

***pilar***

---

# Tool Customization

José A. Mañas

**April 2023**  
**PILAR 2023.1**



- Configuration for the Analysis of Risk
- A text file you may edit to customize tool behavior

```
# Pilar configuration
tool= pilar
version= 2023.1

# localisation
locale= en_GB
# see http://java.sun.com/javase/6/docs/technotes/guides/intl/locale.doc.html
csv.separator= ,

# home is the directory of this file

# other components, relative to "home"
util= util

# tool configuration, under "home/util"
texts= common_en.txt

# licensee icon
licensee_icon=

# splash screen
splash=

# examples, relative to "home"
examples= exs

# libraries, relative to "home"
library= bib_en
info= info_en
```

customization

configuration  
files



# marking

---

- document classification

CIS\_en.car

marking= marking\_en.xml

```
<?xml version="1.0" encoding="UTF-8" ?>  
  
<marking>  
  <mark C="TS">TOP SECRET</mark>  
  <mark C="S">SECRET</mark>  
  <mark C="C">CONFIDENTIAL</mark>  
  <mark C="R">RESTRICTED</mark>  
  <mark C="UC">UNCLASSIFIED</mark>  
</marking>
```



- information items
  - administrative data for projects
  - administrative data for assets
  - standard layers
  - standard information sources

CIS\_en.car

info= info\_en

customization

```
<assets>
  <layer c="B">Essential assets</layer>
  <layer c="IS">Internal services</layer>
  <layer c="E">Equipment
    <group c="SW">Applications</group>
    <group c="HW">Hardware</group>
    <group c="COM">Communications</group>
    <group c="AUX">Other elements</group>
  </layer>
  <layer c="SS">Subcontracted services</layer>
  <layer c="L">Facilities</layer>
  <layer c="P">Personnel</layer>
</assets>
```



- valuation criteria
  - criteria → qualitative levels
  - it is very convenient to have a short list aligned with organization

## CIS\_en.car

```
criteria= criteria_en.xml  
extensions= ext_criteria_pi_en.xml
```

```
<?xml version="1.0" encoding="UTF-8" ?>  
<criteria lang="en">  
  <criterion>  
    [pi] Personal Information:  
    <criterion>  
      [classic] Classic  
      <criterion value="6">  
        [6.pi1] is likely to cause significant distress to a gro  
      </criterion>  
      <criterion value="6">  
        [6.pi2] is likely to cause a significant breach of a leg  
      </criterion>  
      <criterion value="5">  
        [5.pi1] is likely to cause significant distress to an in  
      </criterion>  
    </criterion>  
  </criterion>  
</criteria>
```



# new asset classes

---

## CIS\_en.car

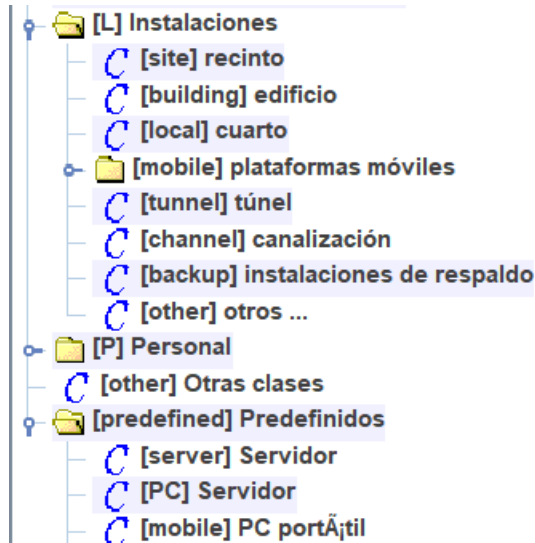
```
extensions= ext_domain-classes_en.xml  
extensions= ext_classes_pi_en.xml  
extensions= ext_classes_ics_en.xml
```

customization

```
<?xml version="1.0" encoding="UTF-8"?>  
<library-extension>  
  <classes under="essential.info.per">  
    <class code=".normal">normal personal data  
      <class code=".1">  
        identification data (name and surname, id, postal address  
, telephone, ...)  
      </class>  
      <class code=".2">  
        personal characteristics (civil status, date and place of  
birth, nationality, ...)  
      </class>  
      <class code=".3">academic data  
      </class>  
      <class code=".4">professional data  
      </class>  
      <class code=".5">bank data  
      </class>  
    </class>
```



