

*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



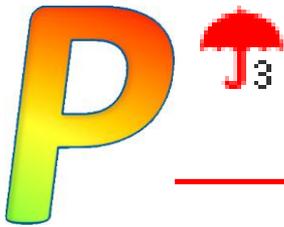
security profiles (evl)

- structural suggestions

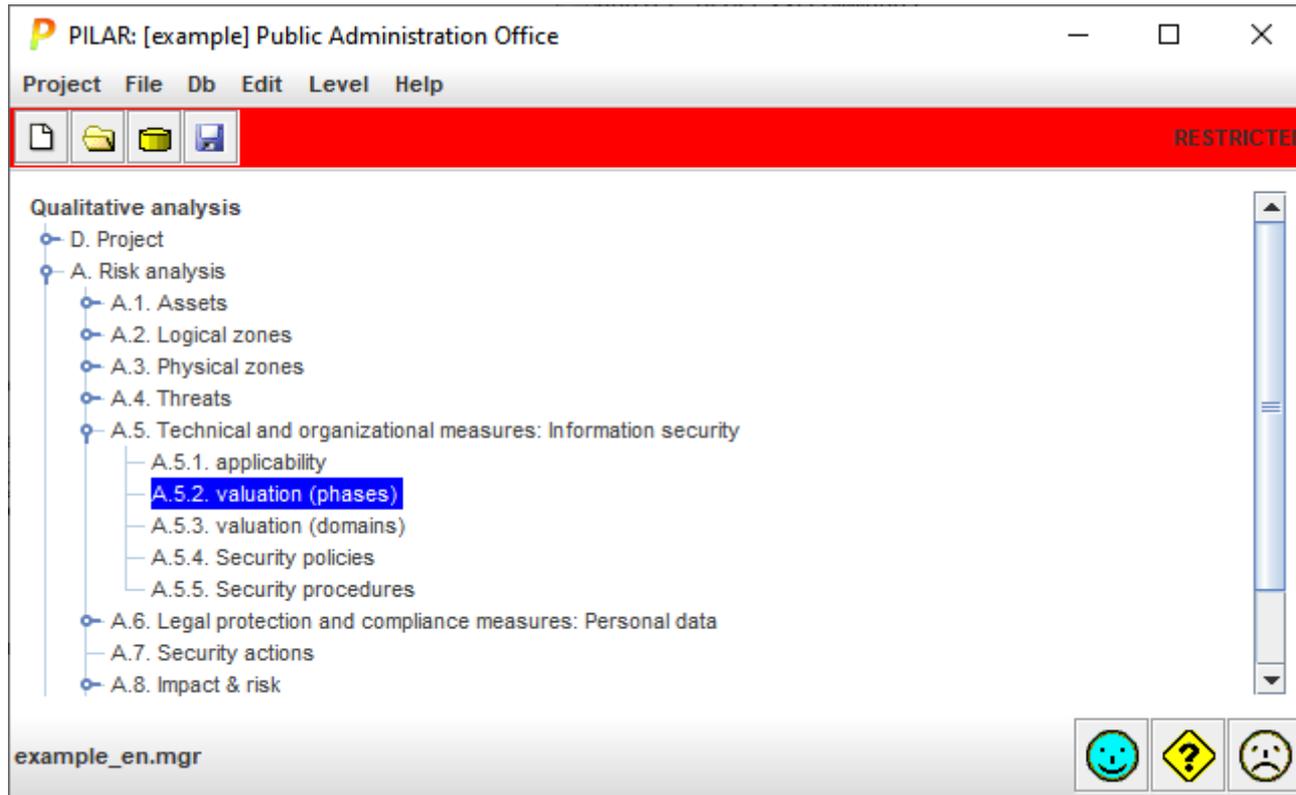
- by security domain

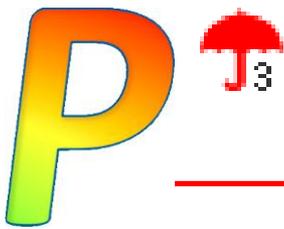
- maturity suggestions

- by security domain



# safeguards by domain





# structural recommendations

1. select one domain (blue band above)

[example] risk analysis > safeguards > edit\_safeguards

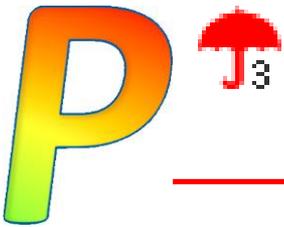
Edit Expand View Export Import Statistics

[base] corporate network Information sources

	as...	top	re...	safeguard	do...	so...	ap...	co...	cu...	tar...	Pl...
				SAFEGUARDS							
	M	EL	8	[M] Identification and authentication					L1...	L3...	L2...
	T	EL	7	[M] Logical access control			...		L0...	L3...	L2...
	M	PR	7				...		L1...	L1...	L2...
	M	EL	8				...		L3	L4	L2...
	M	PR	6				...		L0...	L3...	L2...
	M	PR	7				...		L0...	L3...	L2...
	M	PR	7				...		L0...	L0...	L2...
	M	PR	9	[COM] Protection of Communications			...		L0...	L2...	L2...
	M	PR	9	[IP] Logical border protection system			...		L1	L3	n.a.
	M	PR	7	[MP] Protection of Media					L1...	L3...	L2...
	M	PR	6	[AUX] Auxiliary Means		ph...			L0...	L3...	L2...
	PHY	EL	6	[PPE] Physical protection of equipment			...		L2	L4...	L3...
	PHY	PR	6	[L] Protection of the installations		ph...	...		L0...	L3...	L2...
	PHY	EL	6	[PPS] Physical Perimeter Protection					L0...	L3...	L2...
	PER	PR	6	[PS] Personnel			n.a.		n.a.	n.a.	n.a.
	M	PR	5	[PDSI] Potentially dangerous services			...		L2	L4	L2...

structural recommendation

1 sources operation suggest find >>



# 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

[example] risk analysis > safeguards > edit\_safeguards

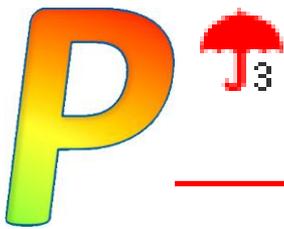
Edit Expand View Export Import Statistics

