pilar

PILAR suggestions

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

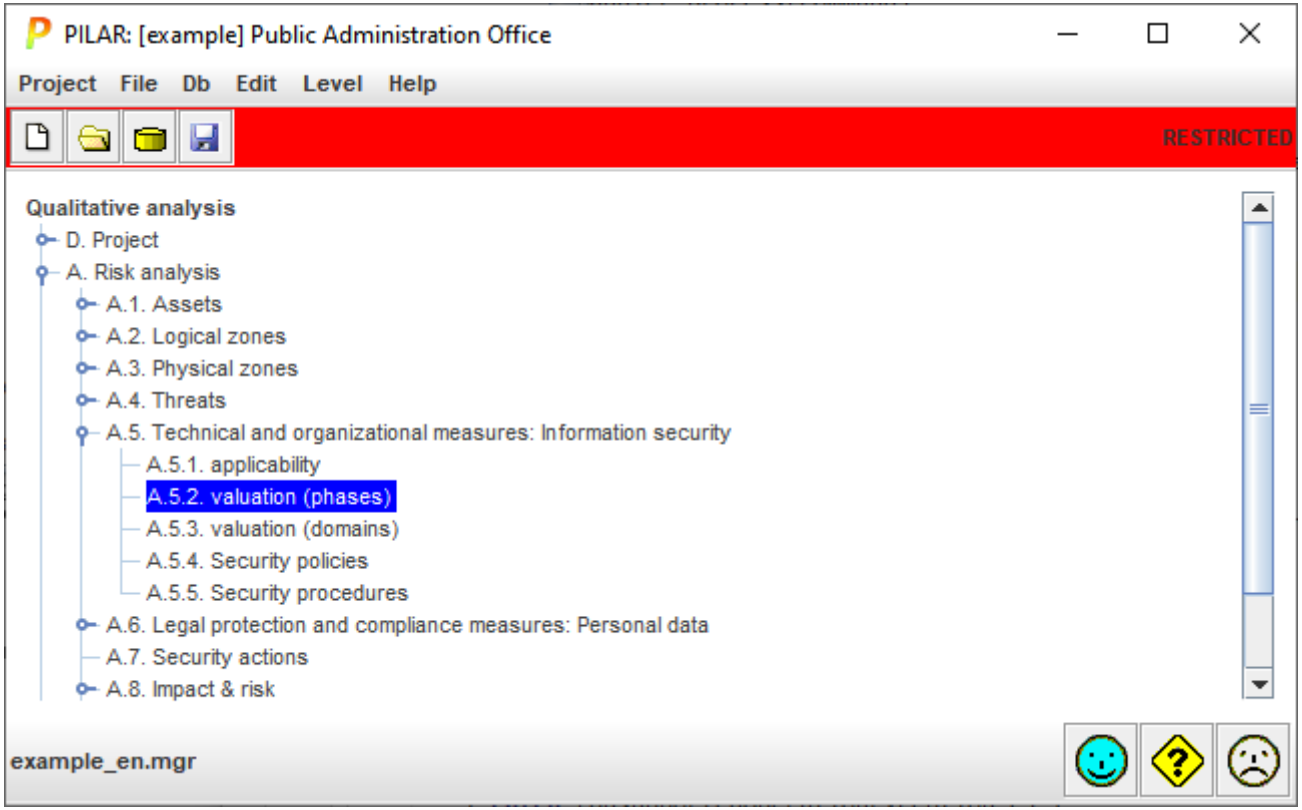
October 25, 2019

suggestions in PILAR

- safeguards
- structural suggestions
  - by security domain
- maturity suggestions
  - by security domain
  - for a subset of risks

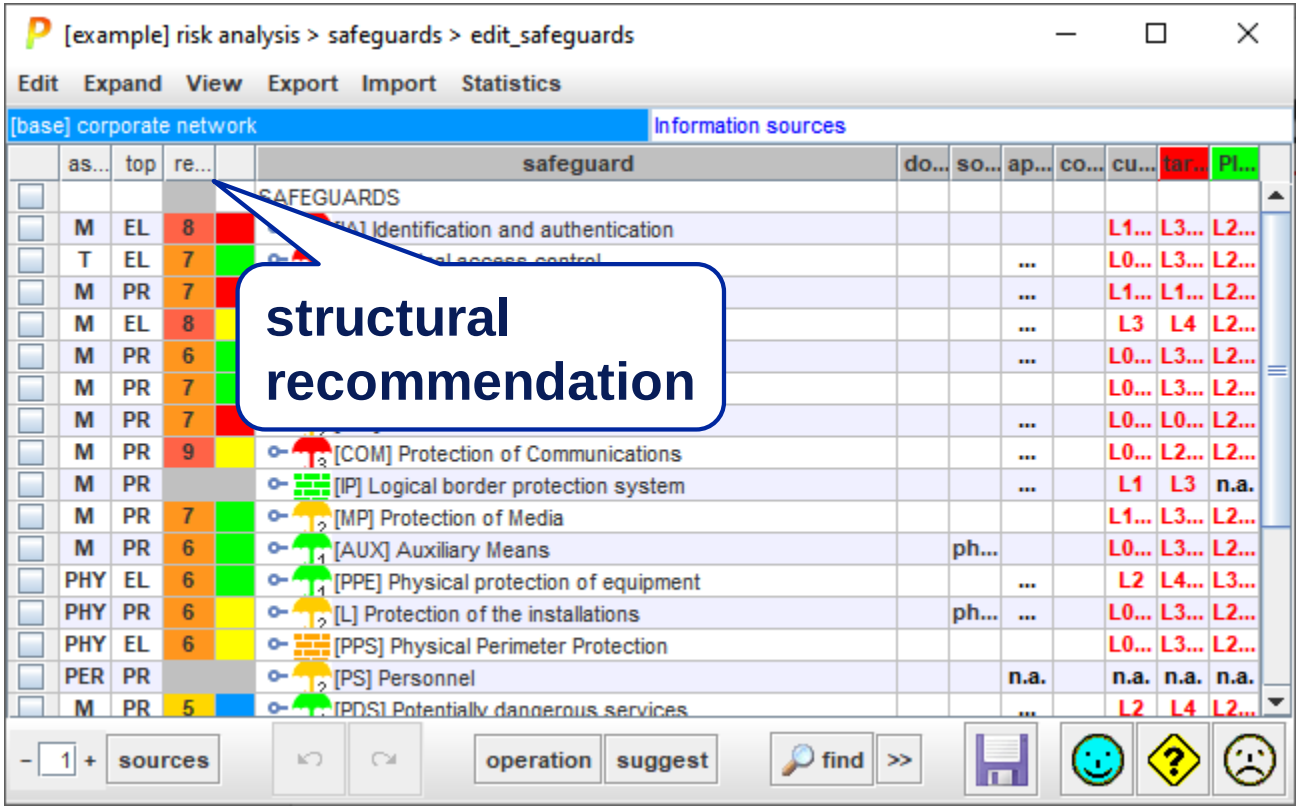
- security profiles (evl)
- structural suggestions
  - by security domain
- maturity suggestions
  - by security domain

safeguards by domain



structural recommendations

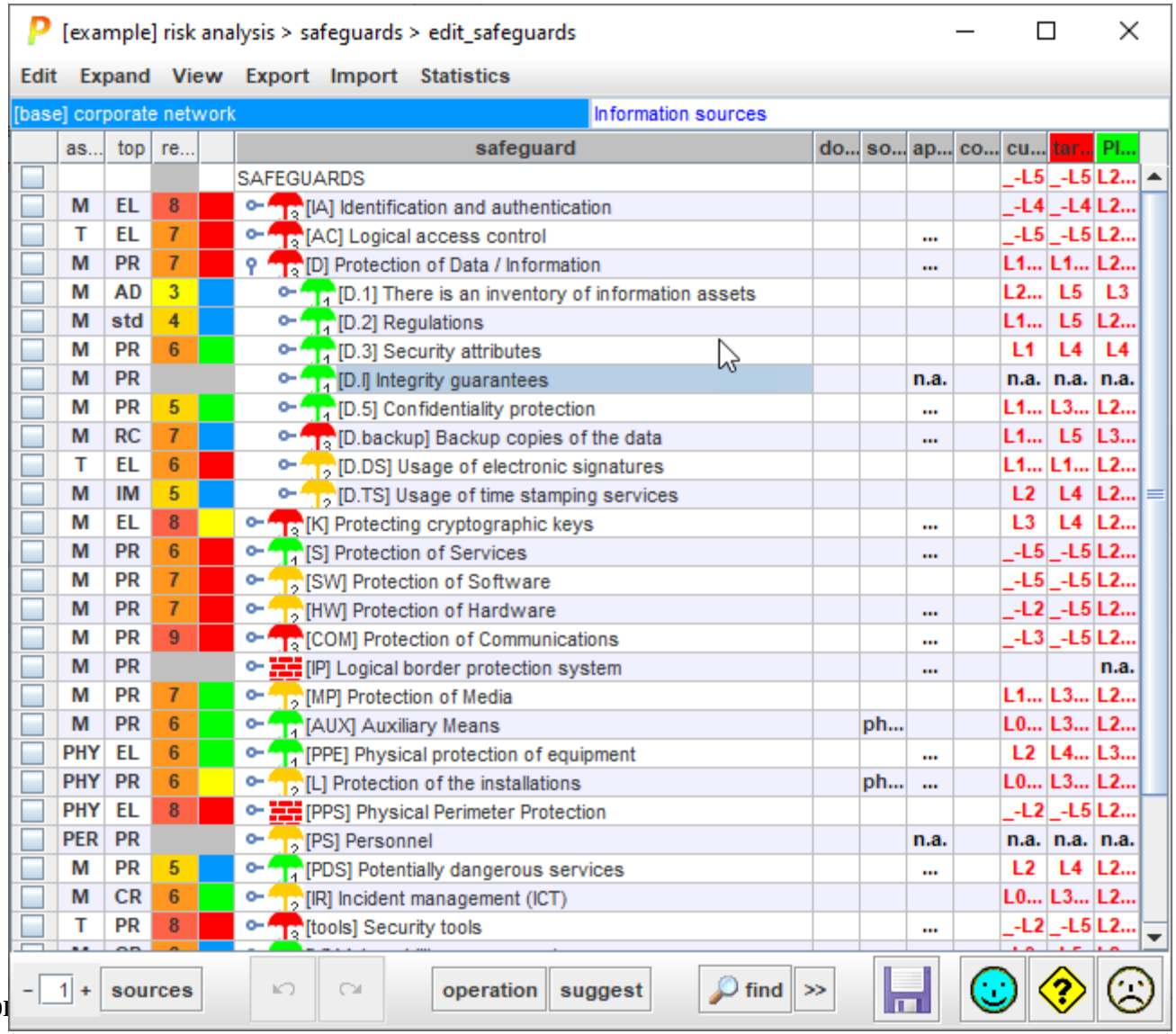
1. select one domain (blue band above)