# new asset classes



```
<?xml version="1.0" encoding="UTF-8" encoding="áéíóú" ?>
<library-extension>
<classes version="2">

  <class code="predefined">
    Predefinidos
    <class code="server">
      aggregate="D.files D.conf D.log
      S.prov.www S.prov.email
      SW.std.www SW.std.app SW.std.email_server SW.std.directory
      SW.std.file SW.std.os
      SW.sec.av
      HW.mid HW.data Media.electronic.disk">
      Servidor
    </class>

    <class code="PC">
      aggregate="D.files D.conf
      S.client.www S.client.email
      SW.std.browser SW.std.email_client SW.std.office
      SW.std.os
      SW.sec.av
      HW.pc HW.data Media.electronic.disk">
      Servidor
    </class>
```

customization



# new threats

- new threats

CIS\_en.car

extensions= ext\_threats\_en.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<library-extension>
  <threats under="N.*">
    <threat code="N.*.1">Storms</threat>
    <threat code="N.*.2">Thunderstorms and Lightning</threat>
    <threat code="N.*.3">Hurricanes</threat>
    <threat code="N.*.4">Earthquakes</threat>
    <threat code="N.*.5">Tornadoes</threat>
    <threat code="N.*.6">Cyclones</threat>
    <threat code="N.*.7">Landslide and mudslide</threat>
    <threat code="N.*.8">Meteorites</threat>
    <threat code="N.*.9">Tsunamis</threat>
    <threat code="N.*.10">Winter storms and extreme cold</threat>
    <threat code="N.*.11">Extreme heat</threat>
    <threat code="N.*.12">Volcanoes</threat>
  </threats>
</library-extension>
```





- threat standard values
  - assigns threats to asset classes
  - provides default values for likelihood and degradation

## CIS\_en.car

```
tsv= tsv_2018-07-05.xlsx  
tsv= ext_tsv_pi.xml
```

|    | A      | B      | C      | D      | E    | F                      | G                   | H                         | I                         | J                          | K                 |
|----|--------|--------|--------|--------|------|------------------------|---------------------|---------------------------|---------------------------|----------------------------|-------------------|
| 12 |        | D.conf | A.6    | 0      |      |                        |                     |                           |                           |                            |                   |
| 1  | app    | family | threat | likely | step | D=en:A<br>availability | D=en:I<br>integrity | D=en:C<br>confidentiality | D=en:Auth<br>authenticity | D=en:Acc<br>accountability | D=en:Val<br>value |
| 2  | no     |        |        |        |      |                        |                     |                           |                           |                            |                   |
| 3  | D      |        | E.15   | 1      |      |                        | 1%                  |                           |                           |                            |                   |
| 4  | D      |        | E.18   | 1      | 1d   | 1%                     |                     |                           |                           |                            |                   |
| 5  | D      |        | E.19   | 1      |      |                        |                     | 10%                       |                           |                            |                   |
| 6  | D      |        | A.5    | 10     |      |                        | 10%                 | 50%                       | 100%                      |                            |                   |
| 7  | D      |        | A.6    | 10     | 1d   | 1%                     | 10%                 | 50%                       |                           |                            |                   |
| 8  | D      |        | A.11   | 100    |      |                        | 10%                 | 50%                       |                           |                            |                   |
| 9  | D.conf |        | E.15   | 0      |      |                        |                     |                           |                           |                            |                   |
| 10 | D.conf |        | E.19   | 0      |      |                        |                     |                           |                           |                            |                   |
| 11 | D.conf |        | E.4    | 1      |      |                        | 1%                  |                           |                           |                            |                   |
| 12 | D.conf |        | A.6    | 0      |      |                        |                     |                           |                           |                            |                   |
| 13 | D.conf |        | A.11   | 0      |      |                        |                     |                           |                           |                            |                   |
| 14 | D.conf |        | A.4    | 10     | 1d   | 10%                    | 10%                 | 10%                       |                           |                            |                   |
| 15 | D.log  |        | E.19   | 0      |      |                        |                     |                           |                           |                            |                   |
| 16 | D.log  |        | E.3    | 1      |      |                        | 1%                  |                           |                           |                            |                   |
| 17 | D.log  |        | A.3    | 100    |      |                        | 50%                 |                           |                           |                            |                   |



- threat standard values
  - assigns threats to asset classes
  - provides default values for likelihood and degradation

## CIS\_en.car