[base] corporate network Information sources

	as...	top	re...		safeguard	do...	so...	ap...	co...	cu...	tar...	Pl...	
					SAFEGUARDS						-L5	-L5	L2...
	M	EL	8		[IA] Identification and authentication						-L4	-L4	L2...
	T	EL	7		[AC] Logical access control			...			-L5	-L5	L2...
	M	PR	7		[D] Protection of Data / Information			...			L1...	L1...	L2...
	M	AD	3		[D.1] There is an inventory of information assets						L2...	L5	L3
	M	std	4		[D.2] Regulations						L1...	L5	L2...
	M	PR	6		[D.3] Security attributes						L1	L4	L4
	M	PR			[D.] Integrity guarantees			n.a.		n.a.	n.a.	n.a.	
	M	PR	5		[D.5] Confidentiality protection			...			L1...	L3...	L2...
	M	RC	7		[D.backup] Backup copies of the data			...			L1...	L5	L3...
	T	EL	6		[D.DS] Usage of electronic signatures						L1...	L1...	L2...
	M	IM	5		[D.TS] Usage of time stamping services						L2	L4	L2...
	M	EL	8		[K] Protecting cryptographic keys			...			L3	L4	L2...
	M	PR	6		[S] Protection of Services			...			-L5	-L5	L2...
	M	PR	7		[SW] Protection of Software						-L5	-L5	L2...
	M	PR	7		[HW] Protection of Hardware			...			-L2	-L5	L2...
	M	PR	9		[COM] Protection of Communications			...			-L3	-L5	L2...
	M	PR			[IP] Logical border protection system			...					n.a.
	M	PR	7		[MP] Protection of Media						L1...	L3...	L2...
	M	PR	6		[AUX] Auxiliary Means		ph...				L0...	L3...	L2...
	PHY	EL	6		[PPE] Physical protection of equipment			...			L2	L4...	L3...
	PHY	PR	6		[L] Protection of the installations		ph...	...			L0...	L3...	L2...
	PHY	EL	8		[PPS] Physical Perimeter Protection						-L2	-L5	L2...
	PER	PR			[PS] Personnel			n.a.		n.a.	n.a.	n.a.	
	M	PR	5		[PDS] Potentially dangerous services			...			L2	L4	L2...
	M	CR	6		[IR] Incident management (ICT)						L0...	L3...	L2...
	T	PR	8		[tools] Security tools			...			-L2	-L5	L2...

- 1 + sources operation suggest find >>

suggestion



# structural recommendations

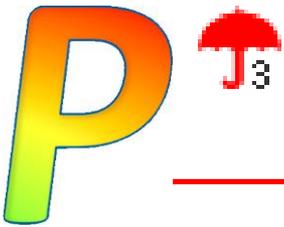
[example] risk analysis > safeguards > edit\_safeguards

Edit Expand View Export Import Statistics

[base] corporate network Information sources

	as...	top	re...		safeguard	do...	so...	ap...	co...	cu...	tar...	Pl...
<input type="checkbox"/>	M	PR	7		[D] Protection of Data / Information			...		_-L5	_-L5	L2...
<input type="checkbox"/>	M	AD	3		[D.1] There is an inventory of information assets					L2...	L5	L3
<input type="checkbox"/>	M	std	4		[D.2] Regulations					L1...	L5	L2...
<input type="checkbox"/>	M	PR	6		[D.3] Security attributes					L1	L4	L4
<input type="checkbox"/>	M	PR			[D.4] Integrity guarantees			n.a.		n.a.	n.a.	n.a.
<input type="checkbox"/>	M	PR	5		[D.5] Confidentiality protection			...		_-L2	_-L4	L2...
<input type="checkbox"/>	M	PR	5		[D.C] Encryption of information					_-L2	_-L4	L2...
<input type="checkbox"/>	M	std	2		[D.C.1] There is a policy for the use of cryptographic controls					L2	L4	L2
<input type="checkbox"/>	M	proc	2		[D.C.2] There are procedures for information encryption					L2	L4	L2
<input type="checkbox"/>	M	AD	2		[D.C.3] Persons are assigned to responsibilities					L2	L4	L2
<input type="checkbox"/>	T	EL	5		[D.C.4] Encryption mechanism					_-L2	_-L4	L3
<input type="checkbox"/>	T	EL	5		[D.C.4.1] {xor} Options							L3
<input type="checkbox"/>	T	EL	5		[D.C.4.1.1] {xor} Shared secret (symmetric encryption)					[ ]	[ ]	[ L...
<input type="checkbox"/>	T	EL	2 (u)		[D.C.4.1.1.1] DES (56 bits) or equivalent					n.s.	n.s.	L2
<input type="checkbox"/>	T	EL	3 (u)		[D.C.4.1.1.2] 3DES (112 bits) or equivalent					n.s.	n.s.	L3
<input type="checkbox"/>	T	EL	4 (u)		[D.C.4.1.1.3] AES-128 (128 bits) or equivalent					n.s.	n.s.	L3
<input type="checkbox"/>	T	EL	5		[D.C.4.1.1.4] AES-192 (192 bits) or equivalent					[ ]	[ ]	[ L...
<input type="checkbox"/>	T	EL	4 (o)		[D.C.4.1.1.5] AES-256 (256 bits) or equivalent					n.s.	n.s.	L3
<input type="checkbox"/>	T	EL	5		[D.C.4.1.2] {xor} Public key cryptography RSA (+ session key)					n.s.	n.s.	L3

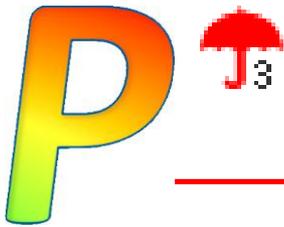
suggestion - 1 + sources operation suggest find >>



# 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 too easy to ignore by convenience
    - **residual risk may be falsely low because of obviating important protection measures**



# how to proceed

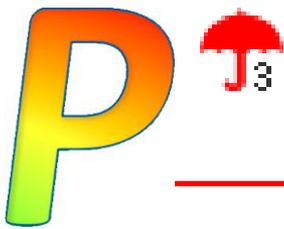
- with respect to selection
  - you may need to change selection to reflect real facts