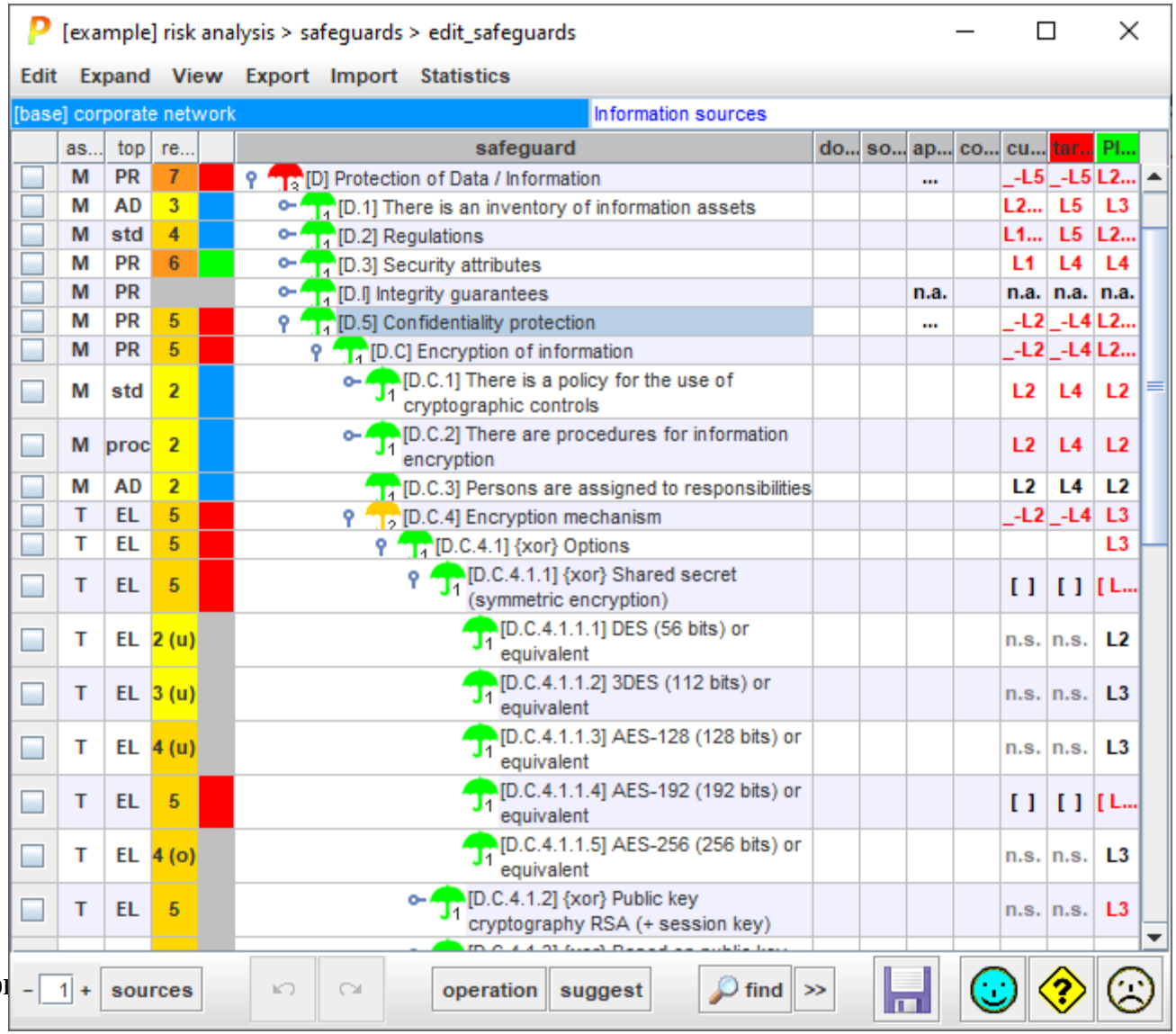
structural recommendations

- for those safeguards that apply
  - safeguards may not apply ...
    - because you said so (n.a.)
    - because PILAR thinks they are useless in your project
      based on asset classes, assets security requirements, and threats
- rating: a level between 0 (no use) to 10 (critical)
- caveats
  - (u) underkill: it is not powerful enough for your risks
  - (o) overkill: it is oversized for your risks

structural recommendations



structural recommendations



how to proceed

- with respect to n.a.
  - if PILAR says n.a. but you think you need it,
    revise asset classes, asset dependencies, asset requirements, and threats
  - if PILAR says n.a. and you agree,
    mark as n.a.
  - if PILAR recommends it, you agree,
    retain it, and go for maturity
  - PILAR recommends it, but you think you do not need it,
    - mark as n.a. and prepare a good argument to defend yourself
    - please think twice; it is just to easy to ignore by convenience
    - **residual risk may be falsely low because of obviating important protection measures**

how to proceed

- with respect to selection
  - you may need to change selection to reflect real facts

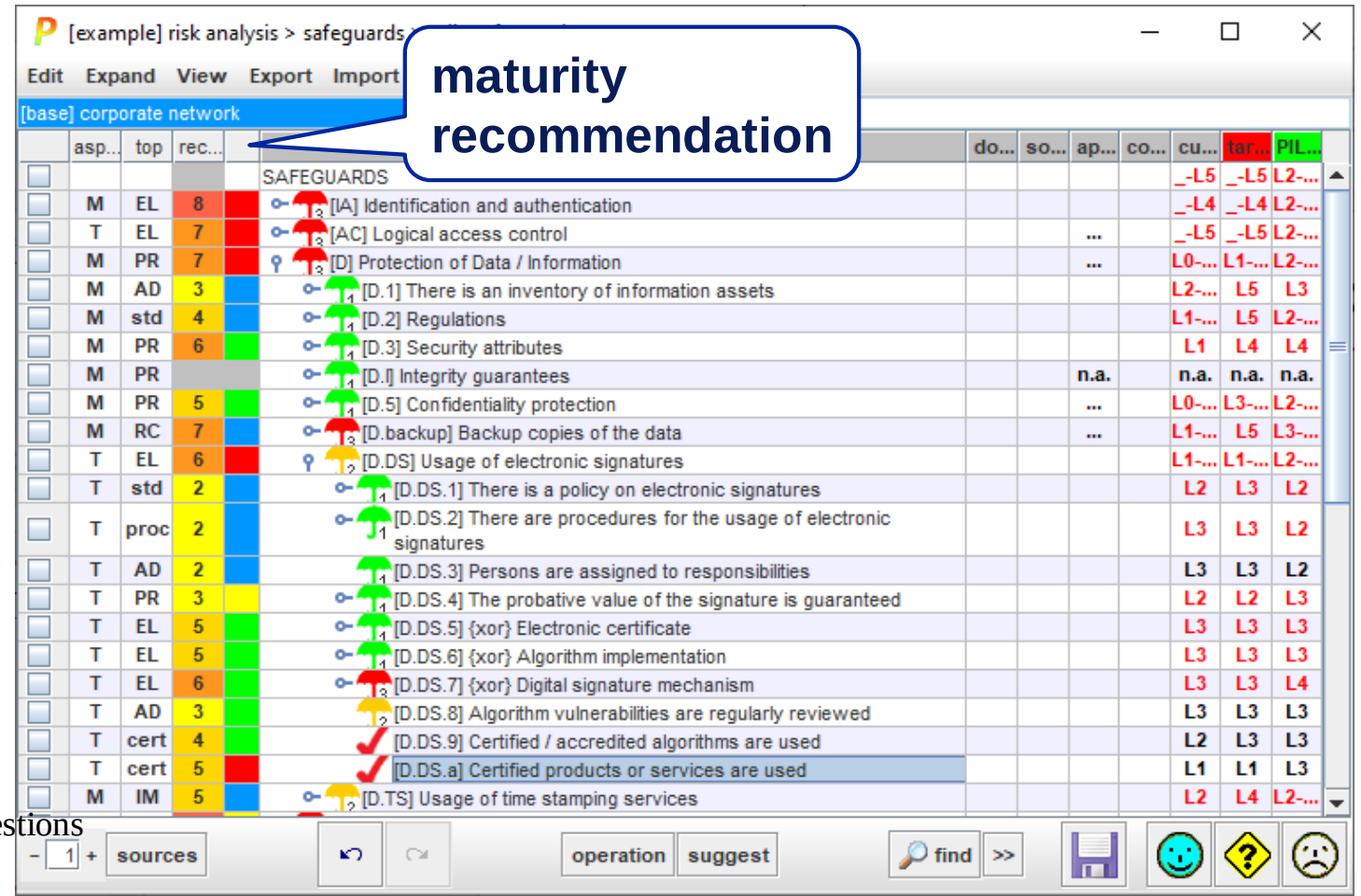
5		[D.C.4] Encryption mechanism					L2	L2-...	L3
5		[D.C.4.1] {xor} Options					L2	L2	L3
5		[D.C.4.1.1] {xor} Shared secret (symmetric encryption)					[L2]	[L2]	[L3]
2 (u)		[D.C.4.1.1.1] DES (56 bits) or equivalent					[L2]	[L2]	L2
3 (u)		[D.C.4.1.1.2] 3DES (112 bits) or equivalent					n.s.	n.s.	L3
4 (u)		[D.C.4.1.1.3] AES-128 (128 bits) or equivalent					n.s.	n.s.	L3
5		[D.C.4.1.1.4] AES-192 (192 bits) or equivalent					n.s.	n.s.	[L3]
4 (o)		[D.C.4.1.1.5] AES-256 (256 bits) or equivalent					n.s.	n.s.	L3

