:

- **presentation:**
you may browse results, but you cannot edit data.
- **working:**
you may use the full set of possibilities.
(you need a commercial license)

license

A license is needed to go beyond presentation (view-only) mode. Either select the license you received, or auto-generate an evaluation license for 30 days, or order a commercial license.

Read Only

Read-only mode enables browsing, but prevents [accidental] data modification.

Usage license

The license panel displays the currently selected license. Use the license menu to select a working license, that will be remember after the first selection.

Tool selection

- Risk Management
- Business Continuity (not in Pilar Basic)

In both tools, you may choose between

- a qualitative analysis (a list of relative values)

- a quantitative analysis (monetary cost of security incidents)
(not in Pilar Basic)

6 Control board

[[menu_project = project menu]]

The main screen starts empty. This section describes menus. When working with a project, either new or loaded, the screen body works as a control panel.

6.1 Project menu (Pilar Standard)

		Basic Standard
Project menu		
New	Starts a new project from scratch	
Reopen	Returns to recent projects	
Reload	Reloads project from external source	
Save	Sends a copy onto the disk	
Import (xml)	Imports data in XML format. See [[http://www.ar-tools.com/en/tools/pilar/doc.htm]]	
Export (xml)	Exports project data onto XML format. See [[http://www.ar-tools.com/en/tools/pilar/doc.htm]]	
Save and exit	Saves project, and terminates	
Cancel and exit	Terminates without saving data	

6.2 Project menu (Pilar Basic)

		Basic Standard
File menu		
New	Starts a new project from scratch	
Open	Starts an existing project	
Reopen	Returns to recent projects	
Save	Sends a copy onto the disk	
Save as ...	Saves a copy, where the user may select the file, and establishes a password	
Save and exit	Saves data on file, and terminates	
Cancel and exit	Terminates without saving data	

6.3 File menu (Pilar Standard)

		Basic Standard
File menu		
Open	Starts an existing project from a file	

Merge	Merges another project into this one
Save as ...	Saves a copy, where the user may select the file, and establish a password

6.4 DB menu (Pilar / database enabled)

		Basic	Standard
File menu			
Open		Starts an existing project from a database	
Merge		Merges another project into this one	
Save as ...		Saves a copy, where the user may select the database, and establish a password	
Export library		Exports library data to external tables	
Export library extensions		Exports library extensions to the library to external tables	

Database tables are described in a separate document. See “[Additional documents](#)”.

Database access requires a JDBC connector to establish a connection to a database server, either local or on the network. Most databases require a user and password to access. Therefore, PILAR asks for a number of parameters to establish the connection. If you do not understand any of the data, ask your database administrator.

For new projects, the database must be created before PILAR can connect to it. PILAR will create tables as needed.

A large number of databases may be used, anyone with a JDBC connector: MySQL, Oracle, IBM DB2, Microsoft SQL Server, Apache Derby, PostgreSQL, ...

6.5 Edit menu

[[edit/options = edit / options]]

6.5.1 Preferences

Sets user's preferences for type and size of text.

font type type of letter, within those available on the system

font size character size

6.5.2 Options – Valuation of domains

The information system may be valuated asset by asset or by security domains.

You are always requested to value the essential assets.

If valuation by domains is ON, the value of the essential assets is uniformly applied to all the assets in the domain.

If valuation by domains is OFF, the value is distributed according to dependencies between assets.

Domain valuation is faster; while dependencies are more precise.

6.5.3 Options – Frequency

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	L likely	H high	M medium	10
M medium	U unlikely	M medium	D difficult	1
S small	R rare	L low	VD very difficult	0.1

6.5.4 Options – Degradation

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%

6.5.5 Options – Threats

manual:

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

automatic:

the system applies the standard valuation as needed, and reapplies as needed as well (this is the behaviour in Pilar Basic)

6.5.6 Options – Project phases

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

linked

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

independent

no value is inherited from any previous phase

6.5.7 Options – Unevaluated safeguards

If a safeguard is not evaluated, PILAR will use the specified value in this option.

ignore (= n.a.)

as if the safeguard were meaningless for this system

non existent (= L0)

as if the safeguard were needed, but not deployed (this is the default behaviour before version 4.4)

6.5.8 Options – Export: safeguards

6.5.9 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).

6.5.10 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.

6.6 Domains and phases

[[domains_phases = domains and 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.

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

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	7 th	4 th	1 st	3 rd	2 nd	1 st
domain 1	8 th	5 th	2 nd	6 th	5 th	4 th
base	9 th	6 th	3 rd	9 th	8 th	7 th

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	7 th	4 th	1 st	3 rd	2 nd	1 st
domain 1	8 th	5 th	2 nd	6 th	5 th	4 th

base	9th	6 th	3 rd	9 th	8 th	7 th
------	-----	-----------------	-----------------	-----------------	-----------------	-----------------

6.7 Level menu

		Basic	Standard
Level menu			
Controls how many options are presented to the user			
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		

See “[control boards](#)”.

6.8 Help menu

		Basic	Standard
Help menu			
help	starts the in-line help pages		
references	lists international standards related to risk analysis and management		
about	shows version information		
last version?	connects to EAR web site to check for updates		
system status	presents current usage of system resources		

When working on a project, the central panel shows the different activities of analysis and treatment. Jump as needed.

7 Project data

[[rm21 = project data]]

Basic

Standard

Quick start

Select a code and a descriptive name.

Optionally, click **STANDARD** and add some descriptive information.

Click **OK** to continue.

To input data related to the project (mostly, administrative data).

library	identifies the used library (fixed on start: .car file)
TSV	selects a file as default to identify threats and assign values to them; if you use the file threats.tsv in the library directory, the box shows "library"
code	of the project
name	short title of the project A long description may be introduced with the " description " button on the bottom.

The library is chosen when the project is created. It needs to be one of those available in the system. It cannot be changed later on.

However, the library is only identified by its code. This is required to switch languages, and to load new versions of the same library.

To choose a library, the user may take into consideration the adequacy of the library contents to his current project. But most often, the library is mandated by the organization's policy or an external reference that imposes a given collection of elements.

Other data

You may introduce any other data for administrative purposes. Nothing is mandatory by the tool; but there is some standard information:

- description
- owner, responsible people, ...
- organization
- system classification level
- security policy to apply
- version
- date
- historical data
- ...

There is no limit on the number of entries. There may be several entries with the same label.

The standard values may be defined for an organisation editing the values in the library

PILAR / bib_en / info_en.info

```
<model>
  <key c="desc">description</key>
  <key c="resp">responsible</key>
  <key c="org">organisation</key>
  <key c="ver">version</key>
  <key c="date">date</key>
</model>
```

Labelled entries may be managed with the buttons below

up	the row on the cursor is moved up
down	the row on the cursor is moved down
new	add a new entry
delete	the row on the cursor is removed
standard	loads a typical set of labels (uses the info file in the library – see above)
clean	removes empty rows

8 Information sources

[[rm22 = information sources]]



This screen is used to identify and manage information sources.

To declare a new source

- select the source previous to the new one
- click NEW SOURCE
- fill in the data

To add a new source at the end

- do not select any source
- click NEW SOURCE
- fill in the data

To edit the source data

- select a source
- click EDIT SOURCE

To move sources up (before the previous one)

- select one or more sources
- click MOVE UP (or SHIFT + UP_ARROW)

To move sources down (after the next one)

- select one or more sources
- click MOVE DOWN (or SHIFT + DOWN_ARROW)

To remove sources

- select one or more sources
- click DELETE THE SOURCE (or DEL)

9 Security domains

[[ra_sd = 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.