5		☺ ☂ <sub>2</sub> [D.C.4] Encryption mechanism							L2	L2-...	L3
5		☺ ☂ <sub>1</sub> [D.C.4.1] {xor} Options							L2	L2	L3
5		☺ ☂ <sub>1</sub> [D.C.4.1.1] {xor} Shared secret (symmetric encryption)							[L2]	[L2]	[L3]
2 (u)		☺ ☂ <sub>1</sub> [D.C.4.1.1.1] DES (56 bits) or equivalent							[L2]	[L2]	L2
3 (u)		☺ ☂ <sub>1</sub> [D.C.4.1.1.2] 3DES (112 bits) or equivalent							n.s.	n.s.	L3
4 (u)		☺ ☂ <sub>1</sub> [D.C.4.1.1.3] AES-128 (128 bits) or equivalent							n.s.	n.s.	L3
5		☺ ☂ <sub>1</sub> [D.C.4.1.1.4] AES-192 (192 bits) or equivalent							n.s.	n.s.	[L3]
4 (o)		☺ ☂ <sub>1</sub> [D.C.4.1.1.5] AES-256 (256 bits) or equivalent							n.s.	n.s.	L3

5		☺ ☂ <sub>2</sub> [D.C.4] Encryption mechanism							L2-...	L3-...	L3
5		☺ ☂ <sub>1</sub> [D.C.4.1] {xor} Options							L3	L3	L3
5		☺ ☂ <sub>1</sub> [D.C.4.1.1] {xor} Shared secret (symmetric encryption)							[L3]	[L3]	[L3]
2 (u)		☺ ☂ <sub>1</sub> [D.C.4.1.1.1] DES (56 bits) or equivalent							n.s.	n.s.	L2
3 (u)		☺ ☂ <sub>1</sub> [D.C.4.1.1.2] 3DES (112 bits) or equivalent							n.s.	n.s.	L3
4 (u)		☺ ☂ <sub>1</sub> [D.C.4.1.1.3] AES-128 (128 bits) or equivalent							[L3]	[L3]	L3
5		☺ ☂ <sub>1</sub> [D.C.4.1.1.4] AES-192 (192 bits) or equivalent							n.s.	n.s.	[L3]
4 (o)		☺ ☂ <sub>1</sub> [D.C.4.1.1.5] AES-256 (256 bits) or equivalent							n.s.	n.s.	L3

5		☺ ☂ <sub>2</sub> [D.C.4] Encryption mechanism							L2-...	L3-...	L3
5		☺ ☂ <sub>1</sub> [D.C.4.1] {xor} Options							L3	L3	L3
5		☺ ☂ <sub>1</sub> [D.C.4.1.1] {xor} Shared secret (symmetric encryption)							[L3]	[L3]	[L3]
2 (u)		☺ ☂ <sub>1</sub> [D.C.4.1.1.1] DES (56 bits) or equivalent							n.s.	n.s.	L2
3 (u)		☺ ☂ <sub>1</sub> [D.C.4.1.1.2] 3DES (112 bits) or equivalent							n.s.	n.s.	L3
4 (u)		☺ ☂ <sub>1</sub> [D.C.4.1.1.3] AES-128 (128 bits) or equivalent							[L3]	n.s.	L3
5		☺ ☂ <sub>1</sub> [D.C.4.1.1.4] AES-192 (192 bits) or equivalent							n.s.	n.s.	[L3]
4 (o)		☺ ☂ <sub>1</sub> [D.C.4.1.1.5] AES-256 (256 bits) or equivalent							n.s.	[L3]	L3

suggestions



# maturity

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

[example] risk analysis > safeguards

Edit Expand View Export Import

[base] corporate network

**maturity recommendation**

	asp...	top	rec...		do...	so...	ap...	co...	cu...	tar...	PIL...
				SAFEGUARDS							
<input type="checkbox"/>	M	EL	8	 [A] Identification and authentication						_-L5	_-L5 L2-...
<input type="checkbox"/>	T	EL	7	 [AC] Logical access control			...			_-L4	_-L4 L2-...
<input type="checkbox"/>	M	PR	7	 [D] Protection of Data / Information			...			L0-...	L1-... L2-...
<input type="checkbox"/>	M	AD	3	 [D.1] There is an inventory of information assets						L2-...	L5 L3
<input type="checkbox"/>	M	std	4	 [D.2] Regulations						L1-...	L5 L2-...
<input type="checkbox"/>	M	PR	6	 [D.3] Security attributes						L1	L4 L4
<input type="checkbox"/>	M	PR		 [D.4] Integrity guarantees			n.a.		n.a.	n.a.	n.a.
<input type="checkbox"/>	M	PR	5	 [D.5] Confidentiality protection			...			L0-...	L3-... L2-...
<input type="checkbox"/>	M	RC	7	 [D.backup] Backup copies of the data			...			L1-...	L5 L3-...
<input type="checkbox"/>	T	EL	6	 [D.DS] Usage of electronic signatures						L1-...	L1-... L2-...
<input type="checkbox"/>	T	std	2	 [D.DS.1] There is a policy on electronic signatures						L2	L3 L2
<input type="checkbox"/>	T	proc	2	 [D.DS.2] There are procedures for the usage of electronic signatures						L3	L3 L2
<input type="checkbox"/>	T	AD	2	 [D.DS.3] Persons are assigned to responsibilities						L3	L3 L2
<input type="checkbox"/>	T	PR	3	 [D.DS.4] The probative value of the signature is guaranteed						L2	L2 L3
<input type="checkbox"/>	T	EL	5	 [D.DS.5] {xor} Electronic certificate						L3	L3 L3
<input type="checkbox"/>	T	EL	5	 [D.DS.6] {xor} Algorithm implementation						L3	L3 L3
<input type="checkbox"/>	T	EL	6	 [D.DS.7] {xor} Digital signature mechanism						L3	L3 L4
<input type="checkbox"/>	T	AD	3	 [D.DS.8] Algorithm vulnerabilities are regularly reviewed						L3	L3 L3
<input type="checkbox"/>	T	cert	4	 [D.DS.9] Certified / accredited algorithms are used						L2	L3 L3
<input type="checkbox"/>	T	cert	5	 [D.DS.a] Certified products or services are used						L1	L1 L3
<input type="checkbox"/>	M	IM	5	 [D.TS] Usage of time stamping services						L2	L4 L2-...