5		[D.C.4] Encryption mechanism					L2-...	L3-...	L3
5		[D.C.4.1] {xor} Options					L3	L3	L3
5		[D.C.4.1.1] {xor} Shared secret (symmetric encryption)					[L3]	[L3]	[L3]
2 (u)		[D.C.4.1.1.1] DES (56 bits) or equivalent					n.s.	n.s.	L2
3 (u)		[D.C.4.1.1.2] 3DES (112 bits) or equivalent					n.s.	n.s.	L3
4 (u)		[D.C.4.1.1.3] AES-128 (128 bits) or equivalent					[L3]	[L3]	L3
5		[D.C.4.1.1.4] AES-192 (192 bits) or equivalent					n.s.	n.s.	[L3]
4 (o)		[D.C.4.1.1.5] AES-256 (256 bits) or equivalent					n.s.	n.s.	L3

5		[D.C.4] Encryption mechanism					L2-...	L3-...	L3
5		[D.C.4.1] {xor} Options					L3	L3	L3
5		[D.C.4.1.1] {xor} Shared secret (symmetric encryption)					[L3]	[L3]	[L3]
2 (u)		[D.C.4.1.1.1] DES (56 bits) or equivalent					n.s.	n.s.	L2
3 (u)		[D.C.4.1.1.2] 3DES (112 bits) or equivalent					n.s.	n.s.	L3
4 (u)		[D.C.4.1.1.3] AES-128 (128 bits) or equivalent					[L3]	n.s.	L3
5		[D.C.4.1.1.4] AES-192 (192 bits) or equivalent					n.s.	n.s.	[L3]
4 (o)		[D.C.4.1.1.5] AES-256 (256 bits) or equivalent					n.s.	[L3]	L3

maturity

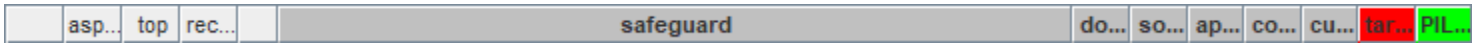
1. select one domain (blue band above)
2. select one phase (table header)



suggestions

how to proceed

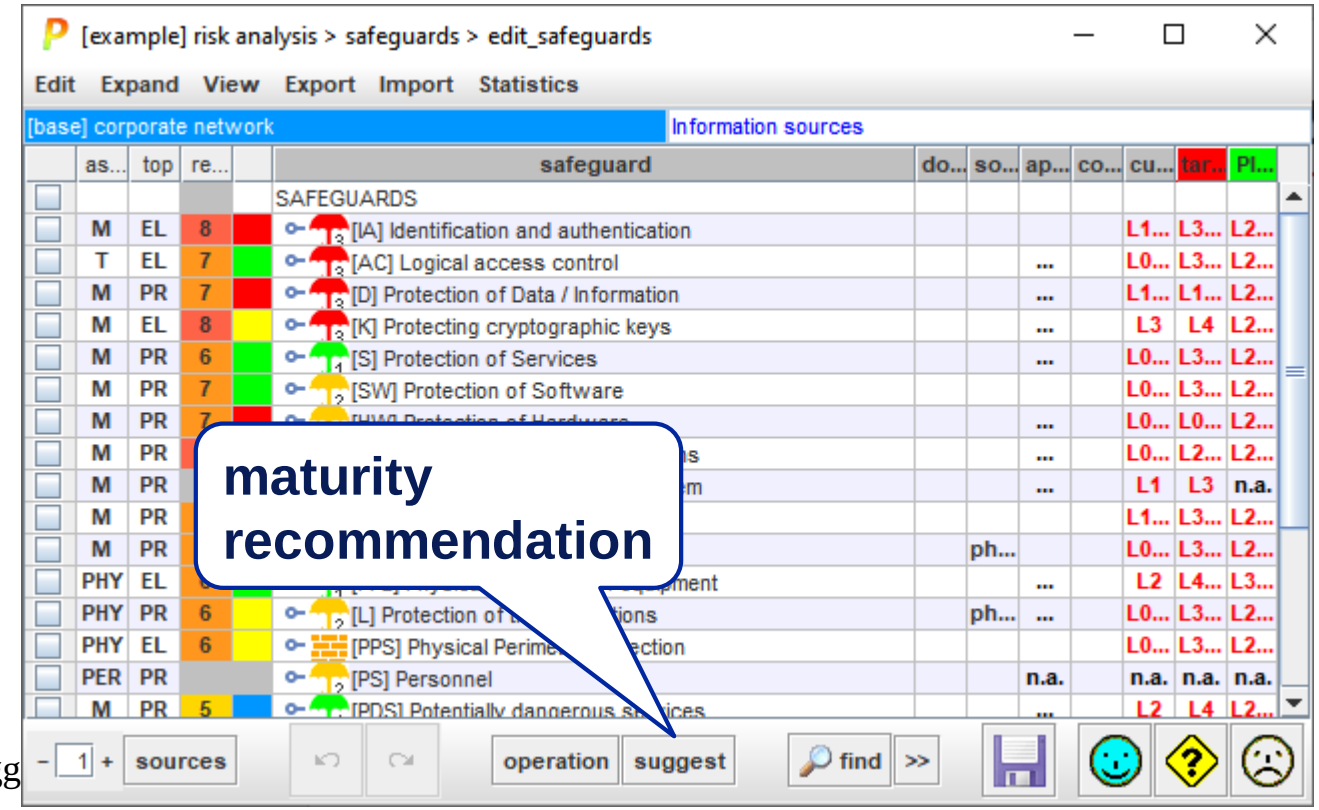
- light reflects differences between selected phase (red) and target phase (green)



  - blue: selected maturity above target
  - green: selected maturity equals target
  - yellow: selected maturity a bit below target
  - red: selected maturity far below target
  - gray: not applies
- objective: avoid red marks

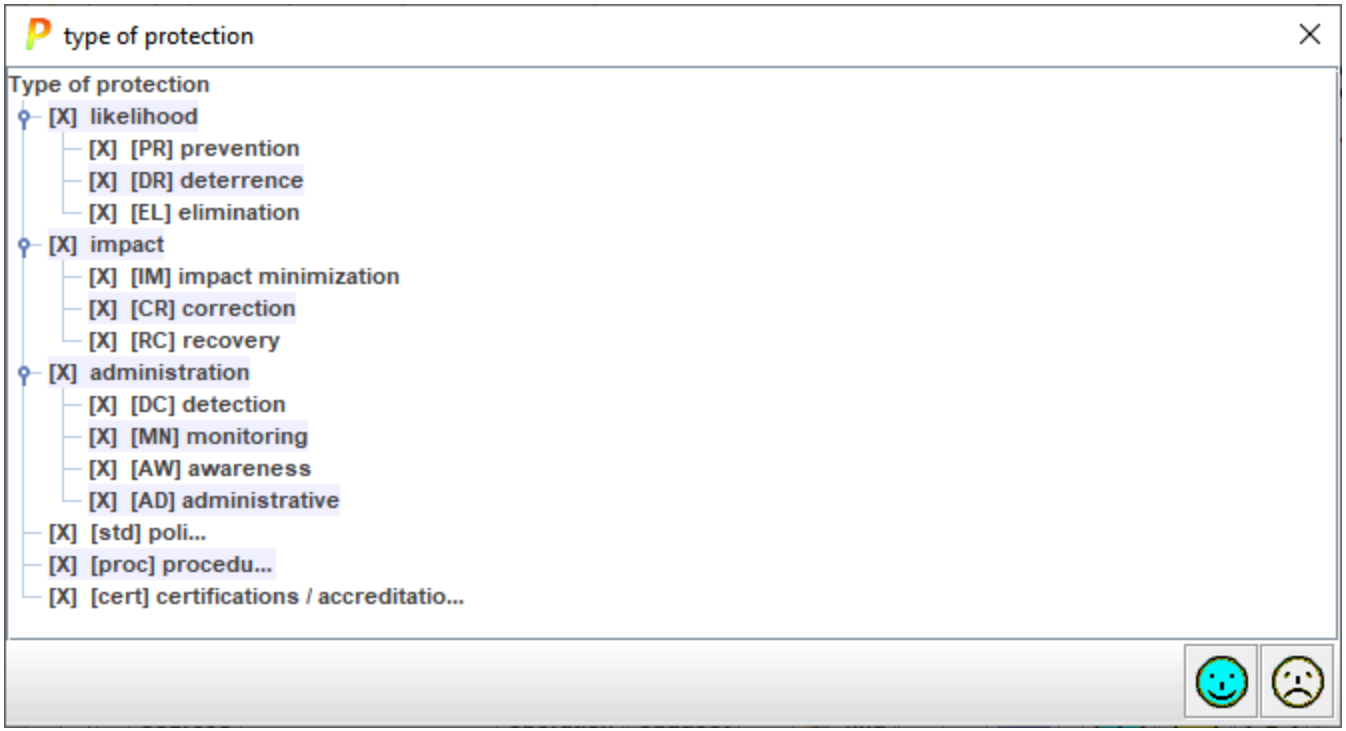
maturity

1. select one domain (blue band above)
2. select one phase (table header)
3. click SUGGEST (bottom)