To create a new domain

- select another root (the next node of the new node) or the root node if the new domain is independent
- click on NEW DOMAIN
- fill in the data

To edit the domain data

- select a domain
- click EDIT DOMAIN

To move domains up (before the previous one)

- select one or more domains
- click MOVE UP (or SHIFT + UP_ARROW)

To move domains down (after the next one)

- select one or more domains
- click MOVE DOWN (or SHIFT + DOWN_ARROW)

To move domains left (become brothers of the current father)

- select one or more domains
- click MOVE LEFT (or SHIFT + LEFT_ARROW)

To move domains right (become sons of the current elder brother)

- select one or more domains
- click MOVE RIGHT (or SHIFT + RIGHT_ARROW)

To remove domains

- select one or more domains
- click DELETE THE DOMAIN (or DEL)

To accept the new data

- click on OK

To discard the new data

- click on CANCEL

10 Selection of dimensions

[[rm23 = selection of dimensions]]



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.

11 Selection of valuation criteria

[[rm24 = selection of valuation criteria]]



The standard library establishes the criteria to assign value levels to assets.

However, you may switch off some criteria. Select the criterion and click ON / OFF buttons on the bottom.

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

12 Selection of threats

[[rm25 = selection of threats]]



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.

13 Value quantification

[[rm26 = value quantification]]



This screen allows associating qualitative valuation levels and quantitative values for changing from one to other type of analysis.

value	the first column shows the qualitative level. It is fixed.
library	the second column shows the standard association in the library. It is fixed.
project	the third column shows the association you want for this project. You may edit it.

You may edit any value on the third column, as far as it is between the values above and below.

It is recommended to use some exponential (or logarithmic) scale.

RESET is used to copy values from the second column into the third one.

After changing the association, close the model and re-open it, since changes apply to the next execution.

PILAR allows associating qualitative valuation levels to quantitative values. This association works only if the user does not provide information for both.

In qualitative analysis, when several services depend on one single equipment, the accumulated level on the shared equipment is the maximum of the service levels above. You lose the information that the many services make it a shared point of failure. Quantitative analysis shows that accumulation by adding values.

In quantitative analysis, when one server with a highly qualified service is compared to another server with several lower qualified services, the addition of many small values may overtake the single high value, and you may be driven to protect quantity rather than quality. Qualitative analysis shows the difference by taking the maximum level.

The same model may be opened either as qualitative or quantitative. PILAR adapts the analysis to the opening option. If you open qualitative, PILAR uses qualitative valuation levels, either those you entered, or the ones derived from the stated quantities. If you open quantitative, PILAR uses values, either those you entered, or those derived from the stated levels.

Qualitative level to quantitative value

It is used when the user only provides qualitative valuation. Still PILAR is able to run a fictitious quantitative analysis where the impact of many services on a single equipment shows up. So it may be informative to run a qualitative model in quantitative terms.

Quantitative value to qualitative level

It is used when the user only provides quantitative valuation. Still PILAR is able to run a qualitative analysis where the impact of a highly valued service shows up. So it may be informative to run a quantitative model in qualitative terms.

14 Identification of assets

[[ra_ai = identify assets]]

Basic

Standard

Quick start

Go to **layers** menu (above) and click **STANDARD**.
 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 of 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 also 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

14.1 Layers

To insert the standard layers (from info.info file in library directory)

- layers / standar 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 / remove layer

or

- select a layer
- right click + remove layer

or

- select a layer
- click SUPR

To move a layer to another position

- drag & drop with the mouse

14.2 Assets

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 group of assets

or

- select one layer
- right click / new group of assets

or

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

To insert an asset that duplicates another one

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

or

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

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 the asset

or

- select one asset
- right click / delete / delete the 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 indicate whether one asset is subject to threats or not

- select one asset
- menu assets / has threats / ...

or

- select one asset
- right click / has threats / ...

To indicate whether one asset is visible or not

- select one asset
- menu assets / visible / ...

or

- select one asset
- right click / visible / ...

To indicate whether one asset exists or not

- select one asset
- menu assets / exists / ...

or

- select one asset
- right click / exists / ...

To indicate whether one asset is available or not

- select one asset
- menu assets / available / ...

or

- select one asset
- right click / available / ...

To move one asset to another place in the tree

- drag & drop

14.3 Security domains

To edit the security domains

- menu domains / edit

14.4 Statistics

Generates a report of how many assets of each major class per layers, domains or information sources. Be aware that one asset may be qualified with several classes, so the numbers do not add obviously.

The table can be printed clicking on the right button.

14.5 Description of one asset

[[ra_ai1 = description of one asset]]

Basic **Standard**

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.

To characterize asset:

- unique code
- short name
- class(es) of assets that match this one
- domain
- sources of information
- description (informative)

Asset classes

Choose on the right panel.

Assets may be composed: a bit of several classes.

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

[X] denotes a selected class. [-] denotes that some subclass of it is selected.

Informative data

You may add other data for information purposes.

Nothing is mandatory, but usual fields are:

- description
- proprietary or owner
- product name and code
- manufacturer
- provider
- number of
- location
- ...

There is no limit on the number of entries.

There may be several entries with the same label.

Put the mouse on a line ...

up	the row on the cursor is moved up
down	the row on the cursor is moved down
new	add a new entry
delete	the row on the cursor is removed

On the complete data set:

standard	loads a typical set of labels
clean	removes empty rows

Information sources (not in Pilar Basic)

Click on the SOURCES box. There will show up a checklist of declared sources. Check as appropriate.

Security domain

Click on the DOMAIN box. There will pop up a list of declared domains. Choose as appropriate.

14.6 Asset: is it subject to threats?

The assets are usually subject to threats. When indicating that an asset has no threats, the threat profile proposals are ignored.

14.7 Asset: is it visible?

When an asset is not visible, it is not shown on screen or in reports.

14.8 Asset: does it exist?

When an asset does not exist, it does not exist or has value, or spread it, or have threats, or risk, or need safeguards.

14.9 Asset: is it available?

When an asset is not available, those that are critically dependent on it are not available either; ie, its superiors in the dependency tree, except for those with alternative options (OR).

15 Association of classes to assets

[[ra_ac = association of classes to assets]]

Basic Standard

This screen associates classes to assets.

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

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)

or click REMOVE

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)
- select the target asset (left panel)
- click APPLY

16 Association of CPE names to assets

[[ra_cpe = Common Product Enumeration]]

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

See [\[\[http://www.ar-tools.com/en/tools/pilar/doc.htm\]\]](http://www.ar-tools.com/en/tools/pilar/doc.htm)

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

[\[\[http://nvd.nist.gov/download.cfm\]\]](http://nvd.nist.gov/download.cfm)

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 DEL

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

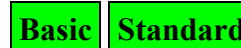
- select one or more names on the right panel
- click ASSETS

To search for an asset or a CPE name

- ctrl-F on the appropriate panel

17 Valuation of security domains

[[ra_dv = domain valuation]]



In PILAR Basic, this is the only way to value the information system.

In PILAR Standard, you may choose

[Edit / Options / domain valuation / ...](#)

This approach provides a quick but imprecise assessment common for all the assets in the 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.

Valuation of the essential assets

For each essential asset, information or service, you can set a valuation that is, make the required level of security in the dimensions of availability (A), integrity (I), confidentiality (C), authenticity (Auth) and accountability (Acc). To set a level, click-click the cell you want to edit and select the criterion or criteria that apply to the case.

HIGH	7	high requirements
MEDIUM	4	medium requirements
LOW	1	low requirements
no value	0	no need to protect

When selecting several criteria, PILAR will keep the higher level. If you wish the level to be X, despite using criteria from another section, mark X in a outer section.

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.

Valuation of the domains

Each domain inherits the valuation of assets and main contents of the associated with 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

18 Dependencies between assets

[[ra_ad = dependencies between assets]]

Basic

Standard

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).

