pilar

since v.2021.1

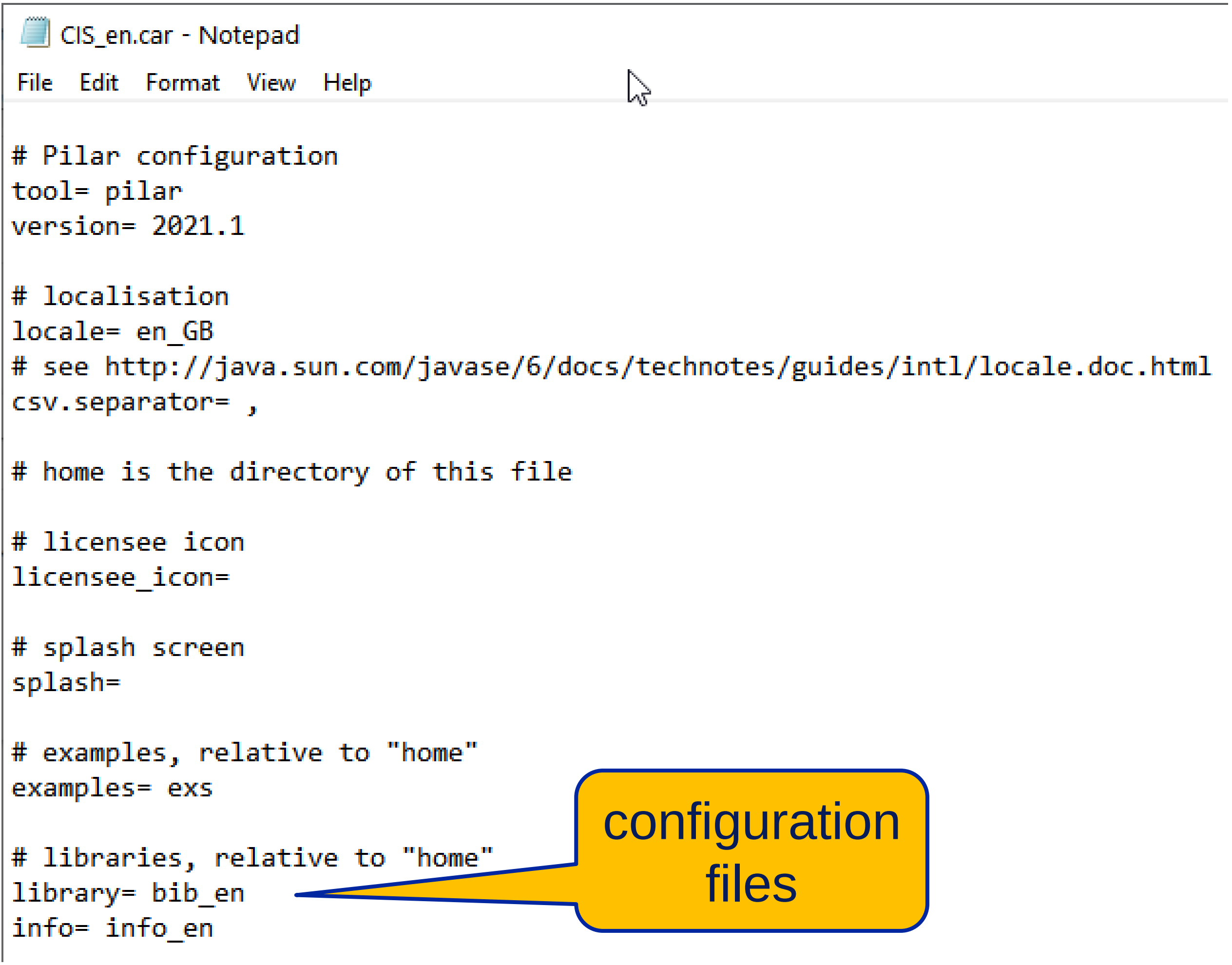
PILAR
Tool Customization

José A. Mañas <jmanas@pilar-tools.com>

April, 2021

CAR file

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



```
# Pilar configuration
tool= pilar
version= 2021.1

# 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

# licensee icon
licensee_icon=

# splash screen
splash=

# examples, relative to "home"
examples= exs

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

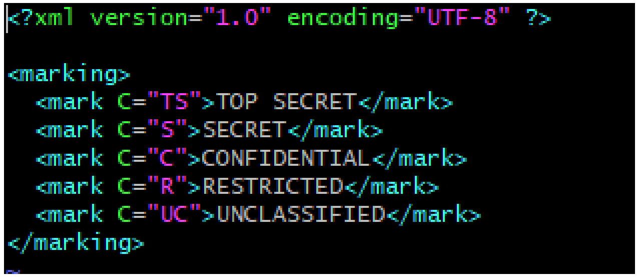
configuration files

marking

- document classification

CIS_en.car

```
marking= marking_en.xml
```



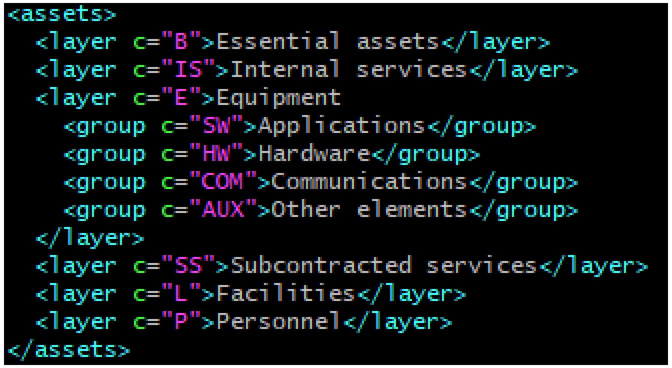
```
<?xml version="1.0" encoding="UTF-8" ?>

<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>
```

info

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

CIS_en.car