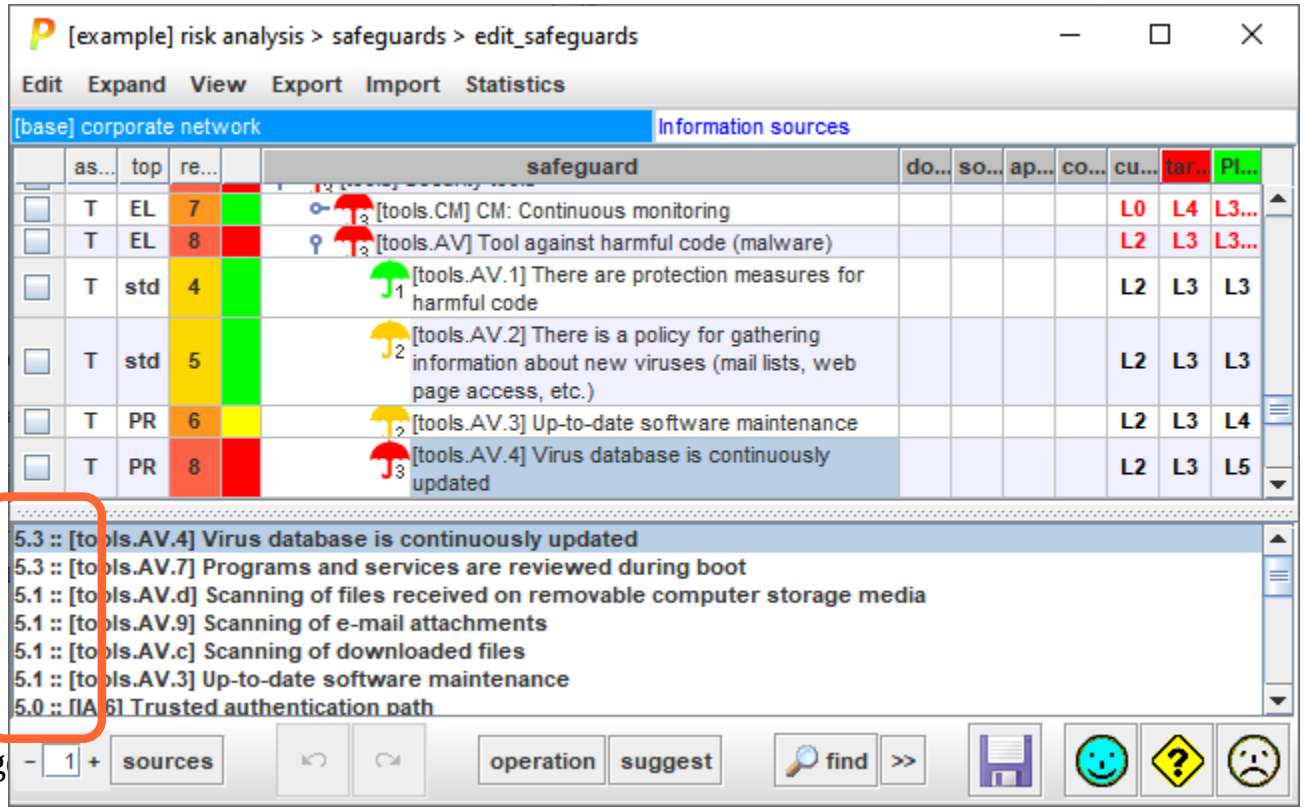
maturity

1. select the type(s) of protection you are looking for



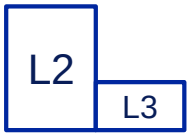
maturity recommendation

1. recommendations are sorted by first column index number
2. click on the suggestion to center it on the upper panel
3. these recommendations apply to the whole security domain

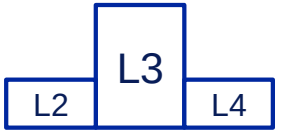


how to proceed

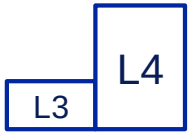
- for low risk systems,
  - minimal objective should be mostly L2, and L3 for some critical measures



- for medium systems,
  - minimal objective should be mostly L3, L4 for some critical measures, and L2 for low effect measures



- for high risk systems,
  - objective should be mostly L4, L3 for low effect measures