```
tsh= tsh_2018-07-05.xlsh  
tsh= ext_tsh_pi.xml
```

customization

```
<?xml version="1.0" encoding="utf-8" ?>  
<threat-standard-values>  
  <family F="essential.info.per">  
    <threat Z="PR.2a" f="10.0"> <set D="en:PD" deg="0.50" /> </threat>  
    <threat Z="PR.2b" f="10.0"> <set D="en:PD" deg="0.10" /> </threat>  
    <threat Z="PR.2c" f="10.0"> <set D="en:PD" deg="0.20" /> </threat>  
    <threat Z="PR.2d" f="10.0"> <set D="en:PD" deg="0.90" /> </threat>  
    <threat Z="PR.2e" f="10.0"> <set D="en:PD" deg="0.50" /> </threat>  
    <threat Z="PR.2f" f="10.0"> <set D="en:PD" deg="0.50" /> </threat>  
    <threat Z="PR.2g" f="10.0"> <set D="en:PD" deg="0.50" /> </threat>  
    <threat Z="PR.2h" f="10.0"> <set D="en:PD" deg="1.00" /> </threat>  
    <threat Z="PR.2i" f="10.0"> <set D="en:PD" deg="1.00" /> </threat>  
    <threat Z="PR.2j" f="10.0"> <set D="en:PD" deg="0.90" /> </threat>  
    <threat Z="PR.2k" f="5.0"> <set D="en:PD" deg="0.50" /> </threat>  
    <threat Z="PR.2l" f="10.0" opt="yes"> <set D="en:PD" deg="0.30" /> </threat>  
    <threat Z="PR.2m" f="10.0"> <set D="en:PD" deg="0.30" /> </threat>  
    <threat Z="PR.2n" f="10.0"> <set D="en:PD" deg="0.80" /> </threat>
```



# attackers (tsv)

---

- attackers initiating attacks at zones (logical, physical, ...)

## CIS\_en.car

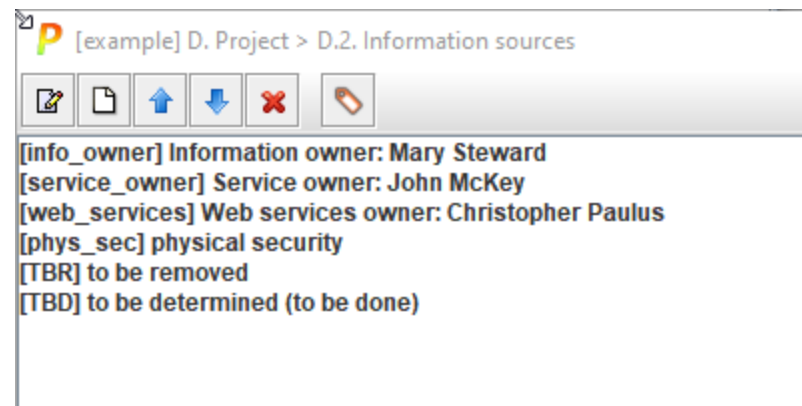
```
attacker= [EXT_L] External attackers (cyber)
tsv:EXT_L= tsv_log.xml, tsv_2018-07-05.xlsx