```
info= info_en
```



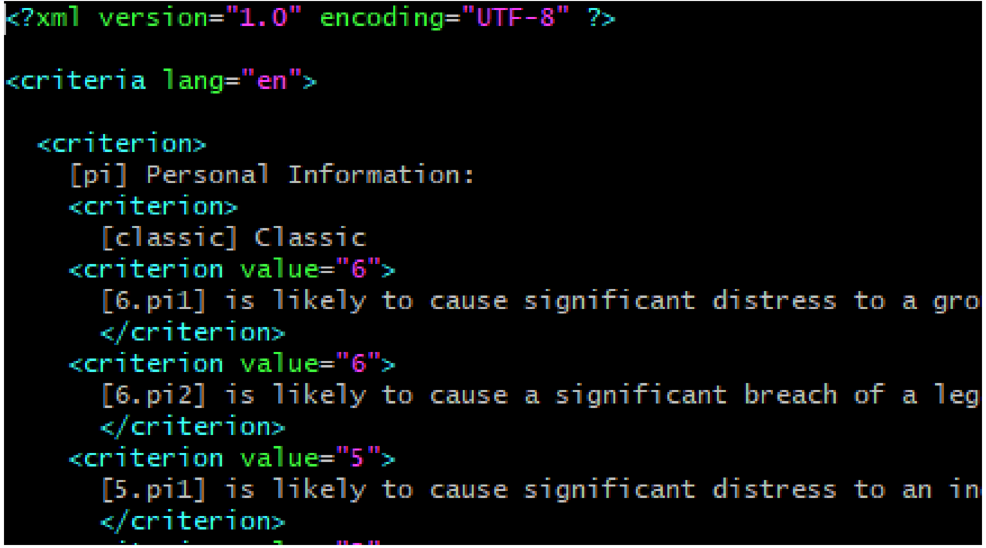
```
<assets>
  <layer c="B">Essential assets</layer>
  <layer c="IS">Internal services</layer>
  <layer c="E">Equipment
    <group c="SW">Applications</group>
    <group c="HW">Hardware</group>
    <group c="COM">Communications</group>
    <group c="AUX">Other elements</group>
  </layer>
  <layer c="SS">Subcontracted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

criteria

- 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
```



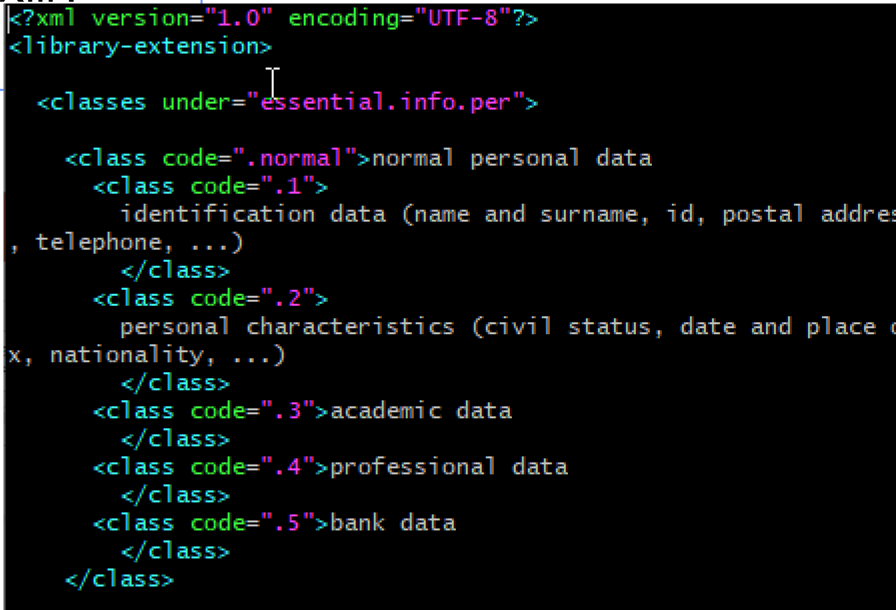
```
<?xml version="1.0" encoding="UTF-8" ?>

<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>
```

new asset classes

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

CIS_en.car

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



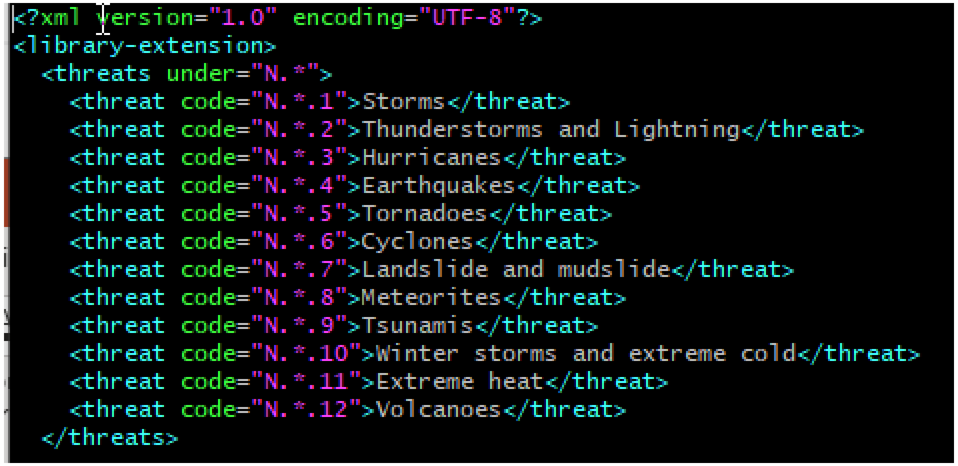
```
<?xml version="1.0" encoding="UTF-8"?>
<library-extension>

  <classes under="essential.info.per">

    <class code=".normal">normal personal data
      <class code=".1">
        identification data (name and surname, id, postal addre
, telephone, ...)
        </class>
      <class code=".2">
        personal characteristics (civil status, date and place o
x, nationality, ...)
        </class>
      <class code=".3">academic data
        </class>
      <class code=".4">professional data
        </class>
      <class code=".5">bank data
        </class>
    </class>
```

new threats

- new threats

CIS_en.car

```
extensions= ext_threats_en.xml
```



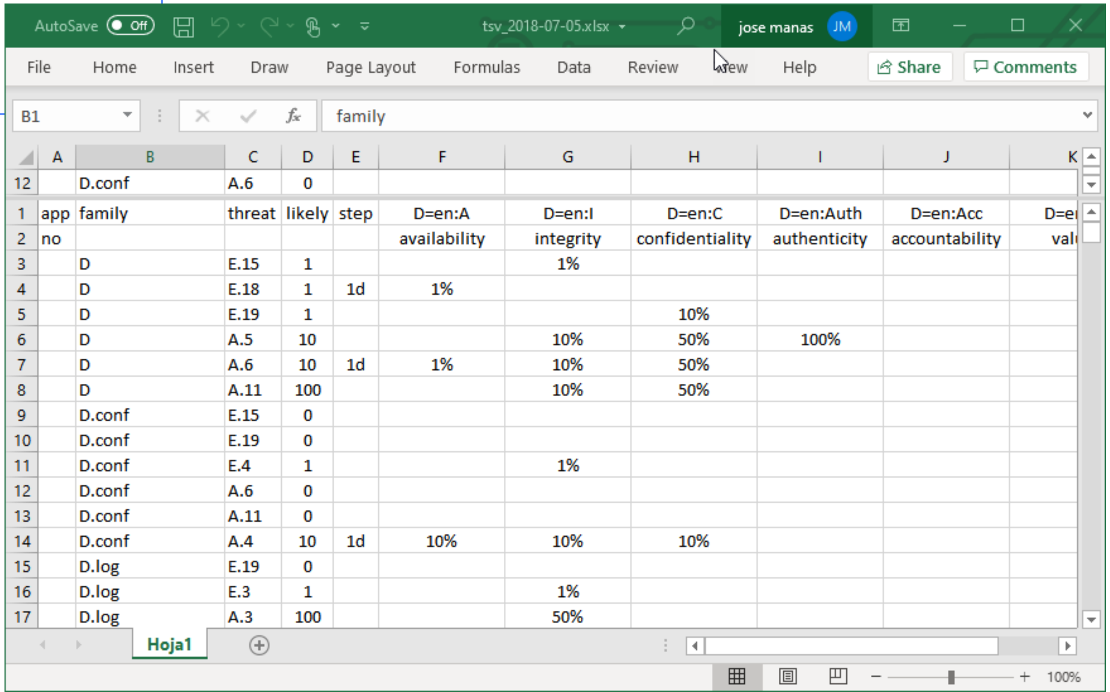
```
<?xml version="1.0" encoding="UTF-8"?>
<library-extension>
  <threats under="N.*">
    <threat code="N.*.1">Storms</threat>
    <threat code="N.*.2">Thunderstorms and Lightning</threat>
    <threat code="N.*.3">Hurricanes</threat>
    <threat code="N.*.4">Earthquakes</threat>
    <threat code="N.*.5">Tornadoes</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>
```

tsv

- 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
```