1 sources operation suggest find >> [icons]

suggestions



# how to proceed

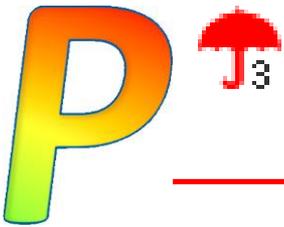
---

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

asp...	top	rec...		safeguard	do...	so...	ap...	co...	cu...	tar...	PIL...
--------	-----	--------	--	-----------	-------	-------	-------	-------	-------	--------	--------

-  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)

[example] risk analysis > safeguards > edit\_safeguards

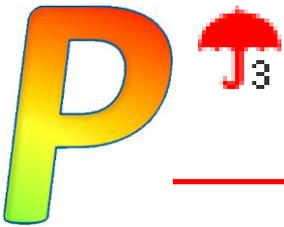
Edit Expand View Export Import Statistics

[base] corporate network Information sources

	as...	top	re...		safeguard	do...	so...	ap...	co...	cu...	tar...	Pl...
SAFEGUARDS												
<input type="checkbox"/>	M	EL	8		[A] Identification and authentication					L1...	L3...	L2...
<input type="checkbox"/>	T	EL	7		[AC] Logical access control			...		L0...	L3...	L2...
<input type="checkbox"/>	M	PR	7		[D] Protection of Data / Information			...		L1...	L1...	L2...
<input type="checkbox"/>	M	EL	8		[K] Protecting cryptographic keys			...		L3	L4	L2...
<input type="checkbox"/>	M	PR	6		[S] Protection of Services			...		L0...	L3...	L2...
<input type="checkbox"/>	M	PR	7		[SW] Protection of Software			...		L0...	L3...	L2...
<input type="checkbox"/>	M	PR	7		[HW] Protection of Hardware			...		L0...	L0...	L2...
<input type="checkbox"/>	M	PR	7		[S] Protection of Services			...		L0...	L2...	L2...
<input type="checkbox"/>	M	PR	7		[S] Protection of Services			...		L1	L3	n.a.
<input type="checkbox"/>	M	PR	7		[S] Protection of Services			...		L1...	L3...	L2...
<input type="checkbox"/>	M	PR	7		[S] Protection of Services			ph...		L0...	L3...	L2...
<input type="checkbox"/>	PHY	EL	6		[L] Protection of Locations			...		L2	L4...	L3...
<input type="checkbox"/>	PHY	PR	6		[L] Protection of Locations			ph...		L0...	L3...	L2...
<input type="checkbox"/>	PHY	EL	6		[PPS] Physical Perimeter Protection					L0...	L3...	L2...
<input type="checkbox"/>	PER	PR	7		[PS] Personnel			n.a.		n.a.	n.a.	n.a.
<input type="checkbox"/>	M	PR	5		[PDS] Potentially dangerous services			...		L2	L4	L2...

sugg - 1 + sources operation suggest find >>

maturity recommendation



# maturity

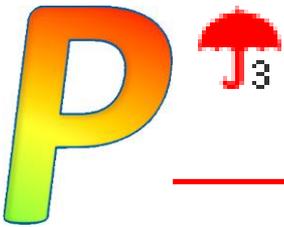
1. select the type(s) of protection you are looking for

**P** type of protection

Type of protection

- [X] likelihood
  - [X] [PR] prevention
  - [X] [DR] deterrence
  - [X] [EL] elimination
- [X] impact
  - [X] [IM] impact minimization
  - [X] [CR] correction
  - [X] [RC] recovery
- [X] administration
  - [X] [DC] detection
  - [X] [MN] monitoring
  - [X] [AW] awareness
  - [X] [AD] administrative
- [X] [std] poli...
- [X] [proc] procedu...
- [X] [cert] certifications / accreditatio...



# maturity recommendation

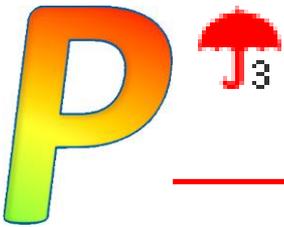
1. recommendations are sorted by first column index number
2. click on the suggestion to center it on the upper panel
3. these recommendations apply to the whole security domain

The screenshot shows a window titled "[example] risk analysis > safeguards > edit\_safeguards". The window has a menu bar with "Edit", "Expand", "View", "Export", "Import", and "Statistics". Below the menu bar is a header bar with "[base] corporate network" and "Information sources". The main area contains a table with columns: "as...", "top", "re...", "safeguard", "do...", "so...", "ap...", "co...", "cu...", "tar...", and "Pl...". The table lists several safeguards, including "[tools.CM] CM: Continuous monitoring", "[tools.AV] Tool against harmful code (malware)", and "[tools.AV.1] There are protection measures for harmful code". Below the table is a list of suggestions, with the first one, "5.3 :: [tools.AV.4] Virus database is continuously updated", highlighted by a red box. The bottom of the window has a toolbar with buttons for "sources", "operation", "suggest", "find", and several icons.

	as...	top	re...	safeguard	do...	so...	ap...	co...	cu...	tar...	Pl...
<input type="checkbox"/>	T	EL	7	[tools.CM] CM: Continuous monitoring					L0	L4	L3...
<input type="checkbox"/>	T	EL	8	[tools.AV] Tool against harmful code (malware)					L2	L3	L3...
<input type="checkbox"/>	T	std	4	[tools.AV.1] There are protection measures for harmful code					L2	L3	L3
<input type="checkbox"/>	T	std	5	[tools.AV.2] There is a policy for gathering information about new viruses (mail lists, web page access, etc.)					L2	L3	L3
<input type="checkbox"/>	T	PR	6	[tools.AV.3] Up-to-date software maintenance					L2	L3	L4
<input type="checkbox"/>	T	PR	8	[tools.AV.4] Virus database is continuously updated					L2	L3	L5

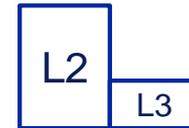
5.3 :: [tools.AV.4] Virus database is continuously updated  
5.3 :: [tools.AV.7] Programs and services are reviewed during boot  
5.1 :: [tools.AV.d] Scanning of files received on removable computer storage media  
5.1 :: [tools.AV.9] Scanning of e-mail attachments  
5.1 :: [tools.AV.c] Scanning of downloaded files  
5.1 :: [tools.AV.3] Up-to-date software maintenance  
5.0 :: [IA.6] Trusted authentication path