attacker= [EXT_P] External attackers (physical)
tsv:EXT_P= tsv_pps.xml, tsv_2018-07-05.xlsx
```



# information sources

- labels for assets, zones, safeguards, evl, ..., security domains, project phases, ..., reports



- for selecting, filtering, marking, and protecting



# sources: assets

**P** [example] A.1. Assets > A.1.1. identification > asset

**code**  
INFO

**name**  
Current files

**Information sources**  
info\_owner

**domain**  
[base] corporate network

**data**

**description**  
state of open files

**content**  
temporarily stores financial data of citizens

**owner**  
file processing chief

**ASSET CLASSES**

- ☐ [essential] Essential assets
  - ☒ [info] information
    - ☒ [adm] public administration data
  - ☐ [per] personal data
    - ☐ [regular] regular personal data
      - ☒ [1] economic
      - ☒ [5] location
  - ☒ [ppd] processing of personal data

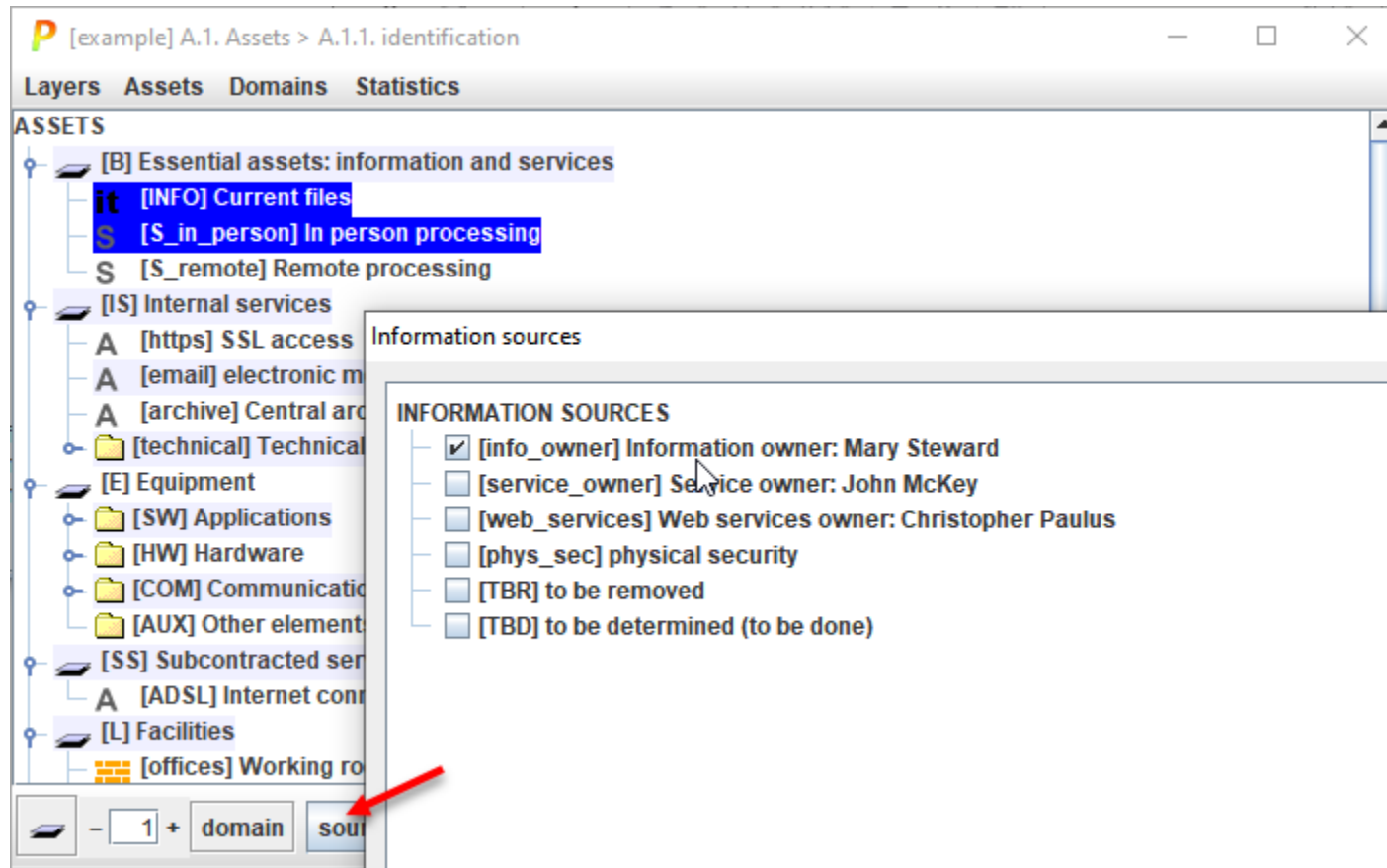
description GDPR

😊 ? ☹️



# sources: assets

- select (filter) by source





# sources: safeguards & controls

- filter by information sources

[example] S. Safeguards > S.2. valuation (phases)