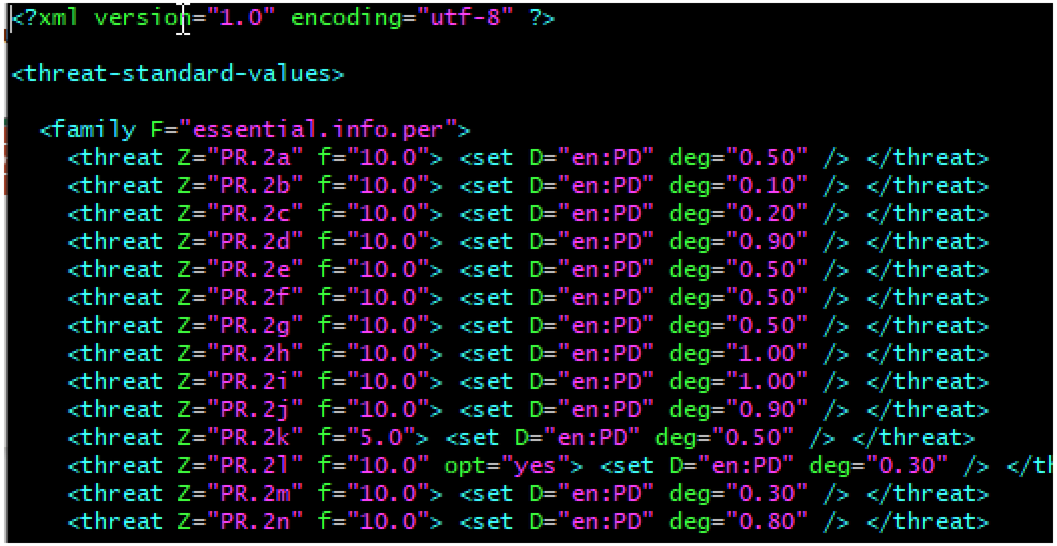
	A	B	C	D	E	F	G	H	I	J	K
12		D.conf	A.6	0							
1	app	family	threat	likely	step	D=en:A	D=en:I	D=en:C	D=en:Auth	D=en:Acc	D=e
2	no					availability	integrity	confidentiality	authenticity	accountability	val
3		D	E.15	1			1%				
4		D	E.18	1	1d	1%					
5		D	E.19	1				10%			
6		D	A.5	10			10%	50%	100%		
7		D	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%				

tsv

- 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
```



```
<?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" /> </th
    <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)

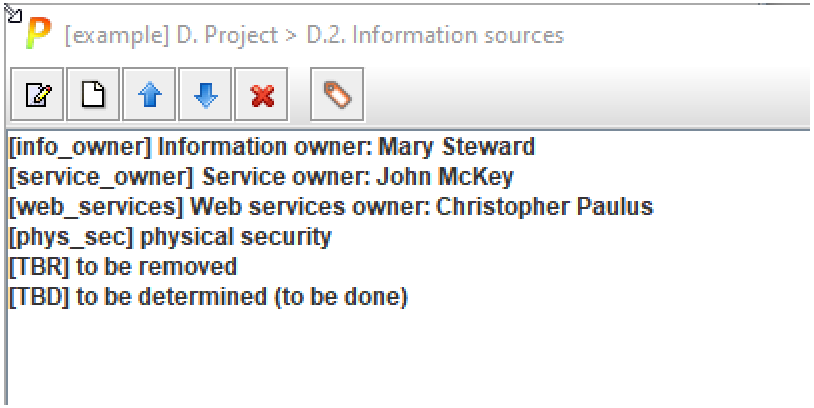
- attackers initiating attacks at zones (logical, physical, ...)