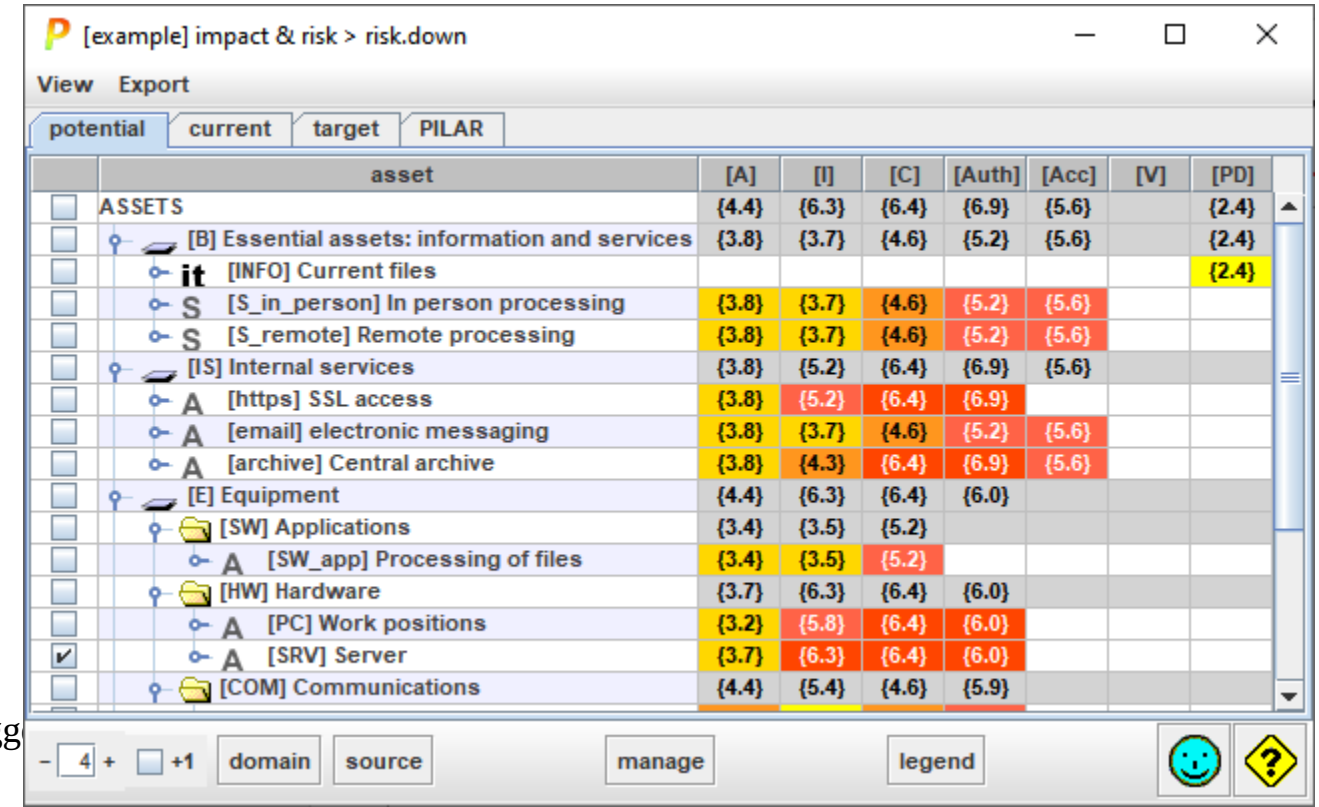


- L5 is most usually utopia

safeguards for some risks /1

- on any presentation of risks; e.g. by assets

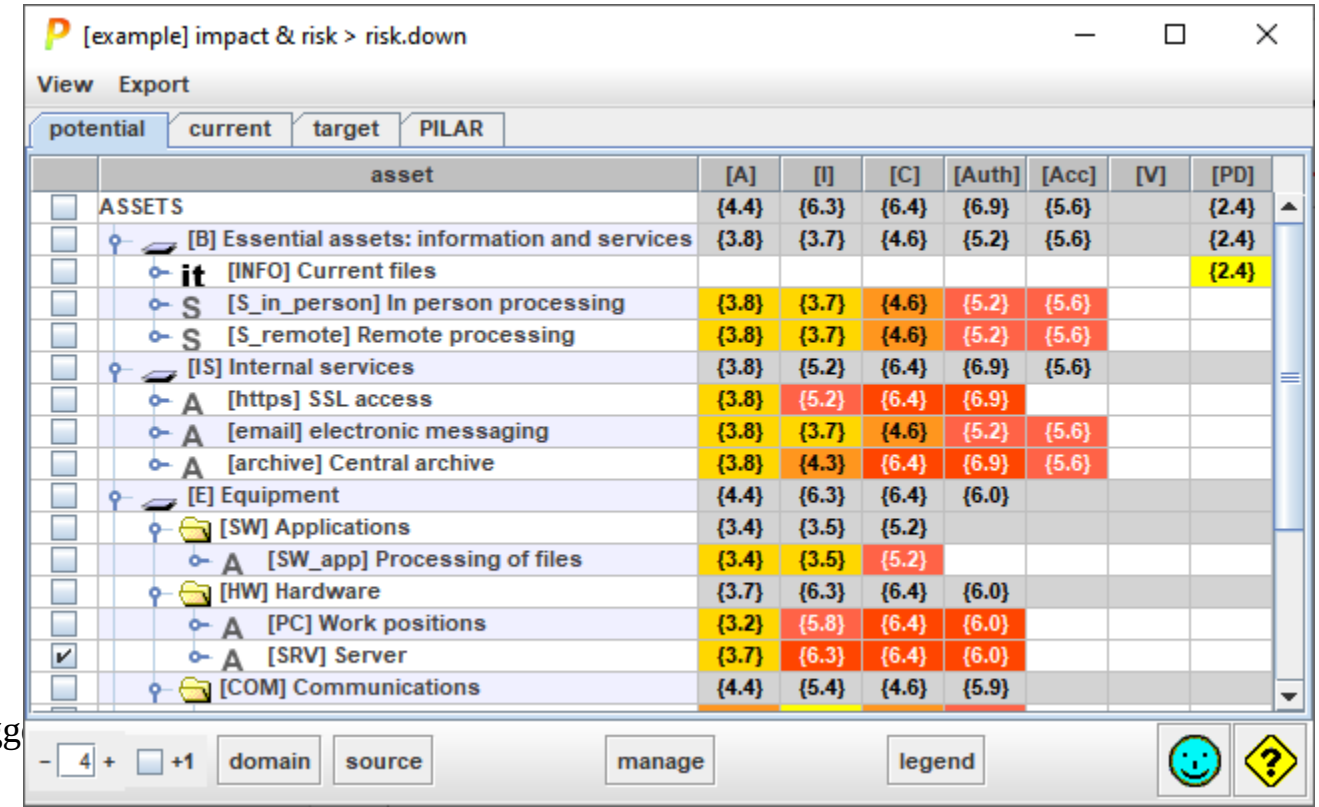
1. select one or more rows on the left column
   you may select complete assets, or some risks
2. click suggest on the bottom tool-bar



safeguards for some risks /2

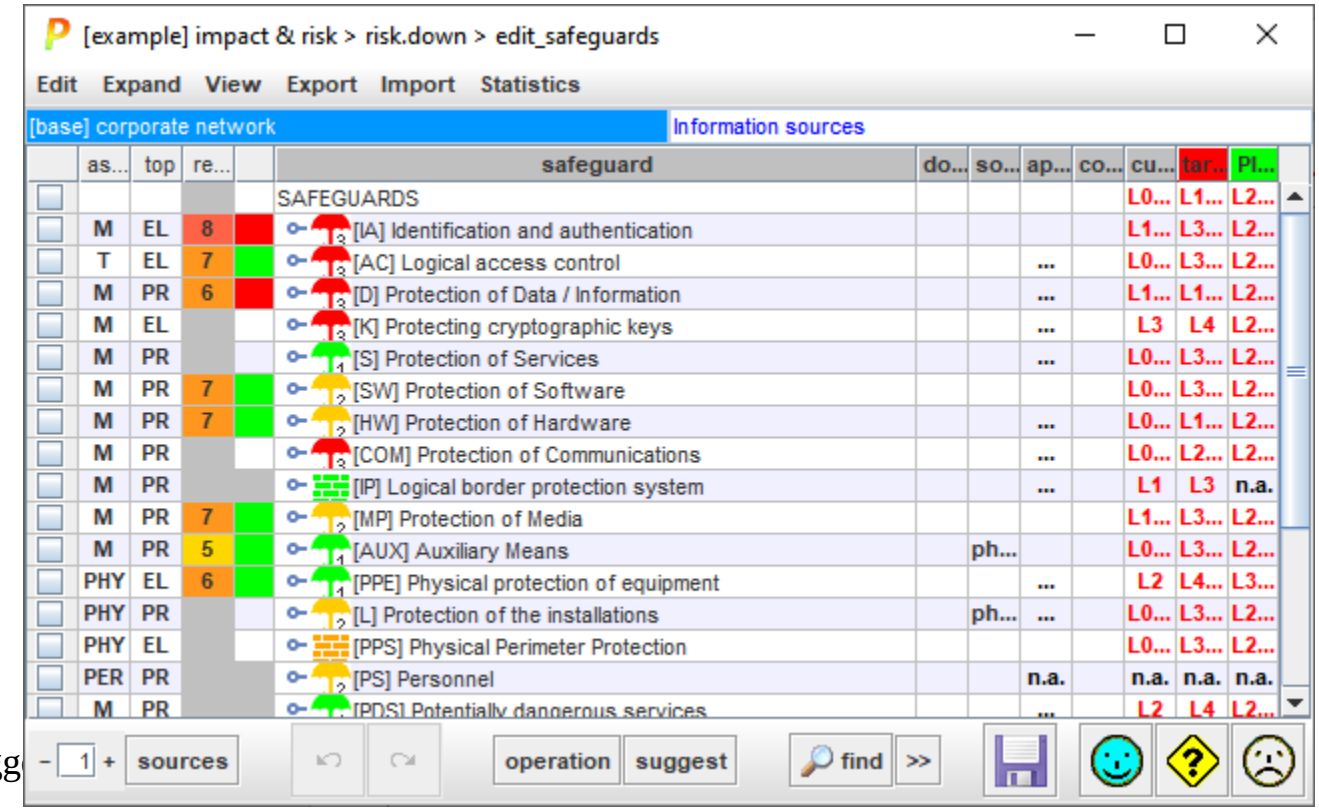
- on any presentation of risks; e.g. by assets

1. select one or more rows on the left column
   you may select complete assets, or some risks
2. click suggest on the bottom tool-bar

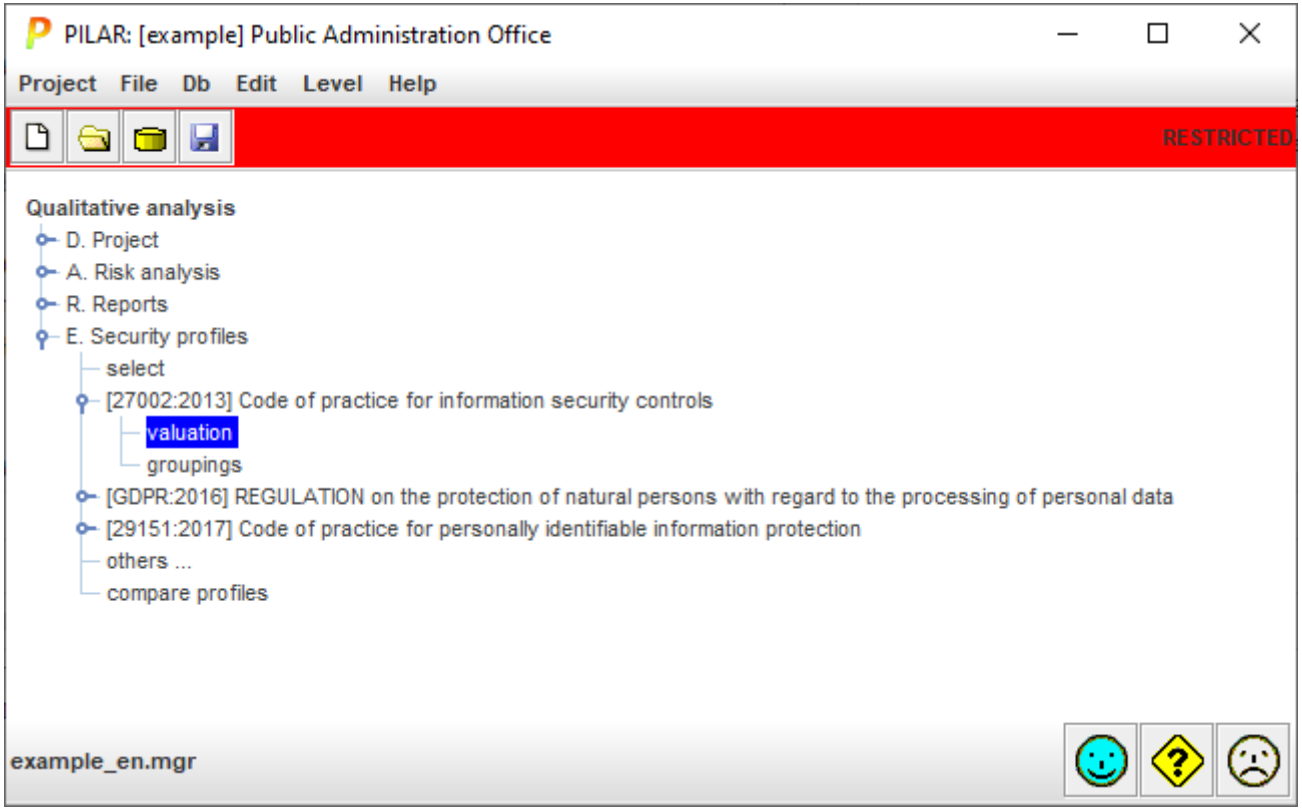


safeguards for some risks /3

- PILAR shows the recommendation for the selected risks
- let PILAR suggest
- etc.