<i>left panel menu</i>		<i>right panel menu</i>	
only layers	collapses the tree to the first level	only layers	collapses the tree to the first level
- (minus)	decrements depth by one	- (minus)	decrements depth by one
counter	sets de desired depth	counter	sets de desired depth
+ (plus)	increments depth by one	+ (plus)	increments depth by one
+1	if selected, one more level of the tree is displayed: the children immediately below		
show children	for the selected father asset, selects the children assets in the right panel	show parents	for the selected child asset, selects the father assets in the left panel

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 them, 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 DELETE

or

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

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 to establish a value

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

18.1 Dependencies per dimension of security

[[ra_add = dependencies per dimension of security]]

Basic **Standard**

You may specify a different dependency degree for each dimension of security. To do so, 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

The first row is to set a common value on every dimension.

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.

18.2 Map of dependencies between layers

[[layer_map = map of dependencies between layers]]

Basic **Standard**

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

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

18.3 Graph of dependencies between assets

Basic **Standard**

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).

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.

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

18.4 Buses: dependencies between assets

Basic **Standard**

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.

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

18.5 Blocks: dependencies between assets

Basic **Standard**

The graph shows the relationships between assets. It only presents all the assets you can see on the main screen. It follows the collapse / expand status of the asset tree.

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, it becomes green, those above turn red, and those below turn blue.

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

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

18.6 Map of dependencies between assets

Basic **Standard**

The map is for graphically studying the dependencies.

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

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

19 Valuation of assets

[[ra_av = valuation of assets]]

Basic

Standard

Quick start

Which is your major concern with this information system?

- Select an 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.

Left column covers data (organised in layers and groups). It may be expanded and collapsed.

The other columns cover security dimensions. Only assets may receive values; the other rows are dead.

To assign value to an asset

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

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.

Checked criteria determine the qualitative level assigned to the asset in the stated dimension.

When done with the data ...

- click ACCEPT to save the new data
- click DO NOT VALUE to remove value from the asset
- click CANCEL to leave the asset as it was.

To discover where does the accumulated value come from ...

- select the asset (row)
- click SOURCES

Top menus:

Edit menu		
copy	ctrl.-C	saves the values of the selected cells
paste	ctrl-V	places the saved values onto the new selected area

Export menu	
to csv	generates a csv file with the shown values (for spreadsheets)
to xml	generates an xml file with the valuation

Import menu	
from xml	reads the valuation from an xml file

Bottom menus

only layers	the tree of assets is collapsed into level 1
- (minus)	decrement tree expansion by one
value	set tree expansion level
+ (plus)	increment tree expansion by one
copy	copies valuations into the pad
paste	pastes valuations from the pad
sources	select an asset, and click to discover where does the accumulated value come from
own / accumulated	switches between values to be presented: own - only values with an explicit assignment accumulated - values with own value show on white background, while accumulated value is shown on colour background
mark	select a value cell, clicking on this button will color the assets to which this value is transmitted

19.1 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 NA.

comment

criteria for valuation

- [n.a.] not applicable
- ▶ [10] Level [10]
- ▶ [9] Level [9]
- ▶ [8] Level [8]
- ▶ [7] Level [7]
- ▶ [6] Level [6]
- ▶ [5] Level [5]
- ▶ [4] Level [4]
- ▶ [3] Level [3]
- ▶ [2] Level [2]
- ▶ [1] Level [1]
- ▶ [0] Level [0]

apply do not value cancel

```

    graph TD
      A1[A1] --- A2[A2]
      A2 --- A3[A3]
  
```

availability: valuation of assets - José A. Mañas (dev)

Edit Export Import

asset	[A]	[I]	[C]	[Auth]	[Acc]
ASSETS					
▼ [E1]					
S [A1]	[7]	[7]	[7]		
A [A2]	[7]	[n.a.]	[7]		
A [A3]	[7]		[7]		
▶ [E2]					
▶ [E3]					

- 1 + sources own value mark

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

19.2 Availability valuation



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

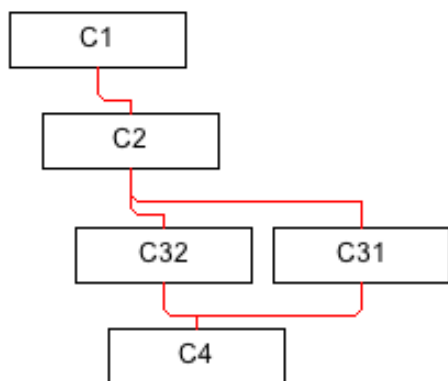
- establishing exact [dependencies](#) between assets
- [nullifying](#) the value
- marking some qualifiers (see below)

If the asset is marked as "[availability.easy]", 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]", 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.



availability: valuation of assets – José A. Mañas (full)

Edit Export Import

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]		

- +

20 Domain vulnerabilities

[[ra_t_dv = domain vulnerabilities]]

Basic **Standard**

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 "[threat valuation](#)"). TSV is applied automatically if threats are set to automatic (see [Edit / Options / threats / ...](#)).

To associate a vulnerability to a domain

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

To remove a vulnerability association

- select the vulnerability (on the left panel)
- click REMOVE

To discover the vulnerabilities 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 vulnerability (on the right panel)
- click DOMAINS (right panel, top)

21 Identification of threats

[[ra_ti = threat identification]]

Basic

Standard

In Pilar Basic, this screen is only for information. Users may not modify entries.

Quick start

1. Select **ASSETS** on the left panel (top).
2. Click **LIBRARY** (bottom left).
3. You have just set a standard threat map, based on the classes of the assets.
4. Click **OK** to continue.

Even faster start

Select automatic threats in [Edit / Options / threats / ...](#)

Let us identify which threats are possible for each asset. Later on, the vulnerability will be estimated.

NOTE. If threats are set to [Edit / Options / threats / automatic](#), then some buttons are disabled:

- copy & paste
- import from XML
- apply and delete
- undo / redo

If you wish to apply a different threat profile

- click on **LOAD**

There are two panels

left panel	right panel
a tree with: <ol style="list-style-type: none"> 1. the assets (classified into layers and groups) 2. the threats currently identified 	a tree with: <ol style="list-style-type: none"> 3. the threats known by PILAR

Top menus:

left panel (TOP)	
- (minus)	decrements assets' tree expansion
number	sets the expansion of the tree of assets
+ (plus)	increments assets' tree expansion
+1	expands the tree one level more, showing threats per asset
suggest	selects (on the right) the standard threats for the selected assets (on the left)
threats	selects (on the right) the identified threats for the selected assets (on the left)

right panel (TOP)	
- (minus)	decrements threats' tree expansion
number	sets the expansion of the tree of threats
+ (plus)	increments threats' tree expansion
assets	selects (on the left) the assets subject to the selected threats (on the right)

Bottom tool bar:

load	loads a TSV file: a threat profile
library TSV	applies the current TSV; the button shows either a loaded TSV, or "library" to refer to the standard one
undo	reverses the last assignment of threats to assets
redo	reapplies what was undone
apply	adds to the selected asset(s) on the left the threat(s) selected on the right
remove	removes the selected threats on the left, or removes the selected threats (right) from the selected assets (left)

To assign a threat to an 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

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

or

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

Which threats are on an asset?

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

To "copy and paste" threats from an asset onto another

- select the source asset on the left
- click THREATS to select on the right
- 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

You may use the library to help. Select one or more assets on the left panel, and then ...

- click SUGGEST to discover the proposal from the library
- click LIBRARY to apply the suggestions from the library
- click LOAD to use a different threat profile (TSV file)

22 Valuation of threats

[[ra_tv = threat valuation]]



Quick start

1. Select **ASSETS** on the first column (top).
2. Click **LIBRARY** (bottom middle).
3. You have just set a standard threat map, based on the classes of the assets.
4. Click **OK** to continue.

Even faster start

Select automatic threats in [Edit / Options / threats / ...](#)

After determining which threats are relevant to each asset, let's introduce the vulnerability of the asset.