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

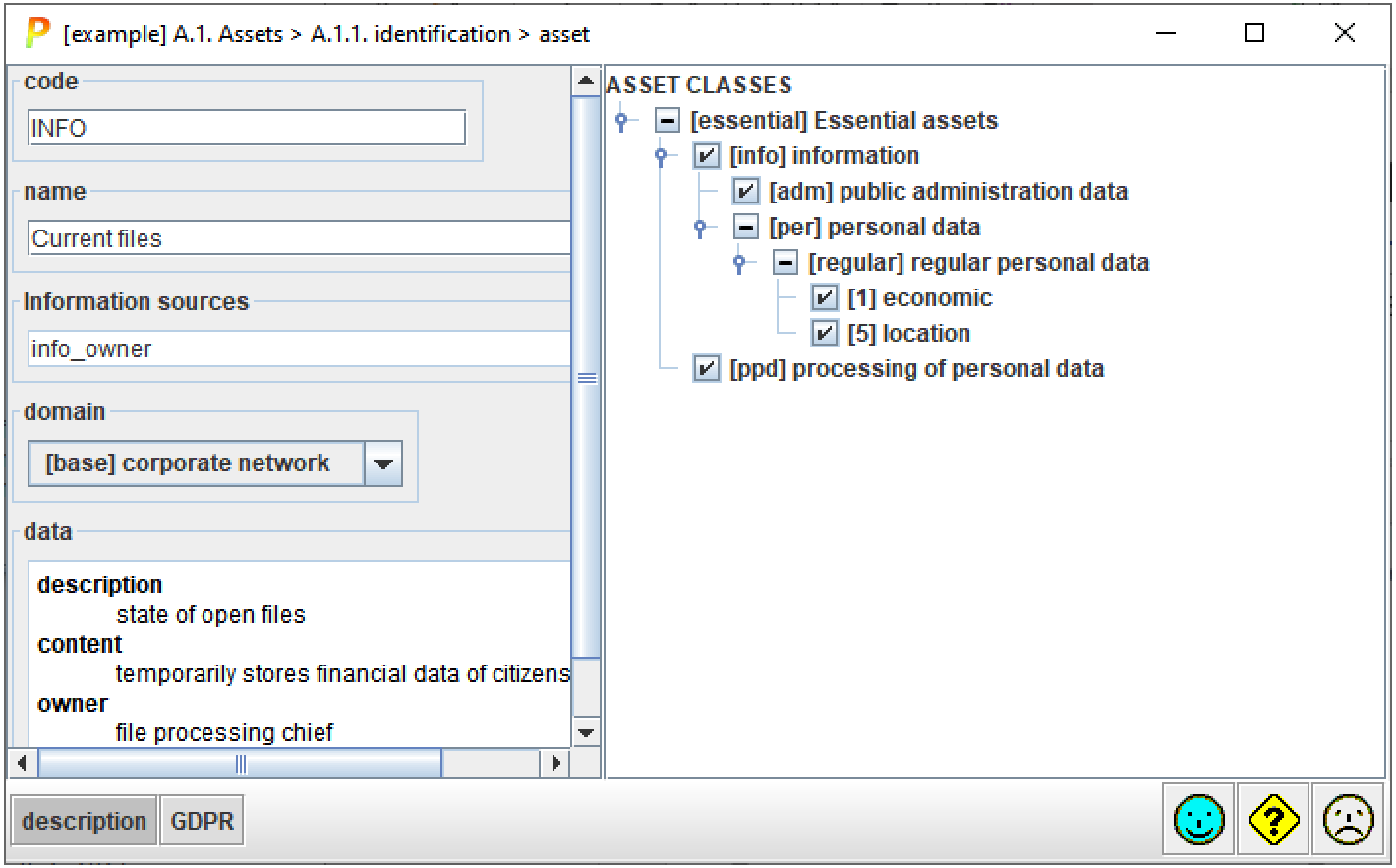
- labels for assets, zones, safeguards, evl, ..., security domains, project phases, ..., reports



[info_owner] Information owner: Mary Steward
[service_owner] Service owner: John McKey
[web_services] Web services owner: Christopher Paulus
[phys_sec] physical security
[TBR] to be removed
[TBD] to be determined (to be done)

- for selecting, filtering, marking, and protecting

sources: assets



[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

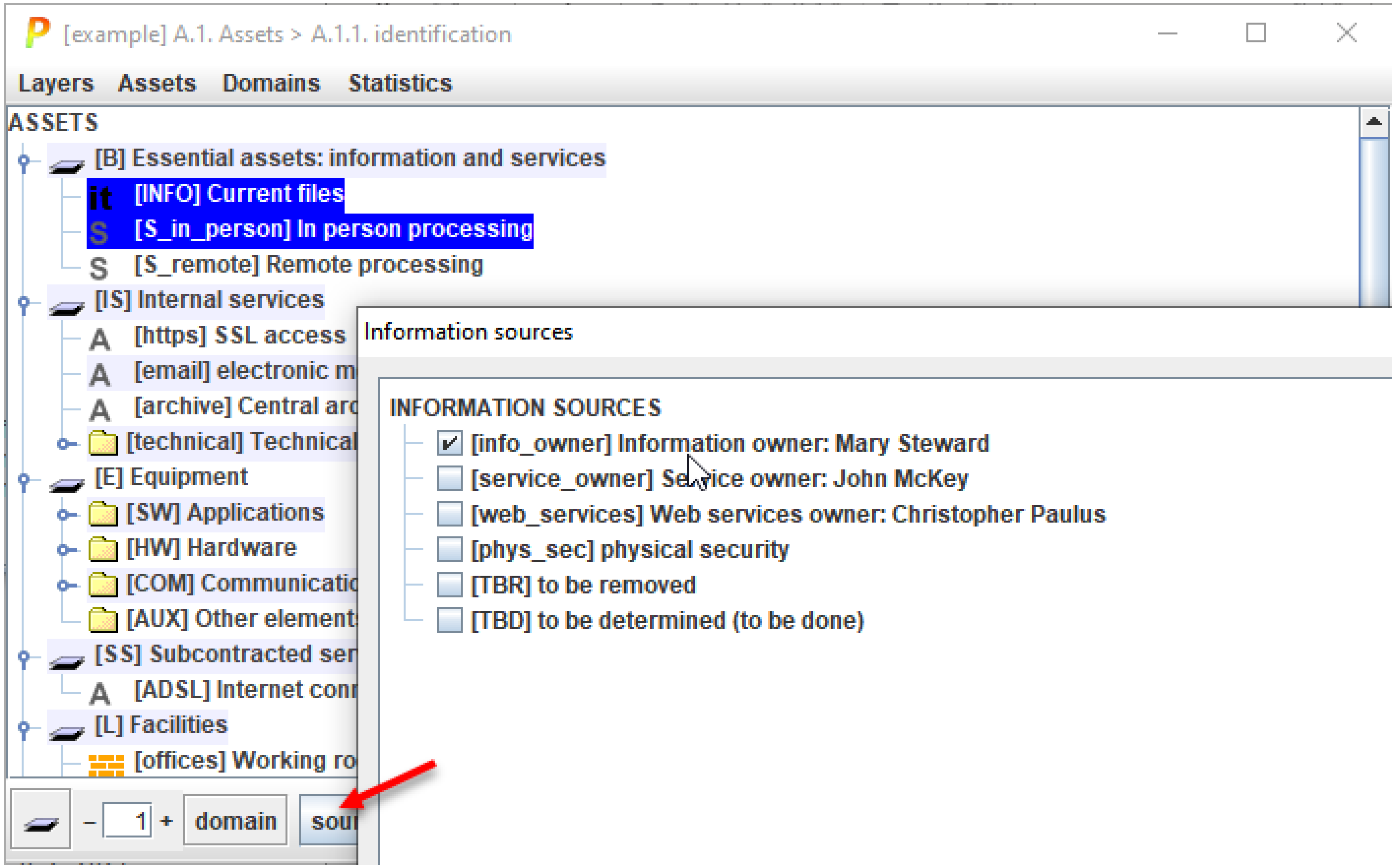
ASSET CLASSES

- [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

customization

sources: assets

- select (filter) by source



[example] A.1. Assets > A.1.1. identification

ASSETS

- [B] Essential assets: information and services
  - it [INFO] Current files
  - S [S_in_person] In person processing
  - S [S_remote] Remote processing
- [IS] Internal services
  - A [https] SSL access
  - A [email] electronic m
  - A [archive] Central arc
  - [technical] Technical
- [E] Equipment
  - [SW] Applications
  - [HW] Hardware
  - [COM] Communicatio
  - [AUX] Other element
- [SS] Subcontracted ser
  - A [ADSL] Internet conn
- [L] Facilities
  - [offices] Working ro