Edit Expand View Export Import Statistics NATO

[base] corporate network phys\_sec, TBD

|                          | as... | top | re... | level | safeguard                                                | do... | so... | ap... | co... | cu... | tar... | Pl... |
|--------------------------|-------|-----|-------|-------|----------------------------------------------------------|-------|-------|-------|-------|-------|--------|-------|
| <input type="checkbox"/> |       |     |       |       | SAFEGUARDS                                               |       |       |       |       | L0... | L3...  | L2... |
| <input type="checkbox"/> | M     | PR  | 5     |       | ☿ [M] Protection of Media                                |       |       |       |       | L2    | L4     | L2... |
| <input type="checkbox"/> | M     | PR  | 5     |       | ☿ [M.2] Media management                                 |       |       |       |       | L2    | L4     | L2... |
| <input type="checkbox"/> | PHY   | EL  | 3     |       | ☿ [M.3] Connection of removable devices is under control |       | TBD   |       |       | L2    | L4     | L2... |
| <input type="checkbox"/> | M     | PR  | 5     |       | ☿ [AUX] Auxiliary Means                                  |       | ph... |       |       | L0... | L3...  | L2... |
| <input type="checkbox"/> | PHY   | PR  | 4     |       | ☿ [L] Protection of the installations                    |       | ph... | ...   |       | L0... | L3...  | L2... |

- 1 + sources

operation suggest

find >>

☺ ? ☹



# sources: reports

- filter by sources

Report data

**P**

Classification: RESTRICTED

Date: 09-Feb-2021

Assets: select

Sort: ☒ by layer ☐ by domain

Information sources: select

Security domains: select

Format: ☐ RTF ☒ HTML

ok cancel

Report data

**P**

Classification: RESTRICTED

Date: 09-Feb-2021

Assets: select

Sort: ☒ by layer ☐ by domain

Information sources: phys\_sec

Security domains: select

Format: ☐ RTF ☒ HTML

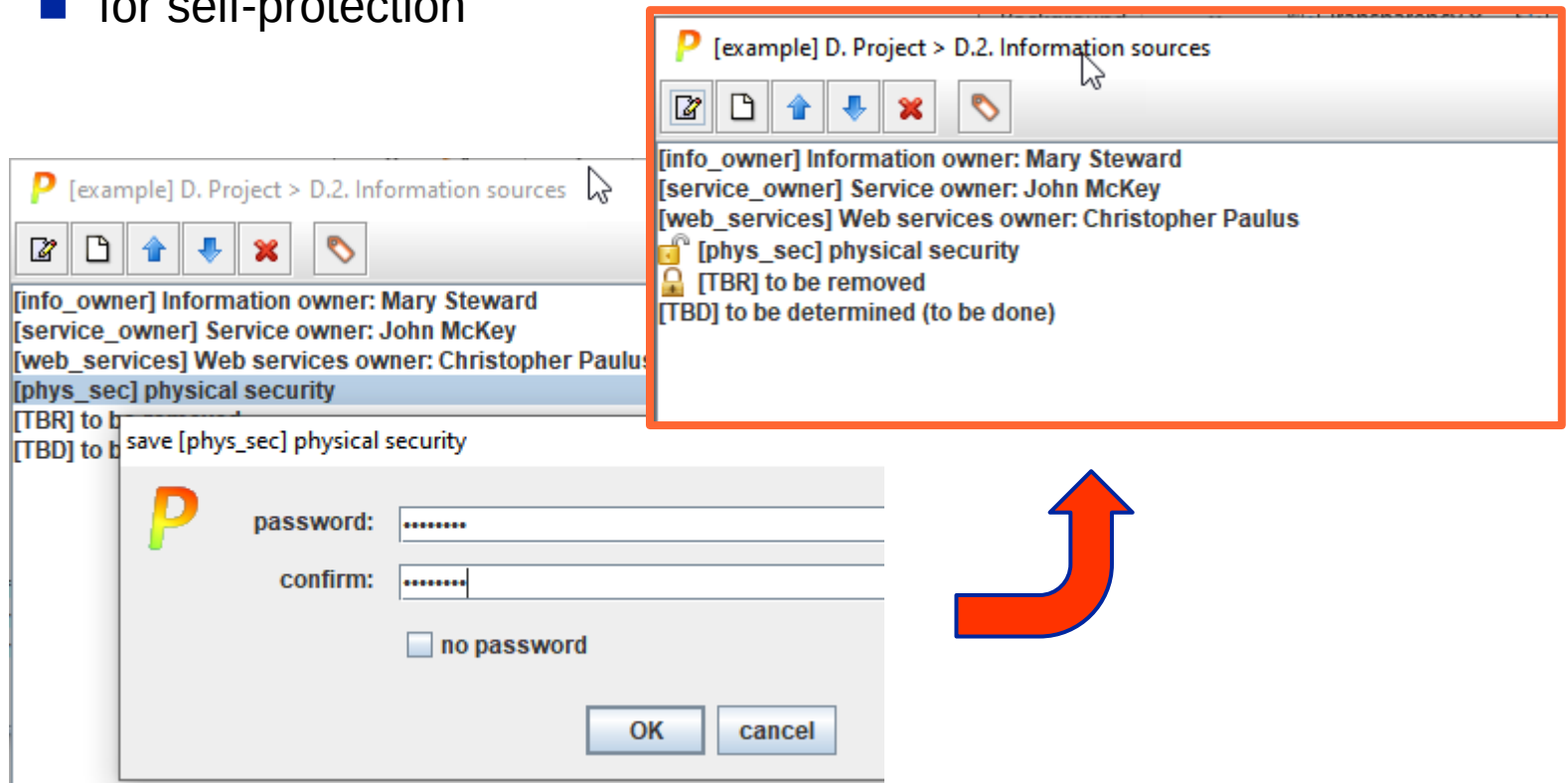
ok cancel





# sources with a password

- password → write protected
  - for shared access
  - for self-protection





# security profiles (evl)

---

- official collections of security measures

## CIS\_en.car