NOTE. If threats are set to [Edit / Options / threats / automatic](#), then some buttons are disabled:

- copy & paste
- import from XML
- apply and delete
- undo / redo

If you wish to apply a different threat profile

- click on LOAD

column		
1	selection	select a few assets /threats to apply an action <ul style="list-style-type: none"> • click to check / uncheck • SHIFT + click to check / uncheck a range • click on header to uncheck everything
2	tree of assets + threats	double click to expand / collapse
3	likelihood	for each threat, show the likelihood for it to occur. Use the buttons to select a value or input a likelihood estimate.
4 ...	dimensions	for each dimension, show the degradation of value caused by the threat. Double click to edit values are in the range 0% - 100%.

The degradation is shown for each threat on each dimension using white background. For assets, it is shown the worst degradation using green background..

Top menus:

Edit menu		
options		Sets the preferred format for likelihood and degradation
copy	ctrl.-C	saves the values of the selected cells
paste	ctrl-V	places the saved values onto the new selected area

Export menu		
to csv		generates a csv file with the shown values (for spreadsheets)
to xml		generates an xml file with the valuation

Import menu		
from xml		reads the valuation from an xml file

Bottom tool bar:

- (minus)	decrements the expansion level of the assets tree
number	sets the expansion level of the assets tree
+ (plus)	increments the expansion level of the assets tree
+1	shows one level more: threats per asset
copy	takes not of the selected values
paste	applies copied values to a new location
load	loads a TSV file: a threat profile
library TSV	applies the current TSV; the button shows either a loaded TSV, or "library" to refer to the standard one
undo	reverses the last assignment of values to threats
redo	reapplies the last assignment undone
clear	removes values from selected rows

You may edit the values manually or, much better, use the library to help. Select one or more assets on the left column, and then ...

- click LIBRARY to apply the suggestions from the library
- click LOAD to use a different threat profile (TSV file)

23 Technical vulnerabilities (CVE)

[[ra_cve = Common Vulnerabilities and Exposures]]



See [[<http://www.ar-tools.com/en/tools/pilar/doc.htm>]].

To associate CVE vulnerabilities to assets, they need to have one or more [CPE names](#) associated.

The columns show the values associated with a vulnerability in the format CVSS v2 (see [[<http://nvd.nist.gov/cvss.cfm>]]).

The vulnerability information is extracted from external files in XML format that the user can provide himself or download it from a repository of vulnerabilities, e.g.

[[<http://nvd.nist.gov/download.cfm>]]

To find vulnerabilities that apply to an asset

- select one or more assets (first column)
- click on FIND
- choose the XML file data

To update the vulnerabilities associated with an asset

- select one or more assets (first column)
- click on UPDATE
- choose the XML file data

To eliminate vulnerabilities associated with an asset

- select one or more active (first column)
- click DELETE

To edit the parameters characterizing a vulnerability associated with an asset

- double-click the asset
- enter data into the edit screen

24 Project phases

[[rt_ph = 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 a number of 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

To create and maintain system phases.

new phase	to add a new phase
edit	to edit the data of a phase
up	to move a phase up (before the previous one) also SHIFT + UP_ARROW (one or more phases)
down	to move a phase down (after the next one) also SHIFT + DOWN_ARROW (one or more phases)
merge	the valuation of safeguards in the selected phase is merged into the valuation in the next phase; 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).
delete	to remove a phase

The actions “up”, “down”, “merge” and “delete” do not occur immediately. PILAR will rather take note, and execute when leaving this screen. Nothing will happen until the OK button is clicked.

24.1 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	

25 Identification of safeguards

[[rt_si = identification of safeguards]]



Quick start

1. Click **recommendation** in the middle of the bottom bar.
2. Click OK.

That's it: you have accepted the recommendation of PILAR.

If you do not agree 100%, you may edit as needed.

This screen allows removing from the analysis those safeguards that are regarded as not applicable.

Discarding a safeguard may be easy to explain when the safeguard is for assets we do not have, dimensions we do not care, threats that are not feasible, or for high risks. Safeguard removal shall be documented for future inspections.

The screen shows all the safeguards known by PILAR organised as a tree.

There are as many screens as security domains. The current security domain is shown on top box (blue). Click to change.

The columns of the table show

aspect	see [[http://www.ar-tools.com/en/glossary/index.html]]
strategy	type of protection ([[http://www.ar-tools.com/en/glossary/index.html]])
safeguards	the tree of safeguards click to select; double click to expand / collapse
doubts	to mark lines that further investigation or discussion; click to change
source	associated source(s) of information; click to change
comment	documentation purposes, in particular whether any safeguards are excluded (n.a.), you must document the reasons that lead to exclusion often make comments on implementation plans or describe the current situation click to change
recommendation	.
on / off	if you want to ignore a safeguard for today (to zoom into some part of the system), click to OFF
applies	click to mark as non-applicable if you think that the safeguard does not make sense in this security domain.

	Be ready to explain why.
--	--------------------------

To select all the safeguards

- click DELETE

To apply what PILAR recommends

- click RECOMMENDATION

To apply only the safeguards that are direct or indirectly referenced from one or more evaluation profiles

- click ONLY IF ...
- select the desired profiles
- click OK

You may be interested on a report of the selected and unselected safeguards. This report is known as “**Statement of Applicability**” (SoA). It is typically requested by auditors.

Right-click on a the name of a safeguard, and there will pop-up a short menu that allow you to ...

copy	copies safeguard text to clipboard
copy path	copies safeguard text and ancestors to clipboard
full path	show the safeguard in context; that is, the complete tree from the root down to this safeguard
additional information	presents additional knowledge, such as <ul style="list-style-type: none"> • aspect of security • strategy to protect • type of protection • external sources of information (links to documents)
sources	to edit (set or remove) the sources associated to a safeguard

26 Evaluation of safeguards per domain

[[rt_sdv = valuation of safeguards]]

Basic

Standard

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. Go to the **combo** on the middle, and select the maturity level that roughly matches your system (for example L2).
4. Click **OPERATION / APPLY** (bottom middle).

If you have a plan in mind ...

- Go to the cell at row **SAFEGUARDS**, and column **TARGET**. Select it.
- Go to the **combo** on the middle, and select the maturity level that you aim to.
- Click **OPERATION / APPLY** (bottom middle).

This screen allows assigning maturity level to safeguards, by domain, by project phase.

There are as many screens as security domains. The current security domain is shown on top box left (blue). Click to change.

To select the domain

- click on upper left panel
- select the domain to show

You may also filter safeguards so you can only see those related to one or more sources of information. In order to apply a filter, click on the top box right, and select sources that apply.

To filter by information source, within a domain

- click on upper right panel
- select the information source(s) to filter

Most columns are explained in the section about "[identification of safeguards](#)", but now we have as many columns as project phases.

The other columns show the maturity of the safeguard for the phase.

To assign a maturity level to a safeguard, either

- with the mouse right click on the safeguard (row) and phase (column) and select from the pop-up menu
- with the mouse select one or more cells for the safeguard(s) (rows) and phase(s) (columns), select the maturity level in the pop-up menu in the bottom bar, and click **OPERATION / APPLY**

When you assign a maturity to a safeguard without sons, the value is applied to it. When the safeguard has sons, the value is applied to every son under it.

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

When the user does not provide a value: see “[domains and phases](#)”

Most frequently, maturity grows phase to phase, but it could also decrease.

When an entry in the tree is further detailed (that is, there are children below), the value shown is calculated from the value of its children components, showing the value range below. This behaviour aims to alert the user towards weaknesses in the system. However, in calculating the efficiency of the whole set of safeguards, PILAR applies a weighted average, taking into account the recommendation as the relative weight of each item.