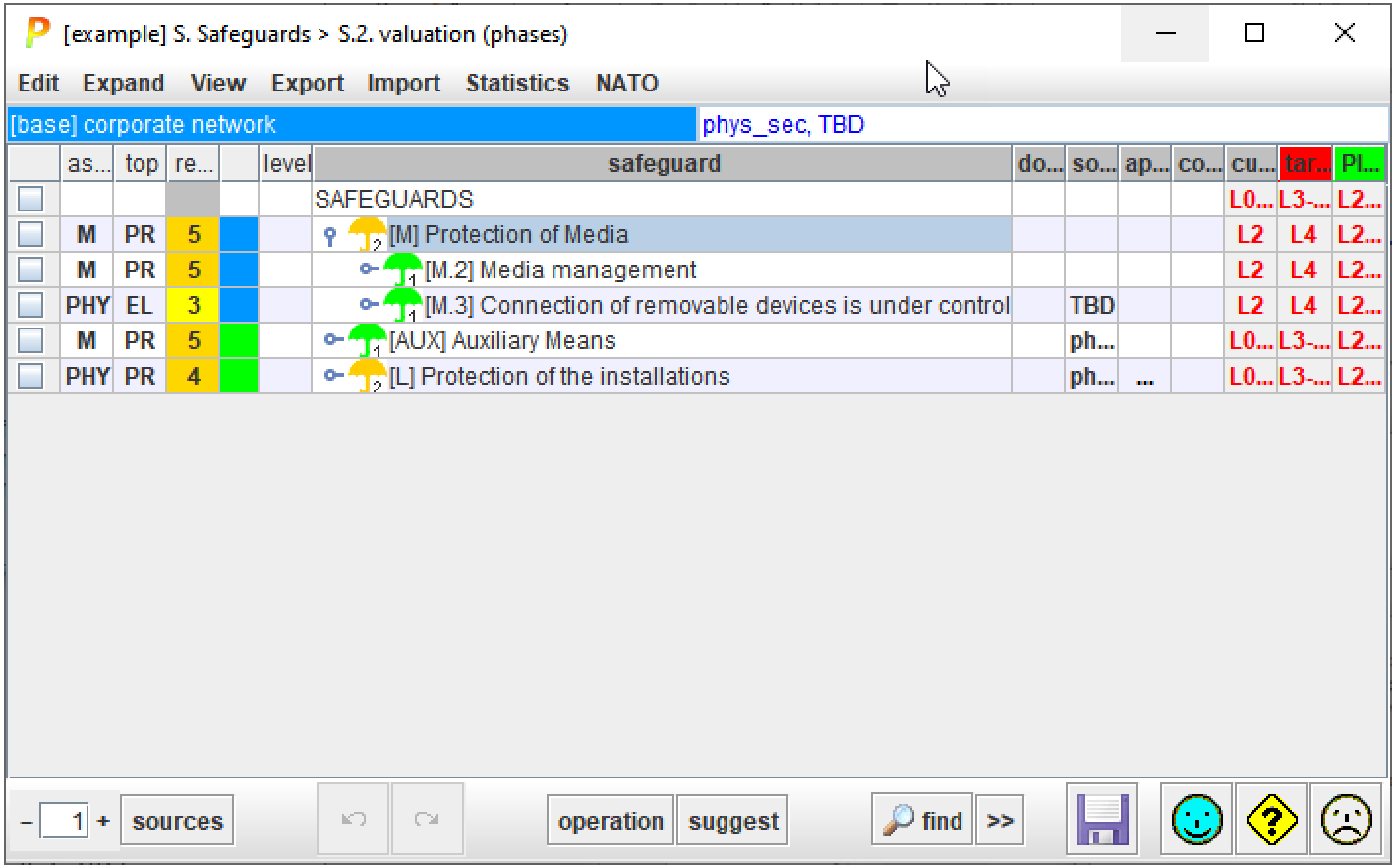
Information sources

INFORMATION SOURCES

- ☑ [info_owner] Information owner: Mary Steward
- □ [service_owner] Service owner: John McKey
- □ [web_services] Web services owner: Christopher Paulus
- □ [phys_sec] physical security
- □ [TBR] to be removed
- □ [TBD] to be determined (to be done)