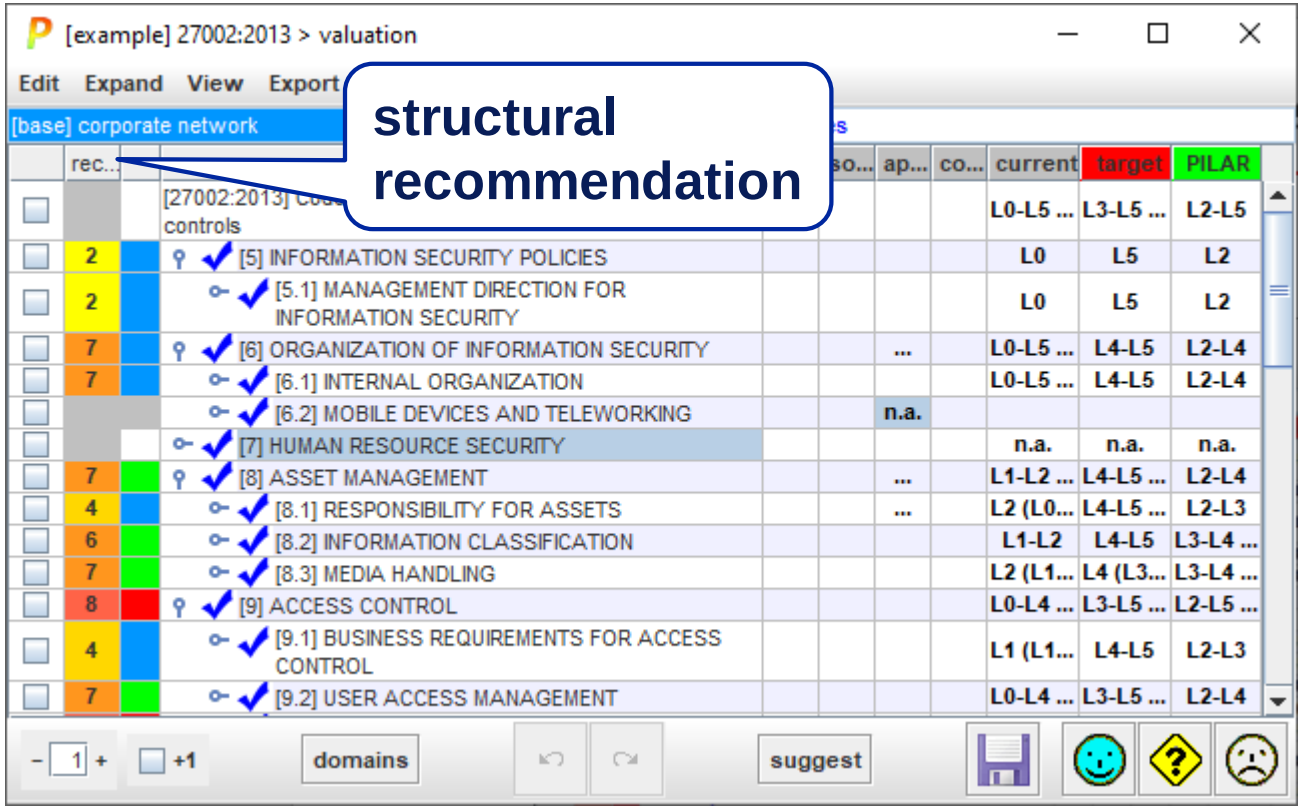


controls by domain



structural recommendations

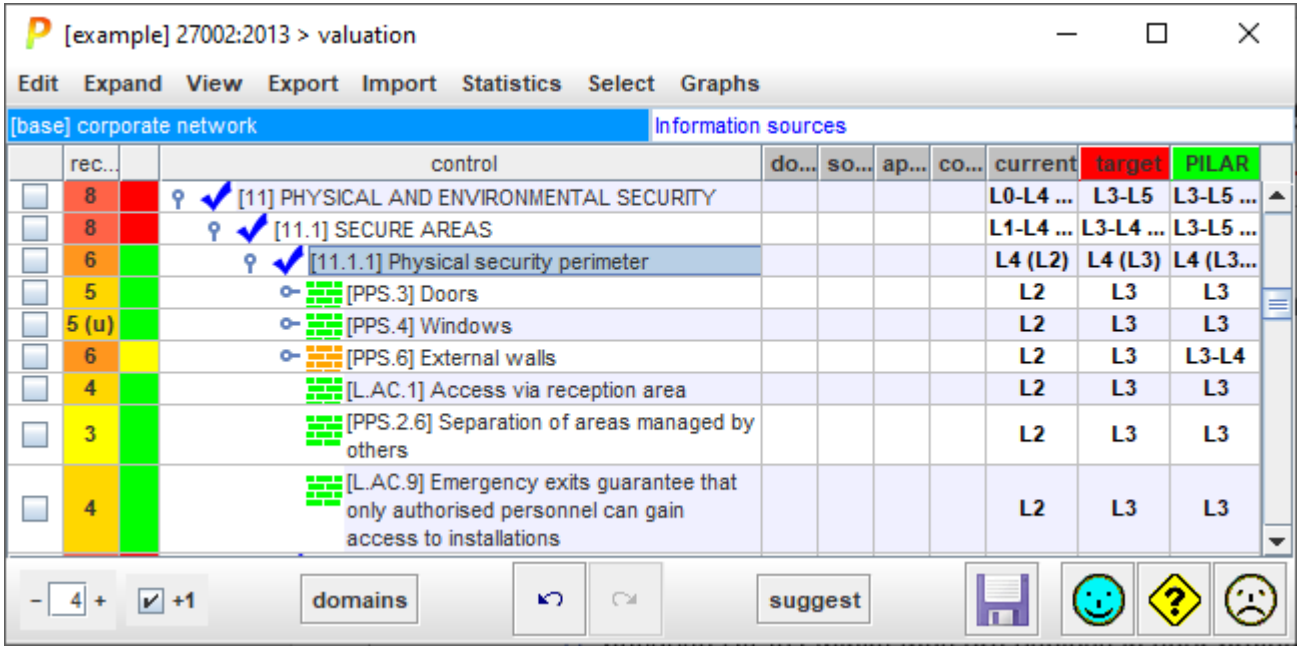
1. select one domain (blue band above)



suggestions

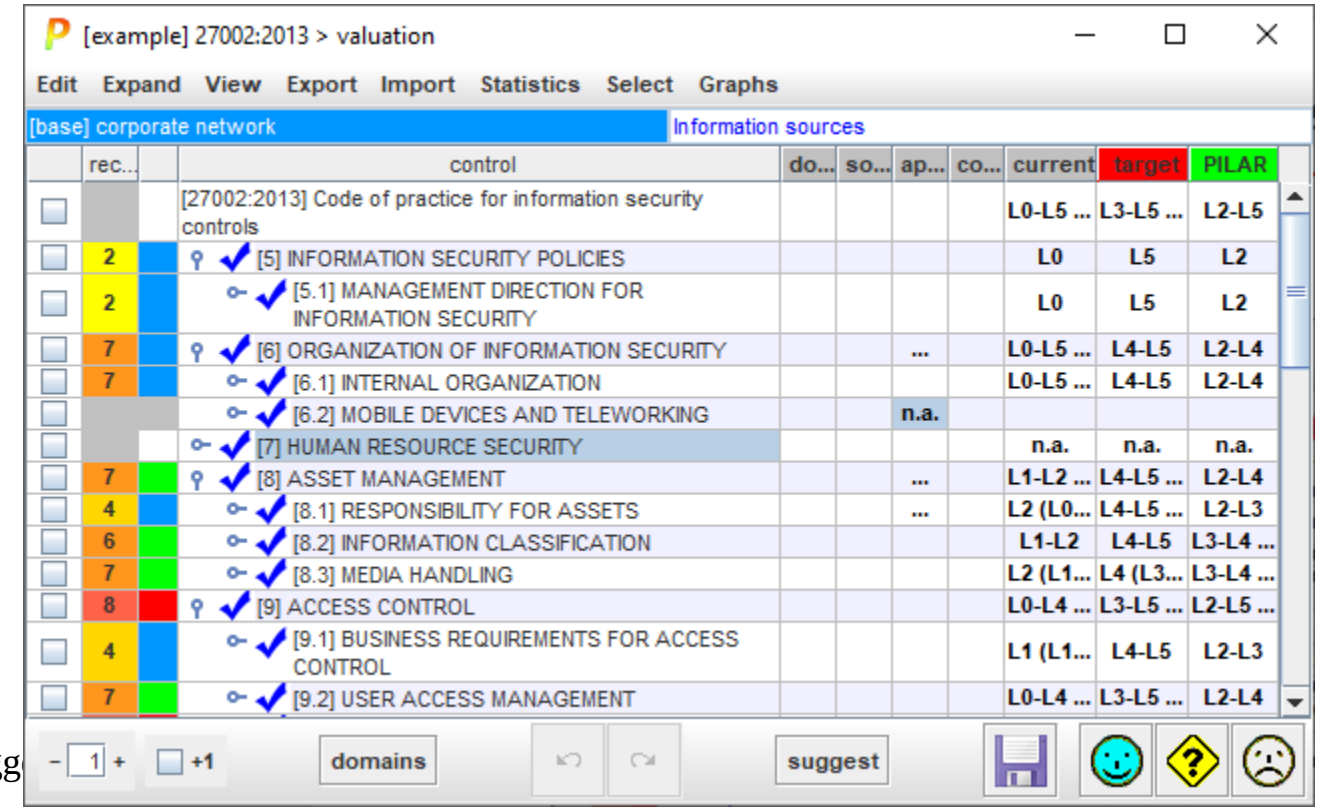
structural recommendations

- rating: a level between 0 (no use) to 10 (critical)
- if maturity of safeguards differs from maturity of controls: revise why!