Bottom toolbar

expertise pop-up	select an expertise level: <ul style="list-style-type: none"> • BASIC expands to the minimum depth regarded as meaningful • MEDIUM expands explanations without going into the details • EXPERT expands thoroughly
- (minus)	expands the selected branch one level less
number	expands the selected branch to the specified depth
+ (plus)	expands the selected branch one level more
sources	select on the tree those safeguards related to one or more sources
undo	steps back the last maturity assignment
redo	re-applies the last undo'ed maturity assignment
maturity combo	selects a value to apply
operation	to apply one of the possible operations on the selected cells. see below the available operations
suggest	proposes safeguards to improve, taking into account its recommendation level and the current maturity; the screen is split into two parts: below there is an ordered list of suggestions, click on a line to locate the suggested safeguard in context (above)
find	jumps along the tree, stopping at the safeguards that meet certain criteria
>>	repeats the last find operation from the current position of the cursor

Menus above

Edit menu		
copy	Ctrl-C	takes the selected maturity cells into the notepad
paste	Ctrl-V	applies the copied values onto the selected maturity cells
find	Ctrl-F	looks for a safeguard with text matches the search pattern
Export		
to csv		generates a CSV file with the values you can see on the screen (spreadsheets)
to xml		generates an XML file with the maturity of the safeguards
report		generates a RTF file with the maturity of the safeguards (word processors)
< Lx		generates an excel report of those safeguards below a threshold
Import		
from csv		loads values from a CSV file
from xml		loads values from an XML file

Please note that the CSV file is rather fragile. The import format must be the same than the export format, and you should not modify the codes to locate the safeguards. XML format is more robust.

Right-click on a the name of a safeguard, and there will pop-up a short menu that allow you to ...

copy	copies safeguard text to clipboard
copy path	copies safeguard and ancestors to clipboard
full path	show the safeguard in context; that is, the complete tree from the root down to this safeguard
additional information	presents additional knowledge, such as <ul style="list-style-type: none"> • aspect of security • type of protection • external sources of information (links to documents)
sources	to edit (add / remove) sources of information related to the safeguard
n.a.	labels the safeguard as inadequate for the current domain (it is equivalent to tag as n.a. in the screen to " evaluate safeguards ")
applies	reverses the applicability of the safeguard in the current domain back to true (it applies)

26.1 Maturity traffic light

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:

target maturity

by default, L4; this default is useful for an absolute colour

alternatively, PILAR can paint a colour relative to the maturity in another phase:

You can select a reference phase, ie to use the maturity of the protection in the selected phase

- click the right button at the header of the phase to use as target
 - the head of the selected column is painted GREEN
 - The colour is relative to the maturity of the protection in the selected phase

to return to maturity by default, click the right mouse button on any header that is not a phase

assessed maturity

by default, PILAR compares the maturity of the last phase with the target maturity

can select any stage as an object of comparison

- 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 selected phase is higher than the maturity at the target phase
GREEN	current maturity is aligned with target
YELLOW	the maturity is poor : should be enhanced
RED	the maturity is too poor: must be enhanced
GREY	if the safeguard does not apply

26.2 Operations

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

26.3 Searches

PILAR can search through safeguards using certain criteria:

CHANGES

jumps along the tree, stopping at safeguards that change from one phase 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

NON EVALUATED

looks for unevaluated safeguards (white hole)

>>

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

27 Evaluation of safeguards for one asset

[[rt_sav = valuation of safeguards for one asset]]



This screen allows specifying the evaluation of safeguards asset by asset, being either

- common values for every asset in the domain, or
- specific values for one asset

The **first column** shows the tree of assets. Use the expand controls on the bottom tool bar to expand / collapse as appropriate.

The **second column** is *clickable*: click to jump into the safeguards evaluation screen.

The other columns stand for every project phase. In every phase you may enable / disable the usage of specific values. When enabled, the value of the safeguard for the asset is taken into consideration for the evaluation of residual impact and risk. When disabled, that value is not taken into consideration. Even when disabled, PILAR retains the values assigned to the safeguards asset by asset.

Safeguard evaluation screen

You come into this after clicking on the second column.

The screen is similar to the one to “[evaluate safeguards per domain](#)”, but now you have one tab for the asset, followed by another tab for the security domain the asset belongs to.

In the asset tab, when the value comes from the domain, the cell is displayed in grey background.

28 Additional protections

[[rt_kbdv = valuation of additional protections]]

[[rt_kbav = valuation of additional protections for one asset]]



Additional protections are, in many aspects, similar to safeguards, but are not taken into consideration to estimate residual impact and risk.

The screen shows all the protections matching assets organised as a tree.

There are as many screens as security domains, and in each domain only shows the protections for assets in the domain. The current security domain is shown on top box (blue). Click to change.

The columns of the table show

aspect	see [[http://www.ar-tools.com/en/glossary/index.html]]
strategy	type of protection ([[http://www.ar-tools.com/en/glossary/index.html]])
protections	the tree of protections, hierarchically located under the corresponding asset class (the class of assets to which it applies) click to select; double click to expand / collapse
doubts	to mark lines that further investigation or discussion; click to change
source	associated sources; click to change
comment	documentation purposes, in particular whether any protections are excluded (n.a.), you must document the reasons that lead to exclusion often make comments on implementation plans or describe the current situation click to change
recommendation	as for safeguards (see " evaluation of safeguards ")
traffic light	as for safeguards (see " evaluation of safeguards ")
maturity	there is one column for each project phase

For further guidance on the use of this screen, see "[evaluation of safeguards](#)".

However, remember that additional protections are not taken into consideration to estimate residual impact and risk.

28.1 Additional protections for one asset

In the tree, PILAR only shows the protections for the classes of assets that qualify the current asset.

29 Evaluation of security policies

[[rt_std = security policies]]



Subset of safeguards marked as "security standards" (std).

The screen is similar to the "[valuation of safeguards](#)," but limited to such safeguards.

30 Evaluation of security procedures

[[rt_proc = security procedures]]



Subset of safeguards marked as "security procedures" (proc).

The screen is similar to the "[valuation of safeguards](#)," but limited to such safeguards.

31 Impact & Risk: Accumulated values

[[rt_i_a = residual accumulated impact]]

[[rt_r_a = residual accumulated risk]]

Basic **Standard**

This screen shows the consequences of threats on assets.

column		
1	selection	select a few assets / threats to apply an action <ul style="list-style-type: none"> • click to check / uncheck • SHIFT + click to check / uncheck a range • click on header to uncheck everything
2	tree of assets and threats	double click to expand / collapse
3 ...	dimensions	shows the impact / risk on each dimension <ul style="list-style-type: none"> • for threat rows: show the impact of the threat • for asset rows: show the worst impact by some threat

Bottom tool bar:

- (minus)	decrements the expansion level of the tree of assets
number	sets the expansion level of the tree of assets
+ (plus)	increments the expansion level of the tree of assets
+1	increments the expansion level by 1 to show threats
domain	selects the assets within a given security domain
source	selects the assets for a given source of information
html	exports selected rows to an HTML file
csv	exports selected rows to a CSV file
xml	exports to xml file
db	(if database enabled) exports selected rows to database

31.1 Residual values

Basic **Standard**

There are two formats to present residual impact / risk

phases as tabs + dimensions as columns

There are as many tabs as project phases. The first one covers potential value (it is calculated ignoring every safeguard). The others show the residual value in each phase (taking safeguard maturity into account).

You may study the effect on each dimension.

phases as columns + dimensions as tabs

There are as many tabs as dimensions.

You may study the evolution along phases.

To switch between presentations, click on phase / dimension column headers.

In any presentation, you may select one or more rows, then click **MANAGE**. PILAR will drive you into the screen to [evaluate safeguards](#), so you can study which safeguards have an effect on the selected row(s). The recommendation levels will be recalculated to focus on the assets, threats, and dimensions covered by the selected row(s).