sources: safeguards & controls

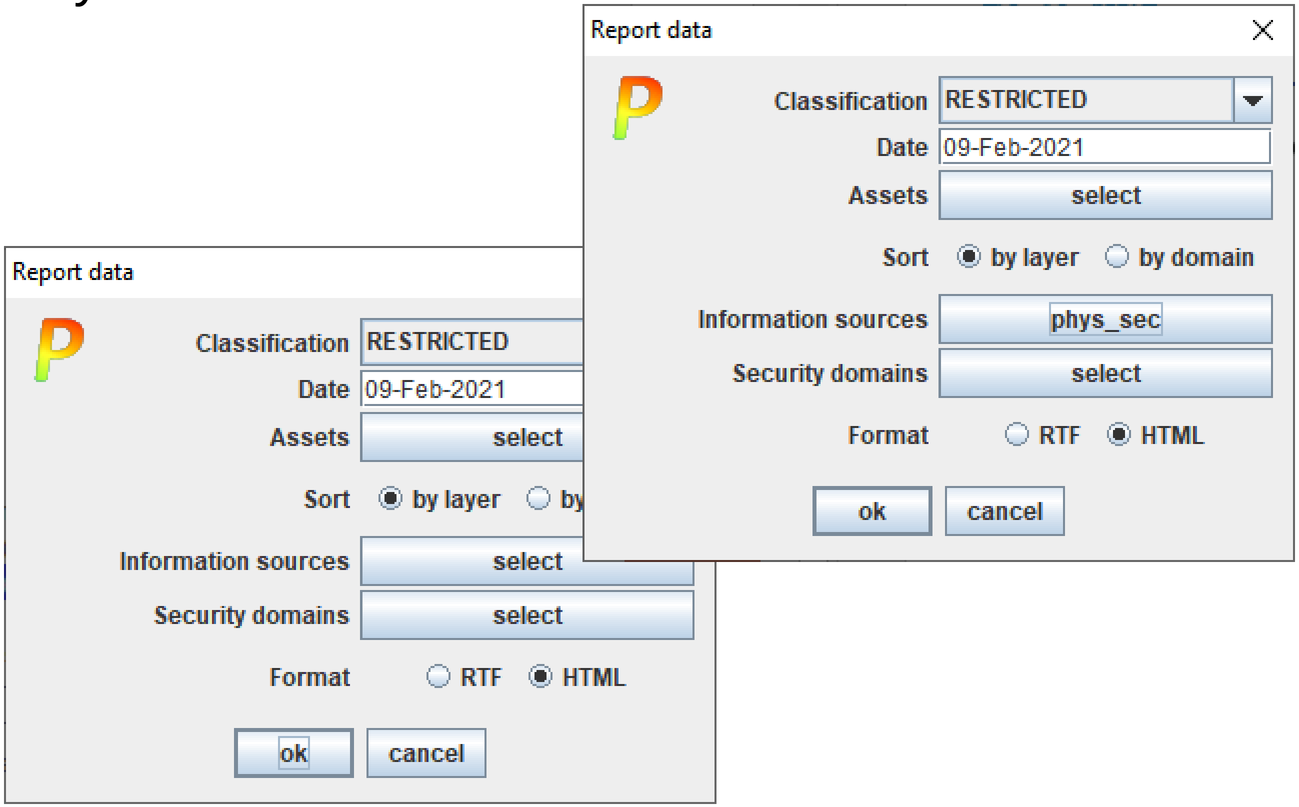
- filter by information sources



	as...	top	re...		level	safeguard	do...	so...	ap...	co...	cu...	tar...	Pl...
□						SAFEGUARDS					L0...	L3-...	L2...
□	M	PR	5	🟦		[M] Protection of Media					L2	L4	L2...
□	M	PR	5	🟦		[M.2] Media management					L2	L4	L2...
□	PHY	EL	3	🟦		[M.3] Connection of removable devices is under control		TBD			L2	L4	L2...
□	M	PR	5	🟩		[AUX] Auxiliary Means		ph...			L0...	L3-...	L2...
□	PHY	PR	4	🟩		[L] Protection of the installations		ph...	...		L0...	L3-...	L2...

sources: reports

- filter by sources



Report data

Classification RESTRICTED

Date 09-Feb-2021

Assets select

Sort ● by layer ○ by

Information sources select

Security domains select

Format ○ RTF ● HTML

Report data

Classification RESTRICTED

Date 09-Feb-2021

Assets select

Sort ● by layer ○ by domain

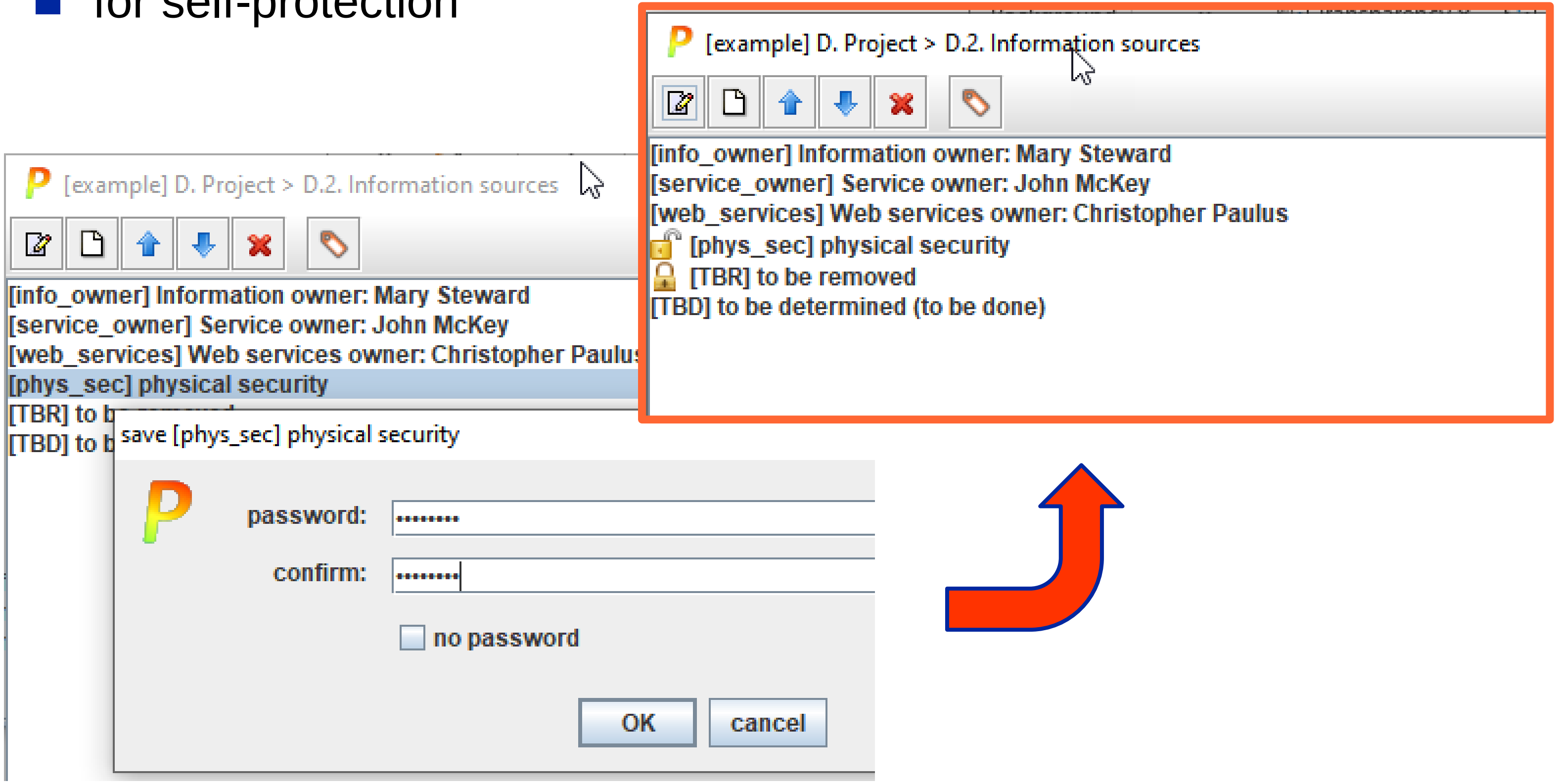
Information sources phys_sec

Security domains select

Format ○ RTF ● HTML

sources with a password

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



[example] D. Project > D.2. Information sources

[info_owner] Information owner: Mary Steward
[service_owner] Service owner: John McKey
[web_services] Web services owner: Christopher Paulus
[phys_sec] physical security
[TBR] to b
[TBD] to b

save [phys_sec] physical security

password: ••••••••

confirm: ••••••••

□ no password

[example] D. Project > D.2. Information sources

[info_owner] Information owner: Mary Steward
[service_owner] Service owner: John McKey
[web_services] Web services owner: Christopher Paulus
[phys_sec] physical security
[TBR] to be removed
[TBD] to be determined (to be done)

security profiles (evl)