```
profile= 27002_2013_2016-06-16_en.evl  
# profile= 27002_2005_2014-04-01_en.evl  
# profile= sp800-53_rev3_2012-07-16_en.evl  
profile:en.PD= GDPR-2016_2020-10-15_en.evl  
profile:en.PD= 29151_A_2017_2017-08-30_en.evl
```



# ignore

- to hide
  - security dimensions
  - asset classes
  - threats
  - security measures

CIS\_en.car

ignore= ignored.xml

customization

```
<?xml version="1.0" encoding="UTF-8" ?>

<ignored-families>
  <accept F="essential.info.per" />
</ignored-families>

<ignored-controls evl="GDPR:2016">
  <ignore C="CC" />
</ignored-controls>

<ignored-dimensions>
  <accept D="en:A" />
  <accept D="en:I" />
  <accept D="en:C" />
  <accept D="en:Auth" />
  <accept D="en:Acc" />
  <accept D="en:V" />
  <accept D="en:PD" />
</ignored-dimensions>

<ignored-threats>
  <xignore F="" Z="" D="" />

  <accept Z="N.*" />
  <accept Z="N.1" />
  <accept Z="N.2" />
</ignored-threats>
```



# reports

- report templates

CIS\_en.car

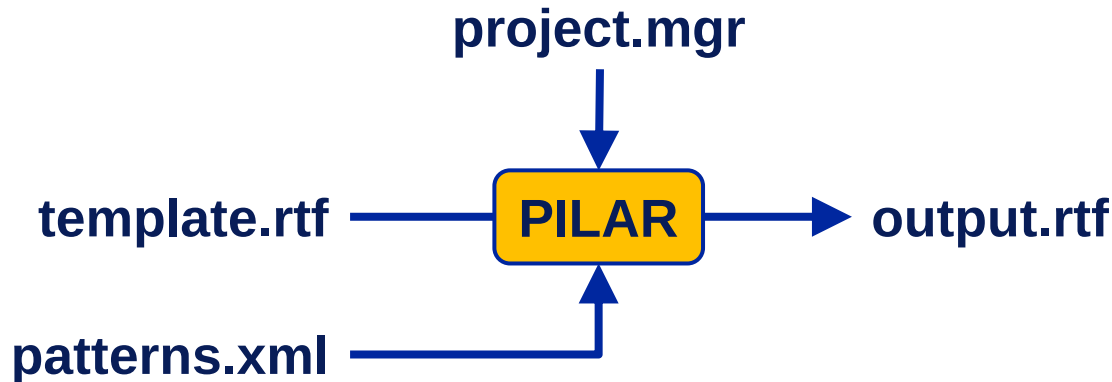
reports= reports.xml

customization

```
<?xml version="1.0" encoding="UTF-8" ?>
<reports>
  <template>
    <file>Risk_en_tpl.rtf</file>
    <name>Risk analysis</name>
  </template>
  <template>
    <file>SOA_27000_2013_en_tpl.rtf</file>
    <name>Statement of Applicability - ISO/IEC 27000 (2013)</name>
    <evl>27002:2013</evl>
  </template>
  <template>
    <file>Compliance_27000_2013_en_tpl.rtf</file>
    <name>Compliance ISO/IEC 27000 (2013)</name>
    <evl>27002:2013</evl>
  </template>
  <template>
    <file>Compliance_27000_2005_en_tpl.rtf</file>
    <name>Compliance ISO/IEC 27000 (2005)</name>
    <evl>27002:2005</evl>
  </template>
  <template>
    <file>Compliance_gdpr_en_tpl.rtf</file>
    <name>Compliance Regulation (UE) 2016/679</name>
    <evl>GDPR:2016</evl>
  </template>
  <template>
    <file>Compliance_29151_2017_en_tpl.rtf</file>
    <name>Compliance ISO/IEC 29151 (2017)</name>
    <evl>29151:2017</evl>
  </template>
</reports>
```



1. reports.xml → user interface
2. user selects a template and an output file



[https://www.pilar-tools.com/doc/ReportTemplates\\_74\\_en\\_e.pdf](https://www.pilar-tools.com/doc/ReportTemplates_74_en_e.pdf)



# hooks

- links safeguards and controls to external URL
- no reference in CAR file: just drop on library

```
$ ls -l bib_en/hooks-*  
bib_en/hooks-kaspersky.json  
bib_en/hooks-sp800-53.json
```