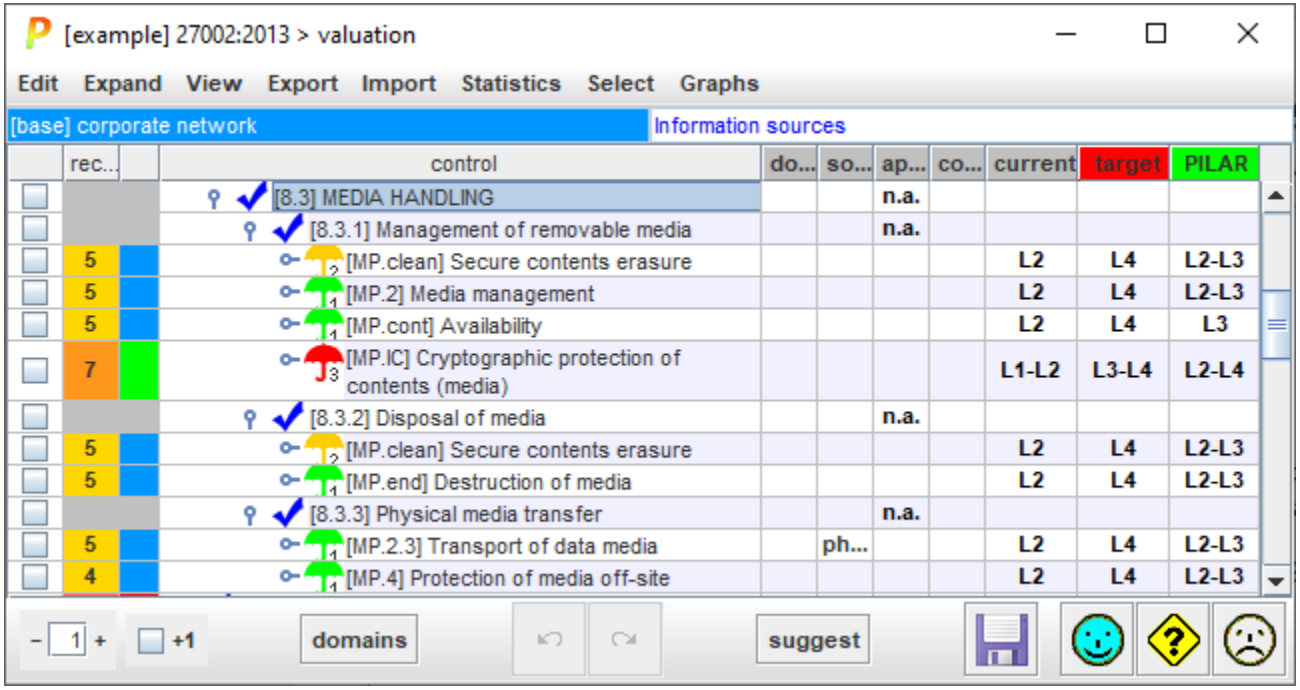
structural recommendations

- controls may not apply ...
  - because you said so (n.a.)
  - because PILAR thinks they are useless in your project
    based on asset classes, assets security requirements, and threats



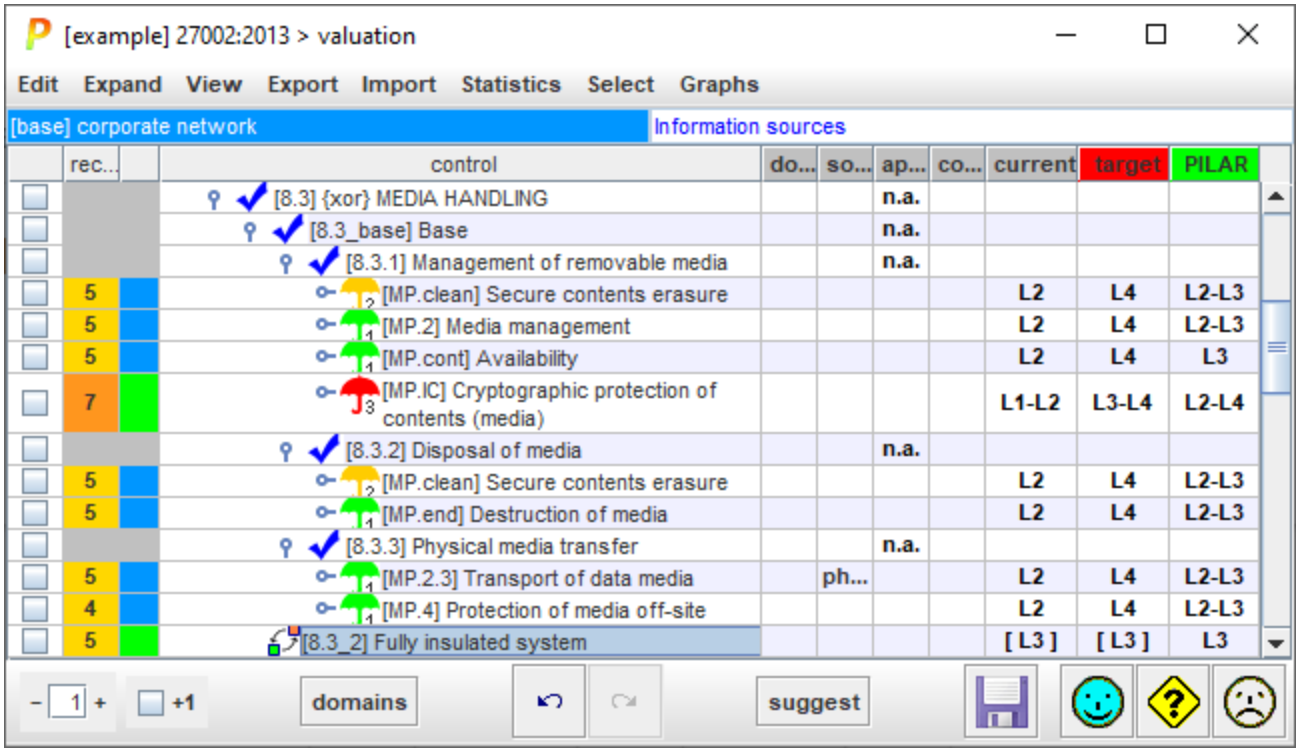
structural recommendations

- a control may not apply (for formal reasons: compliance) but safeguards do apply (for technical reasons)



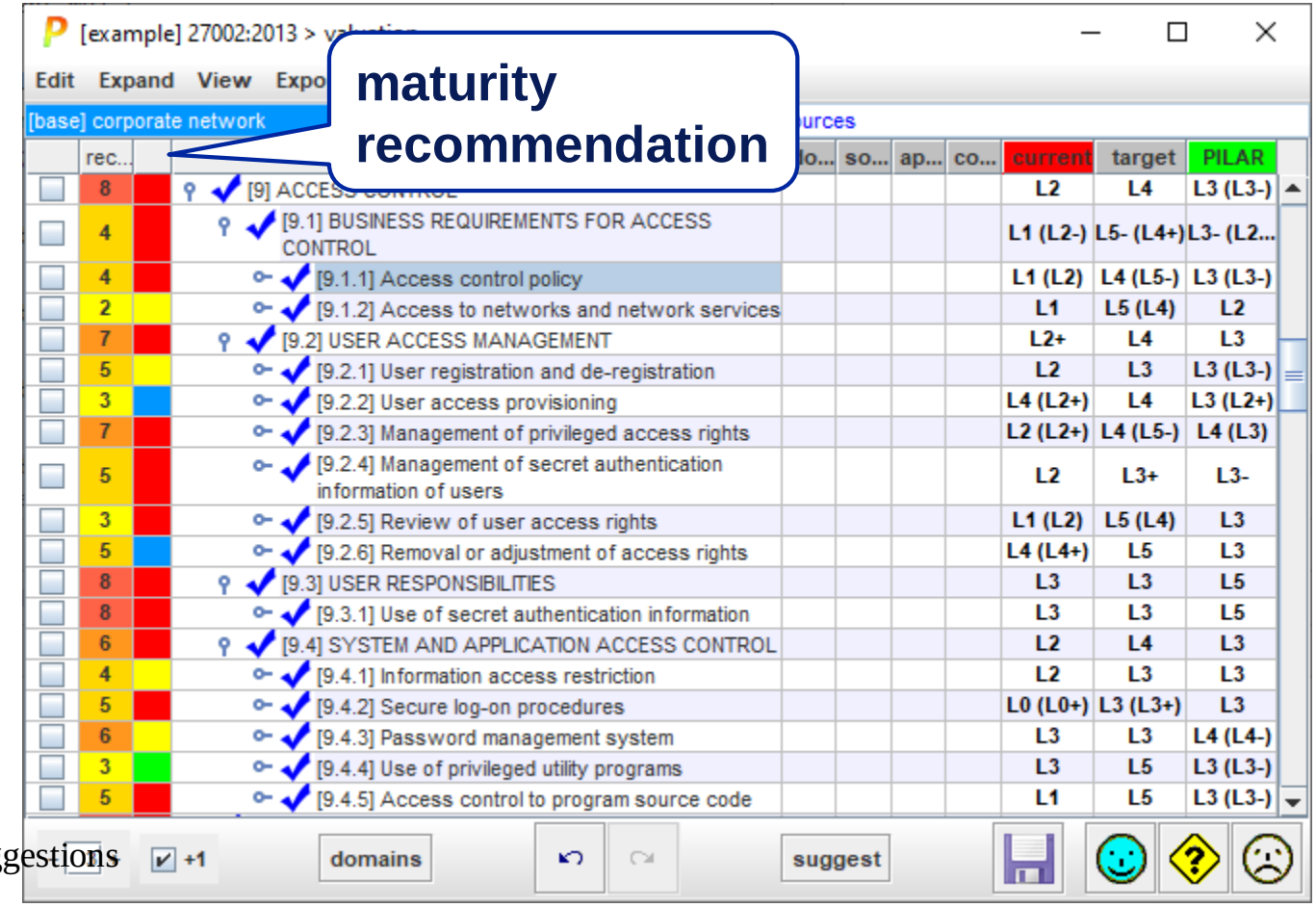
structural recommendations

- a control may be compensated by another control
  - than you may decide independently for safeguards