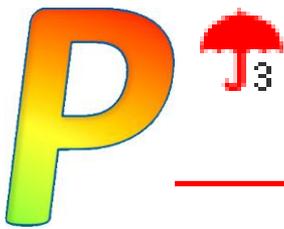
sugg



# 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

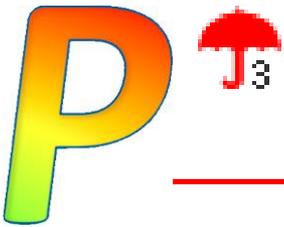
[example] impact & risk > risk.down

View Export

potential current target PILAR

	asset	[A]	[I]	[C]	[Auth]	[Acc]	[V]	[PD]
<input type="checkbox"/>	ASSETS	{4.4}	{6.3}	{6.4}	{6.9}	{5.6}		{2.4}
<input type="checkbox"/>	[B] Essential assets: information and services	{3.8}	{3.7}	{4.6}	{5.2}	{5.6}		{2.4}
<input type="checkbox"/>	[it] [INFO] Current files							{2.4}
<input type="checkbox"/>	[S] [S_in_person] In person processing	{3.8}	{3.7}	{4.6}	{5.2}	{5.6}		
<input type="checkbox"/>	[S] [S_remote] Remote processing	{3.8}	{3.7}	{4.6}	{5.2}	{5.6}		
<input type="checkbox"/>	[IS] Internal services	{3.8}	{5.2}	{6.4}	{6.9}	{5.6}		
<input type="checkbox"/>	[A] [https] SSL access	{3.8}	{5.2}	{6.4}	{6.9}			
<input type="checkbox"/>	[A] [email] electronic messaging	{3.8}	{3.7}	{4.6}	{5.2}	{5.6}		
<input type="checkbox"/>	[A] [archive] Central archive	{3.8}	{4.3}	{6.4}	{6.9}	{5.6}		
<input type="checkbox"/>	[E] Equipment	{4.4}	{6.3}	{6.4}	{6.0}			
<input type="checkbox"/>	[SW] Applications	{3.4}	{3.5}	{5.2}				
<input type="checkbox"/>	[A] [SW_app] Processing of files	{3.4}	{3.5}	{5.2}				
<input type="checkbox"/>	[HW] Hardware	{3.7}	{6.3}	{6.4}	{6.0}			
<input type="checkbox"/>	[A] [PC] Work positions	{3.2}	{5.8}	{6.4}	{6.0}			
<input checked="" type="checkbox"/>	[A] [SRV] Server	{3.7}	{6.3}	{6.4}	{6.0}			
<input type="checkbox"/>	[COM] Communications	{4.4}	{5.4}	{4.6}	{5.9}			

sugg - 4 + 1 domain source manage legend ?



# 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

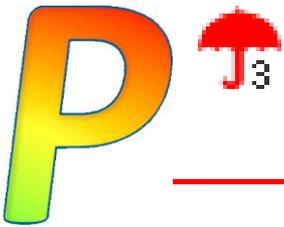
[example] impact & risk > risk.down

View Export

potential current target PILAR

	asset	[A]	[I]	[C]	[Auth]	[Acc]	[V]	[PD]
<input type="checkbox"/>	ASSETS	{4.4}	{6.3}	{6.4}	{6.9}	{5.6}		{2.4}
<input type="checkbox"/>	[B] Essential assets: information and services	{3.8}	{3.7}	{4.6}	{5.2}	{5.6}		{2.4}
<input type="checkbox"/>	[it] [INFO] Current files							{2.4}
<input type="checkbox"/>	[S] [S_in_person] In person processing	{3.8}	{3.7}	{4.6}	{5.2}	{5.6}		
<input type="checkbox"/>	[S] [S_remote] Remote processing	{3.8}	{3.7}	{4.6}	{5.2}	{5.6}		
<input type="checkbox"/>	[IS] Internal services	{3.8}	{5.2}	{6.4}	{6.9}	{5.6}		
<input type="checkbox"/>	[A] [https] SSL access	{3.8}	{5.2}	{6.4}	{6.9}			
<input type="checkbox"/>	[A] [email] electronic messaging	{3.8}	{3.7}	{4.6}	{5.2}	{5.6}		
<input type="checkbox"/>	[A] [archive] Central archive	{3.8}	{4.3}	{6.4}	{6.9}	{5.6}		
<input type="checkbox"/>	[E] Equipment	{4.4}	{6.3}	{6.4}	{6.0}			
<input type="checkbox"/>	[SW] Applications	{3.4}	{3.5}	{5.2}				
<input type="checkbox"/>	[A] [SW_app] Processing of files	{3.4}	{3.5}	{5.2}				
<input type="checkbox"/>	[HW] Hardware	{3.7}	{6.3}	{6.4}	{6.0}			
<input type="checkbox"/>	[A] [PC] Work positions	{3.2}	{5.8}	{6.4}	{6.0}			
<input checked="" type="checkbox"/>	[A] [SRV] Server	{3.7}	{6.3}	{6.4}	{6.0}			
<input type="checkbox"/>	[COM] Communications	{4.4}	{5.4}	{4.6}	{5.9}			

sugg - 4 + 1 domain source manage legend ?



# safeguards for some risks /3

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

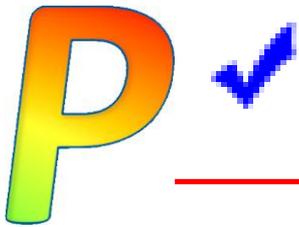
[example] impact & risk > risk.down > edit\_safeguards