```
{  
  "encoding" : "áéíóú",  
  "title" : "SP 800-53 rev.5",  
  "defs" : [  
    {  
      "sm" : [ "ACb" ],  
      "links" : [  
        {  
          "label" : "ACCESS CONTROL",  
          "url" : "https://nvd.nist.gov/800-53/Rev4/family/ACCESS%20CONTROL"  
        }  
      ]  
    },  
    {  
      "sm" : [ "AC-1", "AC-1(0)" ],  
      "links" : [  
        {  
          "label" : "Policy and procedures",  
          "url" : "https://nvd.nist.gov/800-53/Rev4/control/AC-1"  
        }  
      ]  
    },  
    {  
      "sm" : [ "AC-2", "AC-2(0)" ],  
      "links" : [  
        {  
          "label" : "Policy and procedures",  
          "url" : "https://nvd.nist.gov/800-53/Rev4/control/AC-2"  
        }  
      ]  
    }  
  ]  
}
```

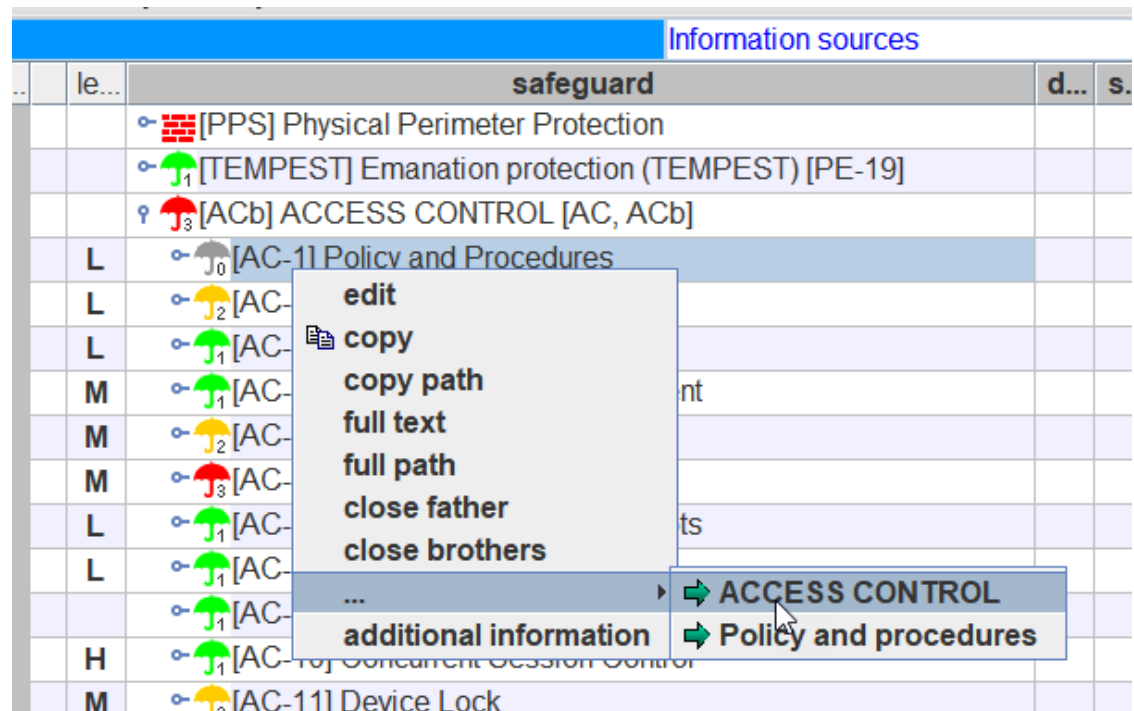
customization



# hooks

- links safeguards and controls to external URL
- no reference in CAR file: just drop on library

```
$ ls -l bib_en/hooks-*  
bib_en/hooks-kaspersky.json  
bib_en/hooks-sp800-53.json
```



customization



# any question?

---



[support@pilar-tools.com](mailto:support@pilar-tools.com)