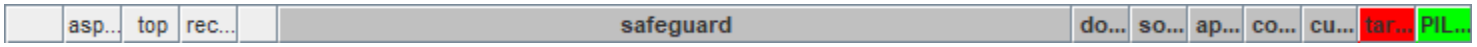
maturity

1. select one domain (blue band above)
2. select one phase (table header)



how to proceed

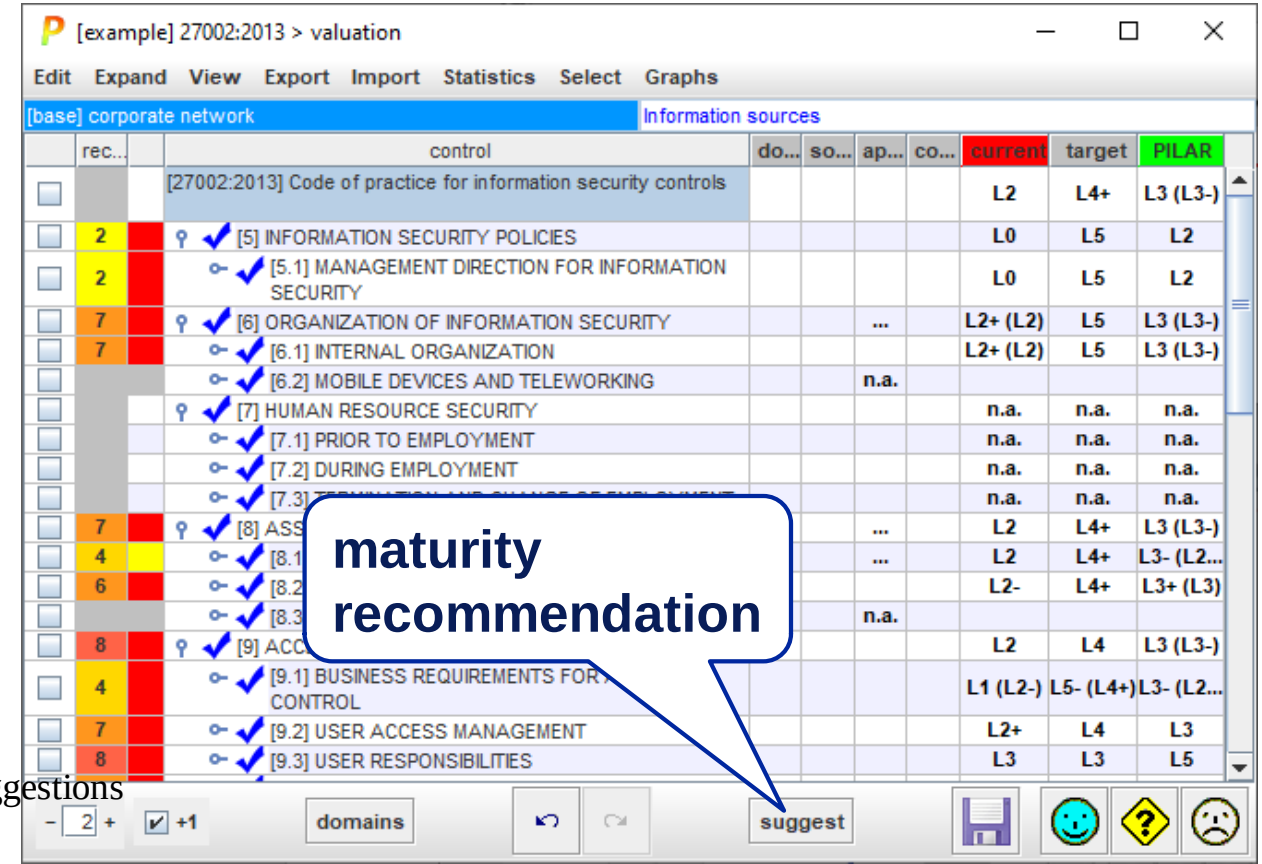
- light reflects differences between selected phase (red) and target phase (green)



  - blue: selected maturity above target
  - green: selected maturity equals target
  - yellow: selected maturity a bit below target
  - red: selected maturity far below target
  - gray: not applies
- objective: avoid red marks

maturity

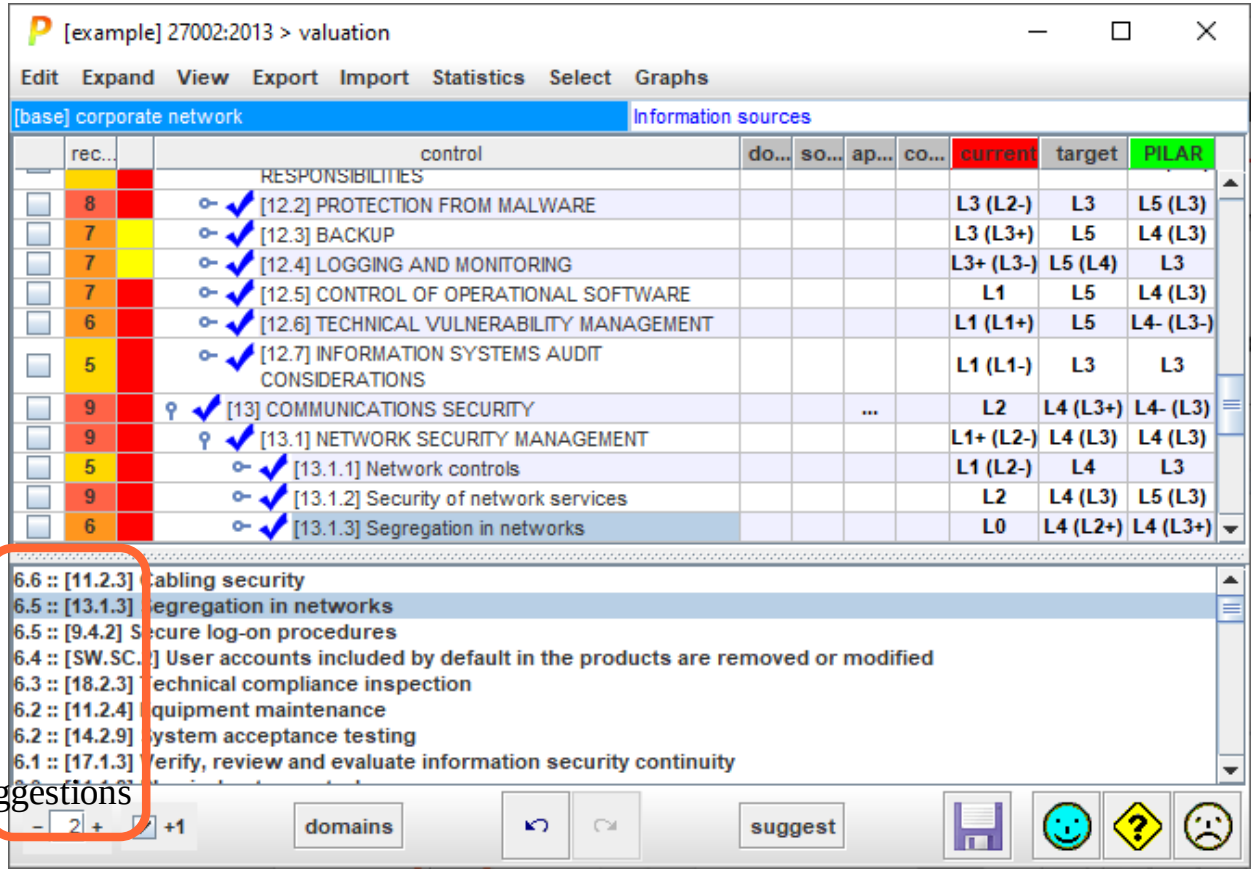
1. select one domain (blue band above)
2. select one phase (table header)
3. click SUGGEST (bottom)



suggestions

maturity recommendation

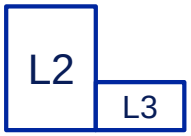
1. recommendations are sorted by first column index number
2. click on the suggestion to center it on the upper panel
3. these recommendations apply to the whole security domain



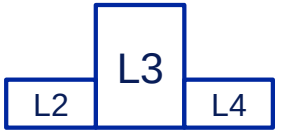
suggestions

how to proceed

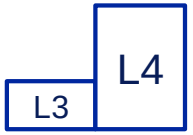
- for low risk systems,
  - minimal objective should be mostly L2, and L3 for some critical measures



- for medium systems,
  - minimal objective should be mostly L3, L4 for some critical measures, and L2 for low effect measures



- for high risk systems,
  - objective should be mostly L4, L3 for low effect measures



- for an ISMS certification, aim at L5

any question?

support@pilar-tools.com