- official collections of security measures

CIS_en.car

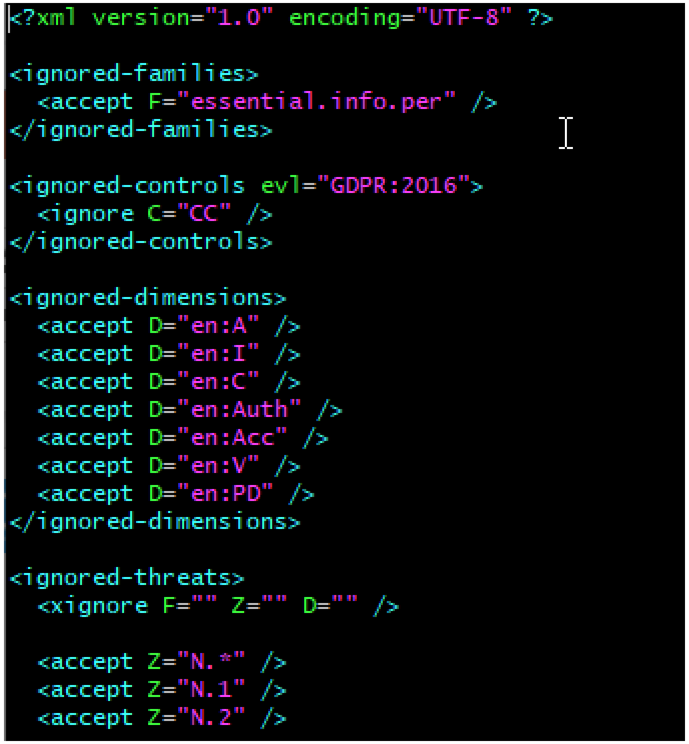
```
profile= 27002_2013_2016-06-16_en.evl
# profile= 27002_2005_2014-04-01_en.evl
# profile= sp800-53_rev3_2012-07-16_en.evl
profile:en.PD= GDPR-2016_2020-10-15_en.evl
profile:en.PD= 29151_A_2017_2017-08-30_en.evl
```

ignore

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

CIS_en.car

```
ignore= ignored.xml
```



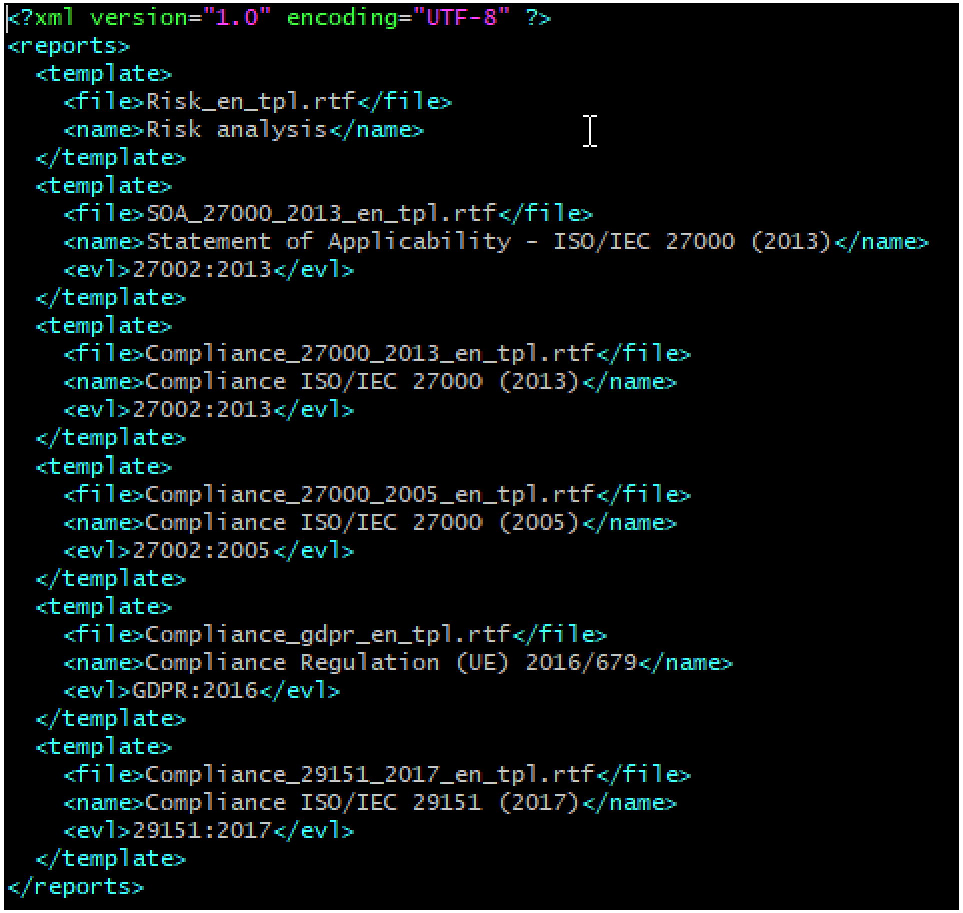
```
<?xml version="1.0" encoding="UTF-8" ?>

<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" />
```

reports

- report templates

CIS_en.car

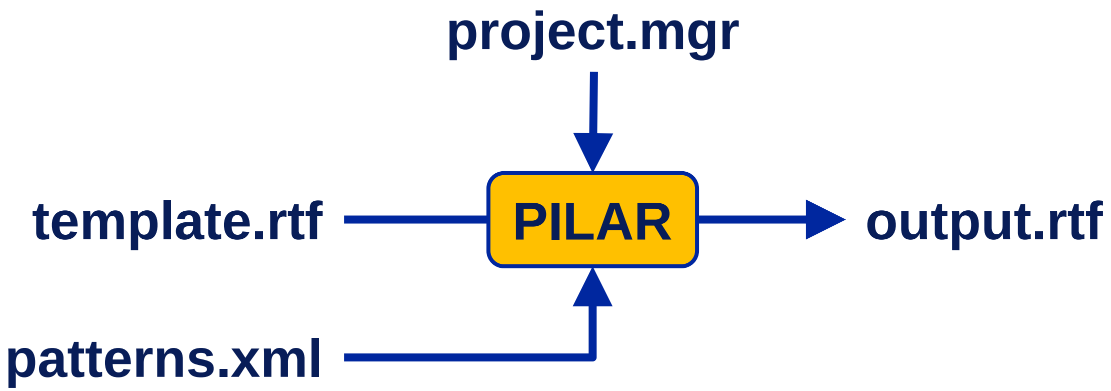
```
reports= reports.xml
```



```
<?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>
```