32 Impact & Risk: Deflected values

[[rt_i_d = residual deflected impact]]

[[rt_r_d = residual deflected risk]]



This screen shows the consequences of threats on assets that have a value, though threats act on the assets below. The dependencies between assets are taken into account.

column		
1	selection	select a few assets / threats to apply an action <ul style="list-style-type: none"> • click to check / uncheck • SHIFT + click to select a range • click on header to uncheck everything
2	tree of assets and threats	double click to expand / collapse
3 ...	dimensions	shows the impact / risk on each dimension <ul style="list-style-type: none"> • for threat rows: show the impact of the threat • for asset rows: show the worst impact by some threat

Bottom tool bar:

- (minus)	decrements the expansion level of the tree of assets
number	sets the expansion level of the tree of assets
+ (plus)	increments the expansion level of the tree of assets
+1	increments the expansion level by 1 to show threats
domain	selects the assets within a given security domain
source	selects the assets for a given source of information
html	exports selected rows to an HTML file
csv	exports selected rows to a CSV file
xml	exports to xml file
db	(if database enabled) exports to database

Rows show a tree with 3 levels:

level	members of the level
1	assets above in the dependency graph: assets with an explicit value
2	assets below in the dependency graph: assets that support the value of the assets in level 1; that is, assets on which level 1 assets depend on, either direct or indirectly
3	threats on the assets below

From this screen you may jump to the deflected values per phase clicking on the header of some dimension column. The table is quite similar, but dimensions become tabs, and project phases become columns. From the screen that presents the values per phase, you may return to see the values per dimension by clicking on the column headers.

You may select (on the first column) one or more rows:

- click on the check box to select / deselect the row
- click on one check box, then SHIFT + click on another check box to repeat the selection of the first box over the range to the second box
- select a domain (bottom tool bar) to select all the assets in that domain
- select a source of information (bottom tool bar) to select all the assets referenced to that source

Selections are cumulative. Click on the selection column header to clean the selection.

32.1 Residual values



There are as many tabs as project phases, presenting residual values, plus one more for the potential values.

In any presentation, you may select one or more rows, then click **MANAGE**. PILAR will drive you into the screen to “[evaluate safeguards](#)” so you can study which safeguards have an effect on the selected row(s). The recommendation levels will be recalculated to focus on the assets, threats, and dimensions covered by the selected row(s).

33 Accumulated impact and risk tables

[[rt_ir_at = accumulated impact and risk tables]]



Collects the details of the impact and risk analysis.

Columns:

column		
1	asset	the asset subject to the threat
2	threat	the threat
3	dimension	the dimension of security damaged by the threat
4	V	the value of the asset (by itself)
5	A	the accumulated value on the asset
6	D	the degradation of the value of the asset
7	I	the impact of the threat on the value of the asset
8	F	the likelihood of the threat
9	risk	the risk of the threat on the asset

Bottom tool bar:

asset	click to select a subset of assets to show
on / off	to apply (or not) the filter of assets to show
threat	click to select a subset of threats to show
on / off	to apply (or not) the filter of threats
dimension	click to select a subset of dimensions to show
on / off	to apply (or not) the filter of dimensions
legend	shows the code of colours
csv	exports shown data to a CSV file
xml	exports to xml file
db	(if database enabled) exports to database

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

Click on any header to sort by the corresponding column:

assets	sorted according the 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)

33.1 Residual values



Now there are several tabs:

- one for the potential values (without safeguards)
- one per project phase
- one to show impact evolution (along project phases)
- one to show risk evolution (along project phases)

In any presentation, you may select one or more rows, then click **MANAGE**. PILAR will drive you into the screen to “[evaluate safeguards](#)” so you can study which safeguards have an effect on the selected row(s). The recommendation levels will be recalculated to focus on the assets, threats, and dimensions covered by the selected row(s).

34 Deflected impact and risk tables

[[rt_ir_dt = deflected impact and risk tables]]



Collects the details of the impact and risk analysis, when done on deflected values.

Columns:

column		
1	father	the asset above: the harm is caused because it depends on the asset below
2	dimension	the dimension of security that suffers the consequences on the father
3	child	the asset subject to the threat
4	dimension	the dimension of security damaged by the threat, on the child
5	threat	the threat
6	V	the value of the asset (by itself)
7	D	the degradation of the value of the asset
8	I	the impact of the threat on the value of the asset
9	F	the likelihood of the threat
10	risk	the risk of the threat on the asset

Bottom tool bar:

asset	click to select a subset of assets to show
on / off	to apply (or not) the filter of assets to show
threat	click to select a subset of threats to show
on / off	to apply (or not) the filter of threats
dimension	click to select a subset of dimensions to show
on / off	to apply (or not) the filter of dimensions
legend	shows the code of colours
csv	exports shown data to a CSV file
xml	exports to xml file
db	(if database enabled) exports to database

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

Click on any header to sort by the corresponding column:

assets	sorted according the 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)

34.1 Residual values



Now there are several tabs:

- one for the potential values (without safeguards)
- one per project phase
- one to show impact evolution (along project phases)
- one to show risk evolution (along project phases)

In any presentation, you may select one or more rows, then click **MANAGE**. PILAR will drive you into the screen to “[evaluate safeguards](#)” so you can study which safeguards have an effect on the selected row(s). The recommendation levels will be recalculated to focus on the assets, threats, and dimensions covered by the selected row(s).

35 Textual reports

Basic **Standard**

Pilar generated 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.

- 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.

Threat report (not in Pilar Basic)

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

Safeguard evaluation

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

Defects report (not in Pilar Basic)

Similar to the “safeguard evaluation” 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.

Security procedures (not in Pilar Basic)

The report shows the maturity of security procedures phase by phase.

Business impact analysis (not in Pilar Basic)

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

Risk position

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

Security profile (not in Pilar Basic)

The reports the evaluation of the controls of specific security profiles.

35.1 Report templates

[[report_templates = reports by template]]

Basic **Standard**

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. PILAR passes unmodified most of the template files, but when it finds a hook, it is replaced by contents from the risk model. Hooks are small scripts written in XML, such as

```
<pilar> script to be interpreted </pilar>
```

The hook is replaced by the outcome of executing the contents.

The format of templates is described at

```
[[http://www.ar-tools.com/en/tools/pilar/doc.htm]]
```

36 Graphical reports

[[reports_gif = graphical reports]]



36.1 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

36.2 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

36.3 Safeguards / aspect

Overall valuation of safeguards by aspect of security.

- select one or more planes 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

36.4 Safeguards / strategy

Overall valuation of safeguards by strategy.

- select one or more planes 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

36.5 Safeguards / type of protection

Overall valuation of safeguards by type of operation.

- select one or more planes 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

36.6 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 CLEAR to clear the selection
 - click on top-button ALL to select all the assets
 - click on top-button DOMAIN 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

36.7 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

36.8 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 CLEAR to clear the selection
 - click on top-button ALL to select all the assets
 - click on top-button DOMAIN 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

36.9 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

36.10 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

36.11 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 CLEAR to clear the selection
 - click on top-button ALL to select all the assets
 - click on top-button DOMAIN 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

36.12 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 CLEAR to clear the selection
- click on top-button ALL to select all the assets
- click on top-button DOMAIN 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

36.13 Pareto

- 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. This graph is only available in quantitative analysis.

37 Security profiles

[[evl = security profiles]]



We may see the security position of the system from the point of view of a given security profile.

There are as many tabs as security domains.

This is a [partial] presentation of the evaluated safeguards, and a summary of the coverage of security objectives or controls in the selected profile.

selection	to select a few rows
recommendation	recommendation level
traffic lights	Estimation of the control / question / safeguard on the reference phase. To select the reference phase, click on the phase column header.
tree	controls in the profile + explicit questions + references to the safeguards in PILAR
doubts	to mark lines that further investigation or discussion; click to change
source	associated sources; click to change
applies	yes / no – as the user decides. Be ready to explain to inspectors.
comment	documentation purposes, in particular whether any controls are excluded (n.a.), you must document the reasons that lead to exclusion often make comments on implementation plans or describe the current situation click to change
assessment	as many columns as phases, collecting the values at each stage

Control values are derived from “coverage percentage”, that is calculated as the average value of the corresponding safeguards, using the standard effective values for maturity levels.