Edit Expand View Export Import Statistics

[base] corporate network Information sources

	as...	top	re...		safeguard	do...	so...	ap...	co...	cu...	tar...	Pl...
					SAFEGUARDS						L0... L1... L2...	
<input type="checkbox"/>	M	EL	8		[A] Identification and authentication						L1... L3... L2...	
<input type="checkbox"/>	T	EL	7		[AC] Logical access control			...			L0... L3... L2...	
<input type="checkbox"/>	M	PR	6		[D] Protection of Data / Information			...			L1... L1... L2...	
<input type="checkbox"/>	M	EL			[K] Protecting cryptographic keys			...			L3 L4 L2...	
<input type="checkbox"/>	M	PR			[S] Protection of Services			...			L0... L3... L2...	
<input type="checkbox"/>	M	PR	7		[SW] Protection of Software						L0... L3... L2...	
<input type="checkbox"/>	M	PR	7		[HW] Protection of Hardware			...			L0... L1... L2...	
<input type="checkbox"/>	M	PR			[COM] Protection of Communications			...			L0... L2... L2...	
<input type="checkbox"/>	M	PR			[IP] Logical border protection system			...			L1 L3 n.a.	
<input type="checkbox"/>	M	PR	7		[MP] Protection of Media						L1... L3... L2...	
<input type="checkbox"/>	M	PR	5		[AUX] Auxiliary Means		ph...				L0... L3... L2...	
<input type="checkbox"/>	PHY	EL	6		[PPE] Physical protection of equipment			...			L2 L4... L3...	
<input type="checkbox"/>	PHY	PR			[L] Protection of the installations		ph...	...			L0... L3... L2...	
<input type="checkbox"/>	PHY	EL			[PPS] Physical Perimeter Protection						L0... L3... L2...	
<input type="checkbox"/>	PER	PR			[PS] Personnel			n.a.			n.a. n.a. n.a.	
<input type="checkbox"/>	M	PR			[PDSI] Potentially dangerous services						L2 L4 L2...	

sugg - 1 + sources operation suggest find >>



# controls by domain

PILAR: [example] Public Administration Office

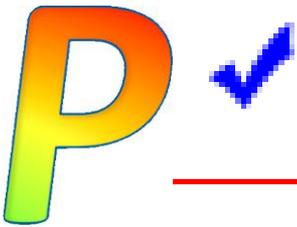
Project File Db Edit Level Help

RESTRICTED

Qualitative analysis

- D. Project
- A. Risk analysis
- R. Reports
- E. Security profiles
  - select
  - [27002:2013] Code of practice for information security controls
    - valuation**
    - groupings
  - [GDPR:2016] REGULATION on the protection of natural persons with regard to the processing of personal data
  - [29151:2017] Code of practice for personally identifiable information protection
  - others ...
  - compare profiles

example\_en.mgr



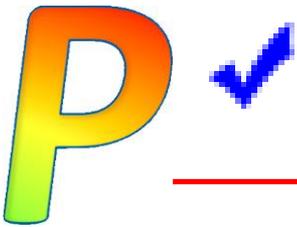
# structural recommendations

1. select one domain (blue band above)

structural recommendation

	rec...		so...	ap...	co...	current	target	PILAR
		[27002:2013] Co... controls				L0-L5 ...	L3-L5 ...	L2-L5
	2	♀ ✓ [5] INFORMATION SECURITY POLICIES				L0	L5	L2
	2	♂ ✓ [5.1] MANAGEMENT DIRECTION FOR INFORMATION SECURITY				L0	L5	L2
	7	♀ ✓ [6] ORGANIZATION OF INFORMATION SECURITY		...		L0-L5 ...	L4-L5	L2-L4
	7	♂ ✓ [6.1] INTERNAL ORGANIZATION				L0-L5 ...	L4-L5	L2-L4
		♂ ✓ [6.2] MOBILE DEVICES AND TELEWORKING		n.a.				
		♂ ✓ [7] HUMAN RESOURCE SECURITY				n.a.	n.a.	n.a.
	7	♀ ✓ [8] ASSET MANAGEMENT		...		L1-L2 ...	L4-L5 ...	L2-L4
	4	♂ ✓ [8.1] RESPONSIBILITY FOR ASSETS		...		L2 (L0...	L4-L5 ...	L2-L3
	6	♂ ✓ [8.2] INFORMATION CLASSIFICATION				L1-L2	L4-L5	L3-L4 ...
	7	♂ ✓ [8.3] MEDIA HANDLING				L2 (L1...	L4 (L3...	L3-L4 ...
	8	♀ ✓ [9] ACCESS CONTROL				L0-L4 ...	L3-L5 ...	L2-L5 ...
	4	♂ ✓ [9.1] BUSINESS REQUIREMENTS FOR ACCESS CONTROL				L1 (L1...	L4-L5	L2-L3
	7	♂ ✓ [9.2] USER ACCESS MANAGEMENT				L0-L4 ...	L3-L5 ...	L2-L4

- 1 +    +1    domains    suggest    [save icon] [happy face] [question mark] [sad face]

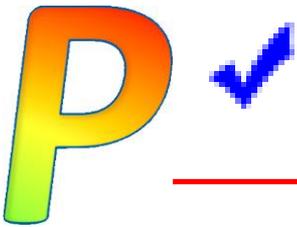


# structural recommendations

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

The screenshot shows a software window titled "[example] 27002:2013 > valuation". The interface includes a menu bar with options: Edit, Expand, View, Export, Import, Statistics, Select, Graphs. Below the menu is a search bar containing "[base] corporate network" and "Information sources". The main area is a table with columns: rec..., control, do..., so..., ap..., co..., current, target, and PILAR. The table lists various security controls with their current and target ratings. A bottom toolbar contains a numeric input field (set to 4), a checkbox (+1), a "domains" button, a "suggest" button, and several icons (save, smile, question mark, sad face).

rec...	control	do...	so...	ap...	co...	current	target	PILAR
<input type="checkbox"/> 8	♀ ✓ [11] PHYSICAL AND ENVIRONMENTAL SECURITY					L0-L4 ...	L3-L5	L3-L5 ...
<input type="checkbox"/> 8	♀ ✓ [11.1] SECURE AREAS					L1-L4 ...	L3-L4 ...	L3-L5 ...
<input type="checkbox"/> 6	♀ ✓ [11.1.1] Physical security perimeter					L4 (L2)	L4 (L3)	L4 (L3...)
<input type="checkbox"/> 5	♂ [PPS.3] Doors					L2	L3	L3
<input type="checkbox"/> 5 (u)	♂ [PPS.4] Windows					L2	L3	L3
<input type="checkbox"/> 6	♂ [PPS.6] External walls					L2	L3	L3-L4
<input type="checkbox"/> 4	♂ [L.AC.1] Access via reception area					L2	L3	L3
<input type="checkbox"/> 3	♂ [PPS.2.6] Separation of areas managed by others					L2	L3	L3
<input type="checkbox"/> 4	♂ [L.AC.9] Emergency exits guarantee that only authorised personnel can gain access to installations					L2	L3	L3