reports

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

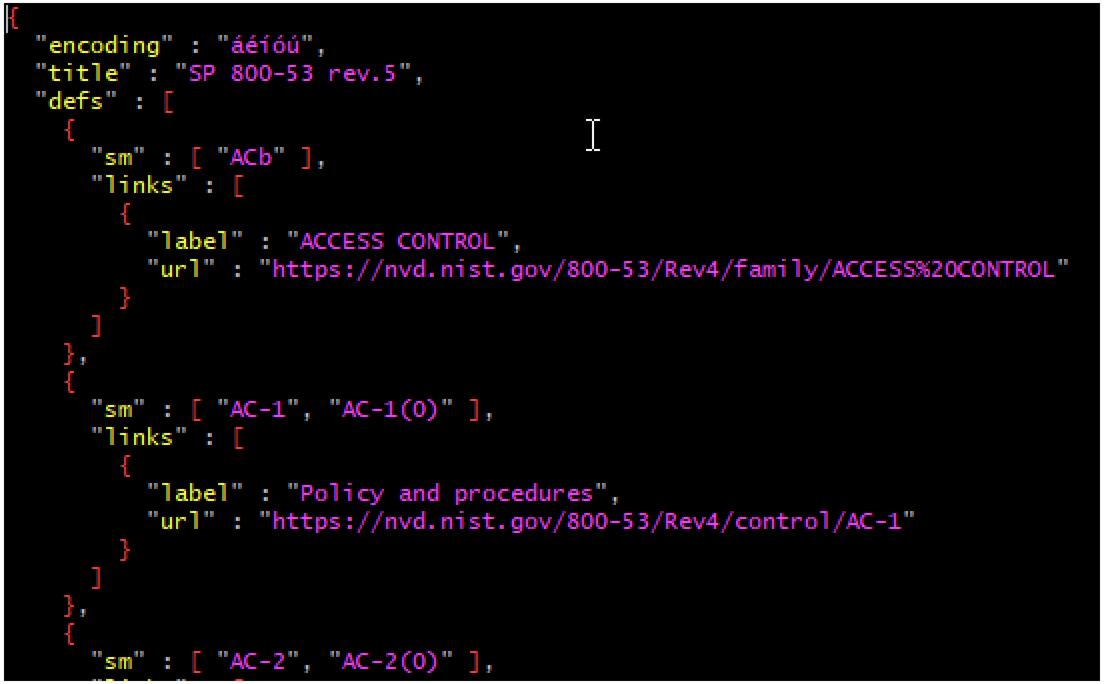


https://www.pilar-tools.com/doc/ReportTemplates_74_en_e.pdf

hooks

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

```
$ ls -1 bib_en/hooks-*
bib_en/hooks-kaspersky.json
bib_en/hooks-sp800-53.json
```

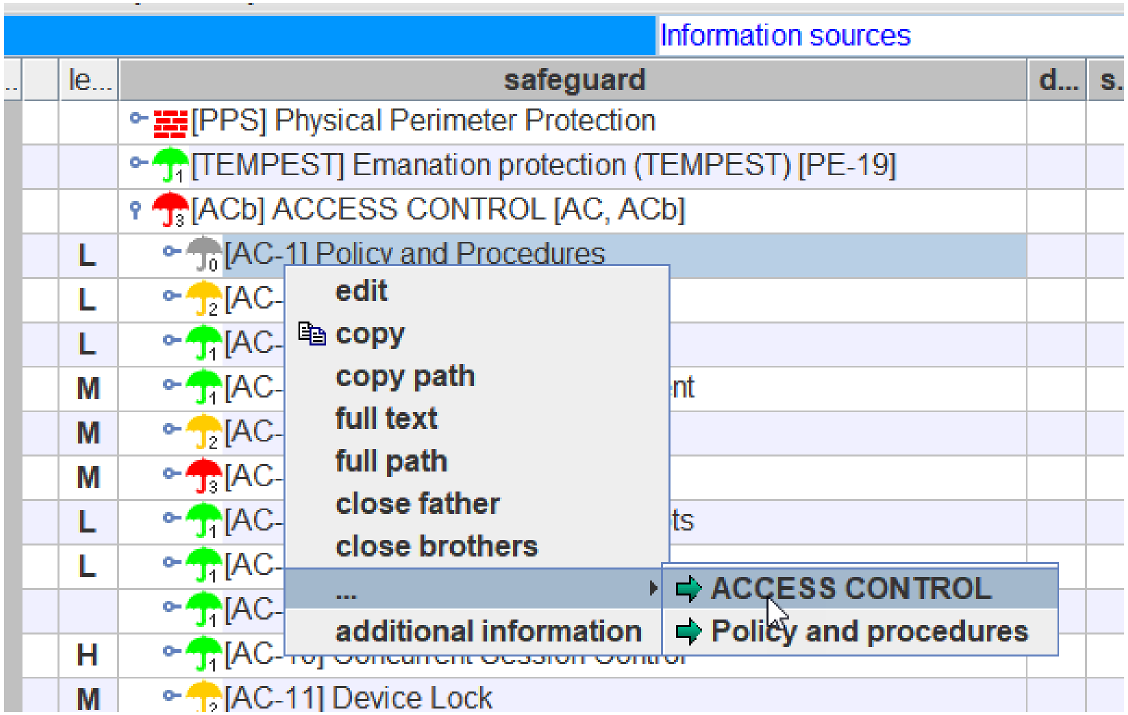


```
{
  "encoding" : "áéíóú",
  "title" : "SP 800-53 rev.5",
  "defs" : [
    {
      "sm" : [ "ACb" ],
      "links" : [
        {
          "label" : "ACCESS CONTROL",
          "url" : "https://nvd.nist.gov/800-53/Rev4/family/ACCESS%20CONTROL"
        }
      ]
    },
    {
      "sm" : [ "AC-1",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

hooks

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

```
$ ls -1 bib_en/hooks-*
bib_en/hooks-kaspersky.json
bib_en/hooks-sp800-53.json
```



Information sources

..		le...	safeguard	d...	s.
			[PPS] Physical Perimeter Protection		
			[TEMPEST] Emanation protection (TEMPEST) [PE-19]		
			[ACb] ACCESS CONTROL [AC, ACb]		
		L	[AC-1] Policy and Procedures		
		L	[AC-		
		L	[AC-		
		M	[AC- nt		
		M	[AC-		
		M	[AC-		
		L	[AC- ts		
		L	[AC-		
			[AC-		
		H	[AC-10] Concurrent Session Control		
		M	[AC-11] Device Lock		

any question?

support@pilar-tools.com