Top tool menus

Edit menu		
find	Ctrl-F	to find a text in the tree of controls
Export menu		
to csv		exports selected or visible controls to an external file using CSV format
to xml		exports selected or visible controls to an external file using XML format
report		exports to RTF or HTML
SoA		exports applicability statements, altogether with comments

Import menu	
from csv	reads an external CSV file
from xml	reads an external XML file
Select menu	
0, 1, 2, ...	selects the elements of the tree at that depth level
graph	select from the available graphs

To input the effectiveness of a safeguard in a phase

Clicking the mouse will open a menu to select out of the possible values.

When establishing a value for a safeguard that is a group, the value is copied into every child.

When a value is known for a phase, the same value will be used by the phases after, until a new value is written.

38 Interruption steps (BCM)

[[bcm_1 = interruption steps]]



To establish a scale of relevant points in time where valuation of consequences makes a difference.

See [[<http://www.ar-tools.com/en/glossary/index.html>]]: interruption steps.

To select a standard scale

- select STANDARD

There is no absolute rule for every situation, but some scales are rather frequent:

- a linear scale over days
1d, 2d, 3d,..., 10d
- a logarithmic scale over a wide spectrum
15s, 1m, 30m, 1h, 6h, 12h, 24h, 2d, 7d, 30d

To add steps

- click ADD and write the value of the interval.
The steps are always sorted by time.

To remove steps

- select one or more steps and click DELETE STEP.

To hide a step in the presentation screens

- select one or more lines, then click OFF

To show a step in the presentation screens

- select one or more lines, then click ON

38.1 Format to describe down time

Internally, PILAR deals with seconds, only; but makes an effort to read and write more friendly figures:

...	seconds
...s	seconds
...m	minutes
...h	hours
...d	days

Any combination is allowed. For instance

3d207m1

stands for 3 days + 207 minutes + 1 second.

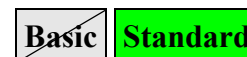
Let's show some normal examples:

15s	15 seconds
------------	------------

1m30s	1 minute + 30 seconds
90s	1 minute + 30 seconds
2h	2 hours
2h30m	2 hours + 30 minutes

39 Domain valuation (BCM)

[[bcm_dv = domain valuation]]



This is a quick way to value the information system.

It may be selected as an option

[Edit / Options / valuation of domains / ...](#)

It is a “quick & dirty” valuation of all the assets in the domain, faster than “valuation by dependencies”. Using this method, every asset in the security domain receives the same values.

The value of the information system is established for domains. The valuation is imposed by essential assets (information and services) and it is transferred to every other asset in the hosting domain and in associated domains.

Quick start

Which is the interruption step that makes a difference in consequences?

Let it be [1d] (for one day);

- go to the cell under [1d] heading, and
- double click to select a value from 0 (negligible) and 10 (absolutely critical) ... or somewhere in between.

Repeat with other interruption steps until the rest is not so important.

The screen shows as many columns as interruption steps.

The rows are split into two blocks, one zone for essential assets, and one zone for security domains. You introduce the value for the essential assets, and PILAR translates them onto the associated domains.

Double click on the selected cell to evaluate one essential asset in one step column.

Valuation of the security domains

Each domain inherits the valuation of assets and main contents of the associated with it.

To associate an asset to a domain

- select one asset
- select one domain
- click ASSOCIATE

To disassociate an asset for a domain

- select one asset
- select one domain
- click DISSOCIATE

40 Asset valuation (BCM)

[[bcm_av = asset valuation]]



Quick start

Which is your major concern with this information system?

- Select an asset (row) in the business (up most) layer,
- select the interruption step that makes a major difference in consequences (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 an incident escalation figure that makes sense to you.

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

Left column covers data (organised in layers and groups). It may be expanded and collapsed.

The other columns cover interruption steps. Only assets may receive values; the other rows are dead.

To assign value to an asset

- 1 select the asset (row) and step (column)
- 2 double click

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.

Checked criteria determine the qualitative level assigned to the asset in the stated step.

When done with the data ...

- click ACCEPT to save the new data
- click DO NOT VALUE to remove value from the asset
- click CANCEL to leave the asset as it was

Top menus:

Edit menu		
copy	ctrl.-C	saves the values of the selected cells
paste	ctrl-V	places the saved values onto the new selected area

Export menu	
to csv	generates a csv file with the shown values (for spreadsheets)
to xml	generates an xml file with the valuation

Import menu	
from xml	reads the valuation from an xml file

Bottom menus

only layers	the tree of assets is collapsed into level 1
- (minus)	decrement tree expansion by one
value	set tree expansion level
+ (plus)	increment tree expansion by one
copy	copies valuations into the pad
paste	pastes valuations from the pad
own / accumulated	switches between values to be presented: own – only values with an explicit assignment accumulated – values with own value show on white background, while accumulated value is shown on colour background

Notice that accumulation is done in two dimensions:

- first: left to right – so the consequences remain until next step with a higher value
- second: top down – so the consequences of an incident on one asset below, are those of the assets above it

41 Valuation of threats (BCM)

[[bcm_tv = threat valuation]]



Quick start

Select **ASSETS** on the first column (top).
 Click **LIBRARY** (bottom middle).
 Click **OK** to continue.

After determining which threats are relevant to each asset, let's introduce the vulnerability of the asset.

column		
1	selection	select a few assets /threats to apply an action <ul style="list-style-type: none"> • click to check / uncheck • SHIFT + click to check / uncheck a range • click on header to uncheck everything
2	tree of assets + threats	double click to expand / collapse
3	likelihood	use the buttons to select a value or input a likelihood estimate
4	step	introduce the estimated time to be back to normal operation after the threat occurs
...	graph	it presents a graphical presentation of the step in column 4

Top menus:

Edit menu		
options		Sets the preferred format for likelihood and degradation
copy	ctrl.-C	saves the values of the selected cells
paste	ctrl-V	places the saved values onto the new selected area

Export menu	
to csv	generates a csv file with the shown values (for spreadsheets)
to xml	generates an xml file with the valuation

Import menu	
from xml	reads the valuation from an xml file

Bottom tool bar:

- (minus)	decrements the expansion level of the assets tree
number	sets the expansion level of the assets tree
+ (plus)	increments the expansion level of the assets tree
+1	shows one level more: threats per asset
copy	takes not of the selected values
paste	applies copied values to a new location
load	loads a TSV file: a threat profile
library TSV	applies the current TSV; the button shows either a loaded TSV, or “library” to refer to the standard one
undo	reverses the last assignment of values to threats
redo	reapplies the last assignment undone
clear	removes values from selected rows

42 Evaluation of backup equipment (BCM)

[[bcm_bv = evaluation of backup equipment]]



Alternative equipment may be ready to replace damaged equipment. By providing quick repair, the impact is limited to acceptable levels.

You specify the replacement time per phase:

- if a phase has no data, it uses the value from the previous phase.
- If no phase has any value, it means there is no replacement equipment.

To set a time,

- select the asset (row) and phase (columns)
- and click on the right button of the mouse.

In the data input screen you may state

- the guaranteed replacement time;
(see the [notation to describe interruption steps](#))
- the maturity of the process to put the backup equipment into place
- add an optional comment explaining why
- select one [or more] means of providing backup, so it is clear how

To close the screen:

- click APPLY to accept the new data
- click NO BACKUP to remove data from the asset
- click DO NOT MODIFY to leave previous data

43 Impact & Risk: Accumulated values (BCM)

[[bcm_ir_a = accumulated values]]



There are as many tabs as phases plus one. The first tab shows the potential values (the values if no backup and no safeguard would be in place).