# 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

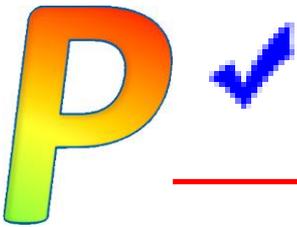
[example] 27002:2013 > valuation

Edit Expand View Export Import Statistics Select Graphs

[base] corporate network Information sources

	rec...		control	do...	so...	ap...	co...	current	target	PILAR
<input type="checkbox"/>			[27002:2013] Code of practice for information security controls					L0-L5 ...	L3-L5 ...	L2-L5
<input type="checkbox"/>	2	♀	✓ [5] INFORMATION SECURITY POLICIES					L0	L5	L2
<input type="checkbox"/>	2	♀	✓ [5.1] MANAGEMENT DIRECTION FOR INFORMATION SECURITY					L0	L5	L2
<input type="checkbox"/>	7	♀	✓ [6] ORGANIZATION OF INFORMATION SECURITY			...		L0-L5 ...	L4-L5	L2-L4
<input type="checkbox"/>	7	♀	✓ [6.1] INTERNAL ORGANIZATION					L0-L5 ...	L4-L5	L2-L4
<input type="checkbox"/>			✓ [6.2] MOBILE DEVICES AND TELEWORKING			n.a.				
<input type="checkbox"/>		♀	✓ [7] HUMAN RESOURCE SECURITY					n.a.	n.a.	n.a.
<input type="checkbox"/>	7	♀	✓ [8] ASSET MANAGEMENT			...		L1-L2 ...	L4-L5 ...	L2-L4
<input type="checkbox"/>	4	♀	✓ [8.1] RESPONSIBILITY FOR ASSETS			...		L2 (L0...	L4-L5 ...	L2-L3
<input type="checkbox"/>	6	♀	✓ [8.2] INFORMATION CLASSIFICATION					L1-L2	L4-L5	L3-L4 ...
<input type="checkbox"/>	7	♀	✓ [8.3] MEDIA HANDLING					L2 (L1...	L4 (L3...	L3-L4 ...
<input type="checkbox"/>	8	♀	✓ [9] ACCESS CONTROL					L0-L4 ...	L3-L5 ...	L2-L5 ...
<input type="checkbox"/>	4	♀	✓ [9.1] BUSINESS REQUIREMENTS FOR ACCESS CONTROL					L1 (L1...	L4-L5	L2-L3
<input type="checkbox"/>	7	♀	✓ [9.2] USER ACCESS MANAGEMENT					L0-L4 ...	L3-L5 ...	L2-L4

sugg - 1 + +1 domains suggest



# structural recommendations

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

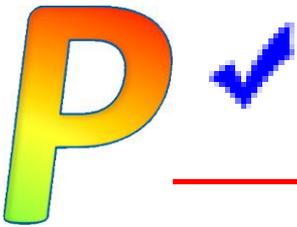
[example] 27002:2013 > valuation

Edit Expand View Export Import Statistics Select Graphs

[base] corporate network Information sources

rec...	control	do...	so...	ap...	co...	current	target	PILAR
	♀ ✓ [8.3] MEDIA HANDLING			n.a.				
	♀ ✓ [8.3.1] Management of removable media			n.a.				
5	• [MP.clean] Secure contents erasure					L2	L4	L2-L3
5	• [MP.2] Media management					L2	L4	L2-L3
5	• [MP.cont] Availability					L2	L4	L3
7	• [MP.IC] Cryptographic protection of contents (media)					L1-L2	L3-L4	L2-L4
	♀ ✓ [8.3.2] Disposal of media			n.a.				
5	• [MP.clean] Secure contents erasure					L2	L4	L2-L3
5	• [MP.end] Destruction of media					L2	L4	L2-L3
	♀ ✓ [8.3.3] Physical media transfer			n.a.				
5	• [MP.2.3] Transport of data media		ph...			L2	L4	L2-L3
4	• [MP.4] Protection of media off-site					L2	L4	L2-L3

- 1 +    domains    suggest    [save icon] [smiley icon] [question mark icon] [sad face icon]

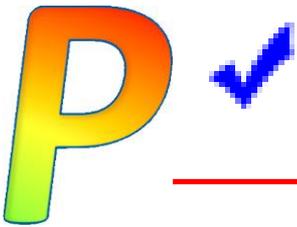


# structural recommendations

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

The screenshot shows a software interface with a table of controls. The table has columns for 'rec...', 'control', 'do...', 'so...', 'ap...', 'co...', 'current', 'target', and 'PILAR'. The 'control' column lists various security controls, some with expandable tree views. The 'current', 'target', and 'PILAR' columns contain numerical values or labels like 'L2', 'L4', 'L3', 'L1-L2', 'L3-L4', 'L2-L4', and '[ L3 ]'. The interface also includes a menu bar with options like 'Edit', 'Expand', 'View', 'Export', 'Import', 'Statistics', 'Select', and 'Graphs'. At the bottom, there are navigation buttons and a 'suggest' button.

rec...	control	do...	so...	ap...	co...	current	target	PILAR
	☺ ✓ [8.3] {xor} MEDIA HANDLING			n.a.				
	☺ ✓ [8.3_base] Base			n.a.				
	☺ ✓ [8.3.1] Management of removable media			n.a.				
5	☺ [MP.clean] Secure contents erasure					L2	L4	L2-L3
5	☺ [MP.2] Media management					L2	L4	L2-L3
5	☺ [MP.cont] Availability					L2	L4	L3
7	☺ [MP.IC] Cryptographic protection of contents (media)					L1-L2	L3-L4	L2-L4
	☺ ✓ [8.3.2] Disposal of media			n.a.				
5	☺ [MP.clean] Secure contents erasure					L2	L4	L2-L3
5	☺ [MP.end] Destruction of media					L2	L4	L2-L3
	☺ ✓ [8.3.3] Physical media transfer			n.a.				
5	☺ [MP.2.3] Transport of data media		ph...			L2	L4	L2-L3
4	☺ [MP.4] Protection of media off-site					L2	L4	L2-L3
5	☺ [8.3_2] Fully insulated system					[ L3 ]	[ L3 ]	L3