You may select (on the first column) one or more rows:

- click on the check box to select / deselect the row
- click on one check box, then SHIFT + click on another check box to repeat the selection of the first box over the range to the second box
- select a domain (bottom tool bar) to select all the assets in that domain
- select a source of information (bottom tool bar) to select all the assets referenced to that source

Selections are cumulative. Click on the selection column header to clean the selection.

2nd column shows assets and threats. The other columns show:

- either the consequences of a threat on an asset
- or the accumulated value on one asset, taking into account all the threats on it

column	
select	current selection
asset / threat	assets and threats on them
F	threat likelihood
S	interruption step
impact	impact corresponding to the interruption step
risk	impact merged with likelihood

For each row, the potential value (in base tab) or its residual value in each phase.

If you are treating risk ...

In any presentation, you may select one or more rows, then click **MANAGE**. PILAR will drive you into the screen to “[evaluate safeguards](#)” so you can study which safeguards have an effect on the selected row(s). The recommendation levels will be recalculated to focus on the assets, threats, and dimensions covered by the selected row(s).

44 Impact & Risk: Deflected values (BCM)

[[bcm_ir_d = deflected values]]



There are as many tabs as phases plus one. The first tab shows the potential values (the values if no backup and no safeguard would be in place).

You may select (on the first column) one or more rows:

- click on the check box to select / deselect the row
- click on one check box, then SHIFT + click on another check box to repeat the selection of the first box over the range to the second box
- select a domain (bottom tool bar) to select all the assets in that domain
- select a source of information (bottom tool bar) to select all the assets referenced to that source

Selections are cumulative. Click on the selection column header to clean the selection.

2nd column shows assets and threats:

- father asset: indirectly harmed
- son asset: on which the threats harms directly threat

The other columns show

- either the impact or the risk of a threat on an asset
- or the contribution of a son to the total harm on the father
- or the deflected harm on one father asset, taking into account all the threats on it

column	
select	current selection
asset / threat	assets and threats on them
F	threat likelihood
S	interruption step
impact	impact corresponding to the interruption step
risk	impact merged with likelihood

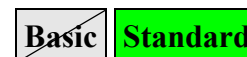
For each value, its potential (in base tab) or its residual value in each phase.

If you are treating risk ...

In any presentation, you may select one or more rows, then click **MANAGE**. PILAR will drive you into the screen “evaluation of safeguards so you can study which safeguards have an effect on the selected row(s). The recommendation levels will be recalculated to focus on the assets, threats, and dimensions covered by the selected row(s).

45 DRP - Disaster recovery plan(s) (BCM)

[[bcm_drp = disaster recovery plan]]



After a serious incident, you may need to rebuild the system.

This screen helps to design a recovery plan.

In a complex system, many plans may be needed:

- depending on which assets are lost
- depending on which services need urgent reconstruction
- depending on the current needs: e.g. end of paying period
- ...

Disaster recovery plans are not saved with the model. The user rather saves and restores them in separate files.

To load a [previous] recovery plan

- Click on LOAD and select a file with extension .DRP.

To save a recovery plan

- Click SAVE and select a file with extension .DRP.

To generate a recovery report

- Click REPORT and select a file for the report

To export data to a CSV file (Comma Separated Values)

- Click EXPORT and select a file for the report

Usage of the screen

First row show impact evolution if nothing is done.

Second row shows the residual impact if the plan below applies, and we are restoring assets step by step. If the analysis is quantitative, this second line adds as well the cost of the recovery actions (see second column below); so we have the actual net cost of the incident:

row 2 = residual impact + recovery cost

This screen does not take safeguards into consideration. It only analysis the case when everything works according to plan, giving the outcome of the plan.

First column shows the map of assets organised in layers.

Second column:

- if the analysis is qualitative:
the user may introduce a comment describing how the asset is recovered.
- if the analysis is quantitative:
the user may introduce a comment describing how the asset is recovered, and also the cost of this recovery action.

The other columns allow preparing a plan.

Click with the mouse button a box; it becomes a TARGET

- in order to reach that target, a number of assets below are REQUIRED: those the target asset depends on, either directly or indirectly; each one of the marked asset needs to be in place to reach the target objective.
- as a nice side effect, other assets may become ENABLED; that is, all they need below is available, and the asset may be itself recovered.
- that's all.

It is usual to start with ambitious targets (end services) that may require a lot of other assets. If possible, go ahead; but if it looks like too coarse for a realistic plan, the user may search for intermediate steps to recover assets below, so we get a phase plan to recover the end services.

In order to establish a recovery plan, never forget to take into considerations other aspects:

- what the management thinks about
- what the users think about
- the information system recovery needs to be aligned with other contingency planning in the organization
- other organizations may be involved: providers

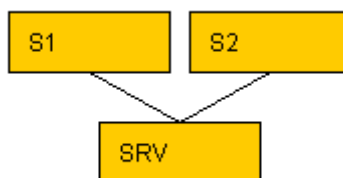
45.1 The meaning of ENABLED assets



TARGET assets are user objectives. REQUIRED assets are the assets below traversing the dependency graph.

ENABLED assets are those assets for which every other asset below is either TARGET or REQUIRED.

An example may help to see it. Let us have two services that depend on a shared server:



These are the consequences of selecting each asset as a target:

ASSETS		
🔍 [capa]		
🔗 [S1] servicio #1		target
🔗 [S2] servicio #2		enabled
🔗 [SRV] servidor compartido		required

ASSETS		
🔍 [capa]		
🔗 [S1] servicio #1		enabled
🔗 [S2] servicio #2		target
🔗 [SRV] servidor compartido		required

ASSETS		
  [capa]		
└─  [S1] servicio #1		enabled
└─  [S2] servicio #2		enabled
└─  [SRV] servidor compartido		target

46 Projects in XML

[[xml_format = XML format]]

Basic

Standard

PILAR may import / export projects using XML. The format is rather flexible, covering the following aspects:

assets

New assets are put in a new layer; the user is expected to move them to the corresponding layer.

Since there cannot be two assets sharing the same code, a new unique code is generated if there is a collision.

dependencies

Dependencies may refer to new assets (just imported) or to those already existing in the model.

If codes collide, the assets in the xml file are preferred.

valuation

Values may refer to new assets (just imported) or to those already existing in the model.

If codes collide, the assets in the xml file are preferred.

46.1 format (import and export)

Basic

Standard

```
file ::=
  <model [ code="..." ] >
    { data }0+
    [ sources ]
    [ domains ]
    { asset }0+
    { depend }0+
    { value }0+
  </model>

data ::=
  <data key="..." text="..." />

sources ::=
  <sources>
    { source }0+
  </sources>

source ::=
  <source c="...">
    name
```

```

    [ <desc> description </desc> ]
  </source>

domains ::=
  <domains>
    { domain }0+
  </domains>

domain ::=
  <domain c="..." [ next="..." ]>
    <name> name </name>
    [ <desc> description </desc> ]
  </domain>

asset ::=
  <asset c="..." domain="...">
    name
    { asset_source }0+
    { type }0+
    { data }0+
    [ <note> description </note> ]
  </asset>

asset_source ::=
  <source c="..." />

type ::=
  <type c="..." />

depend ::=
  <depend above="..." below="..." [ degree="..." ] />

value ::=
  general_value | availability_value

general_value ::=
  <value asset="..."
    dim="..."
    acronym="..."
    [ qualitative_value ]
    [ quantitative_value ]
  />

availability_value ::=
  <value asset="..."
    step="..."
    [ qualitative_value ]
    [ quantitative_value ]
  />

qualitative_value ::=

```

```
vl="..."  
quantitative_value ::=  
  vn="..."
```

46.2 XML Schema Definition (W3C Schema)

The schema may be found at

[\[\[http://www.ar-tools.com/en/tools/pilar/doc.htm\]\]](http://www.ar-tools.com/en/tools/pilar/doc.htm)