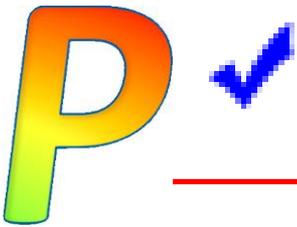
# maturity

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

**maturity recommendation**

rec...	current	target	PILAR
8	L2	L4	L3 (L3-)
4	L1 (L2-)	L5- (L4+)	L3- (L2...)
4	L1 (L2)	L4 (L5-)	L3 (L3-)
2	L1	L5 (L4)	L2
7	L2+	L4	L3
5	L2	L3	L3 (L3-)
3	L4 (L2+)	L4	L3 (L2+)
7	L2 (L2+)	L4 (L5-)	L4 (L3)
5	L2	L3+	L3-
3	L1 (L2)	L5 (L4)	L3
5	L4 (L4+)	L5	L3
8	L3	L3	L5
6	L2	L4	L3
4	L2	L3	L3
5	L0 (L0+)	L3 (L3+)	L3
6	L3	L3	L4 (L4-)
3	L3	L5	L3 (L3-)
5	L1	L5	L3 (L3-)

suggestions  +1 domains



# how to proceed

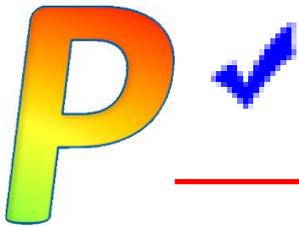
---

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

asp...	top	rec...		safeguard	do...	so...	ap...	co...	cu...	tar...	PIL...
--------	-----	--------	--	-----------	-------	-------	-------	-------	-------	--------	--------

-  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)

[example] 27002:2013 > valuation

Edit Expand View Export Import Statistics Select Graphs

[base] corporate network information sources

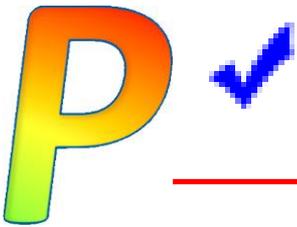
rec...	control	do...	so...	ap...	co...	current	target	PILAR
	[27002:2013] Code of practice for information security controls					L2	L4+	L3 (L3-)
2	♀ ✓ [5] INFORMATION SECURITY POLICIES					L0	L5	L2
2	♂ ✓ [5.1] MANAGEMENT DIRECTION FOR INFORMATION SECURITY					L0	L5	L2
7	♀ ✓ [6] ORGANIZATION OF INFORMATION SECURITY			...		L2+ (L2)	L5	L3 (L3-)
7	♂ ✓ [6.1] INTERNAL ORGANIZATION					L2+ (L2)	L5	L3 (L3-)
	♂ ✓ [6.2] MOBILE DEVICES AND TELEWORKING			n.a.				
	♀ ✓ [7] HUMAN RESOURCE SECURITY					n.a.	n.a.	n.a.
	♂ ✓ [7.1] PRIOR TO EMPLOYMENT					n.a.	n.a.	n.a.
	♂ ✓ [7.2] DURING EMPLOYMENT					n.a.	n.a.	n.a.
	♂ ✓ [7.3] TERMINATION					n.a.	n.a.	n.a.
7	♀ ✓ [8] ASS...			...		L2	L4+	L3 (L3-)
4	♂ ✓ [8.1] ...			...		L2	L4+	L3- (L2...)
6	♂ ✓ [8.2] ...					L2-	L4+	L3+ (L3)
	♂ ✓ [8.3] ...			n.a.				
8	♀ ✓ [9] ACC...					L2	L4	L3 (L3-)
4	♂ ✓ [9.1] BUSINESS REQUIREMENTS FOR CONTROL					L1 (L2-)	L5- (L4+)	L3- (L2...)
7	♂ ✓ [9.2] USER ACCESS MANAGEMENT					L2+	L4	L3
8	♂ ✓ [9.3] USER RESPONSIBILITIES					L3	L3	L5

suggestions

domains

suggest

maturity recommendation



# 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

[example] 27002:2013 > valuation

Edit Expand View Export Import Statistics Select Graphs

[base] corporate network information sources

rec...	control	do...	so...	ap...	co...	current	target	PILAR
	RESPONSIBILITIES							
8	[12.2] PROTECTION FROM MALWARE					L3 (L2-)	L3	L5 (L3)
7	[12.3] BACKUP					L3 (L3+)	L5	L4 (L3)
7	[12.4] LOGGING AND MONITORING					L3+ (L3-)	L5 (L4)	L3
7	[12.5] CONTROL OF OPERATIONAL SOFTWARE					L1	L5	L4 (L3)
6	[12.6] TECHNICAL VULNERABILITY MANAGEMENT					L1 (L1+)	L5	L4- (L3-)
5	[12.7] INFORMATION SYSTEMS AUDIT CONSIDERATIONS					L1 (L1-)	L3	L3
9	[13] COMMUNICATIONS SECURITY			...		L2	L4 (L3+)	L4- (L3)
9	[13.1] NETWORK SECURITY MANAGEMENT					L1+ (L2-)	L4 (L3)	L4 (L3)
5	[13.1.1] Network controls					L1 (L2-)	L4	L3
9	[13.1.2] Security of network services					L2	L4 (L3)	L5 (L3)
6	[13.1.3] Segregation in networks					L0	L4 (L2+)	L4 (L3+)

6.6 :: [11.2.3] enabling security

6.5 :: [13.1.3] Segregation in networks

6.5 :: [9.4.2] Secure log-on procedures

6.4 :: [SW.SC.] User accounts included by default in the products are removed or modified

6.3 :: [18.2.3] technical compliance inspection

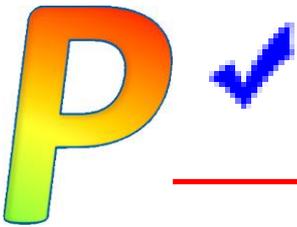
6.2 :: [11.2.4] equipment maintenance

6.2 :: [14.2.9] system acceptance testing

6.1 :: [17.1.3] verify, review and evaluate information security continuity

suggestions

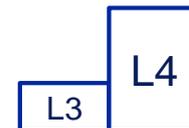
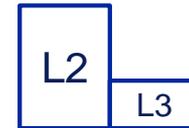
domains suggest



# 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



# P

# any question?

---



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

suggestions