Tailoring information security to business requirements

TRICK Service – A risk management tool

ADACOR Workshop
19th-21st April, 2016

Dr. Carlo Harpes

itrust consulting s.à r.l.
55, rue Gabriel Lippmann
L-6947 Niederanven

Tel: +352 2617 6212

Web: www.itrust.lu

Agenda

1. History and experience on R&D
2. ISO 27005 and its future
3. The tool TRICK Service
4. Ongoing TREsPASS contribution towards TRICK Cockpit

1. History and experience on R&D

Initial idea (2007):

- TRICK = “Tool for Risk management of an ISMS based on a Central Knowledge base”
- Fast, but quantitative risk evaluation
- Models security measures with risk reduction properties
- Integrate many standards
- Maintain parameters of many assessments in one central knowledge base
- Excel prototype

Support by BUGYO Beyond (CELTIC) (2008-2011)

- Asset-based version
- Use of tailored risk scenarios,
- Excel tables to be filled in, Excel Macros to compute ROSI
- Generation of risk treatment plans and statement of applicability for ISO 27001 certification
- Press release: «itrust a pu développer une méthodologie et un outil d’analyse de risques déjà en utilisation auprès de 6 organismes. Cet outil s’adresse à toute entreprise gérant des données personnelles ou sensibles et voulant formellement, mais rapidement chiffrer les risques et trouver les mesures de sécurisation appropriées».

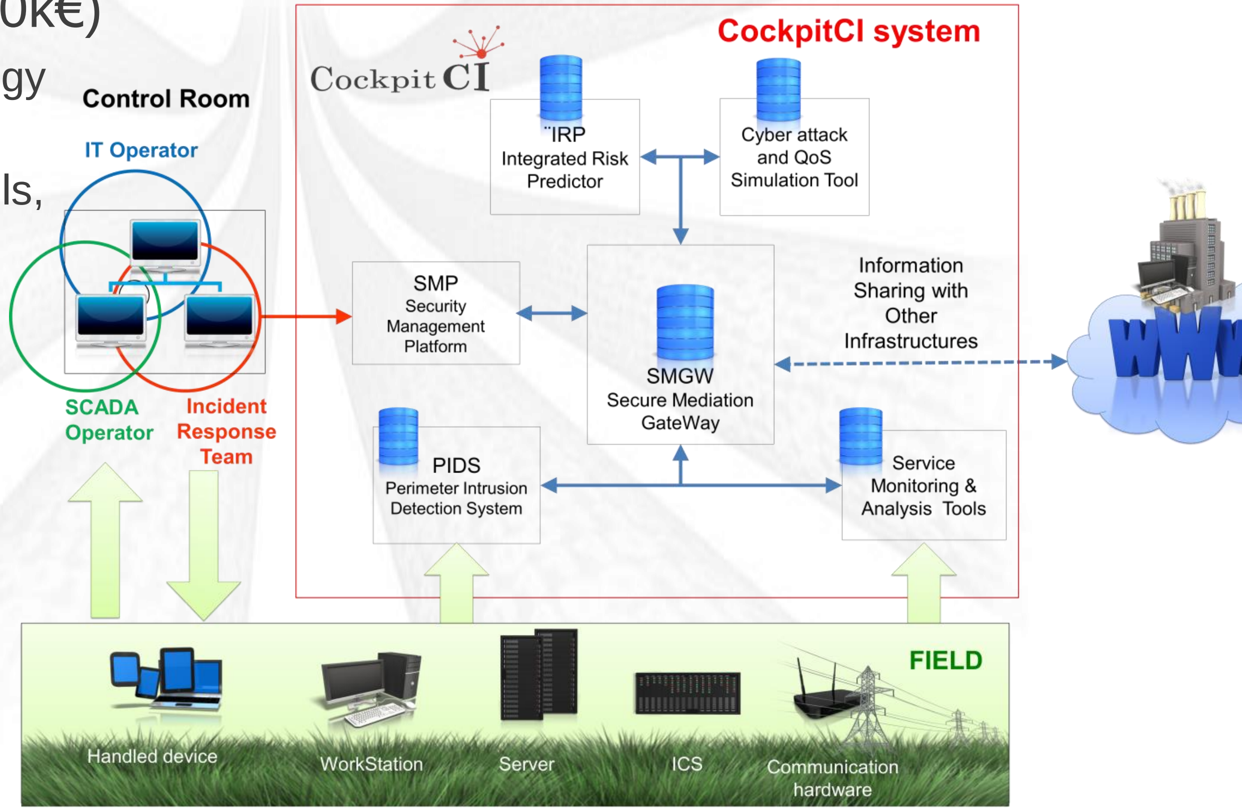
1. History and experience on R&D

Support by diamonds (ITEA2) (40k€)

- Maturity model (under publication)
- Migration to TRICK Service (Web based)

Support by CockpitCI (~40k€)

- Setup SCRUM methodology for development
- Add sector-specific controls, IEC 62433, 27019
- Idea of Cockpit and real-time.


Control Room
IT Operator
SCADA Operator
Incident Response Team
Cockpit CI
CockpitCI system
¨IRP
Integrated Risk Predictor
Cyber attack and QoS Simulation Tool
SMP
Security Management Platform
SMGW
Secure Mediation GateWay
Information Sharing with Other Infrastructures
PIDS
Perimeter Intrusion Detection System
Service Monitoring & Analysis Tools
FIELD
Handled device
WorkStation
Server
ICS
Communication hardware

Critical Infrastructure: e.g. electrical grid + SCADA network + Telecom network

1. History and experience on R&D

Support by TREsPASS (~100k€) (co-founded by FP7)

- New user interface
- Updates for CSSF
- Application of TS and Attack tree to the pseudonymisation service for EPSTAN
- Add multilingual or multi-context control information (easy imported via Excel)

Support by SmartGrid Luxembourg Cockpit (cofunded by eco.etat.lu)

- Towards real-time risk management applied to the LU smart-meter infrastructure

1. History and experience on R&D

SECaaS emerging from R&D

itrust consulting

TRICK Service is a driver for SECaas (SECurity as a Service):

- In support for ISO 27001 (ISMS) implementation in different sectors (CTIE, Energy, Cloud services, SME, …
- We needed several R&D projects and founding to came to an acceptable functionality level

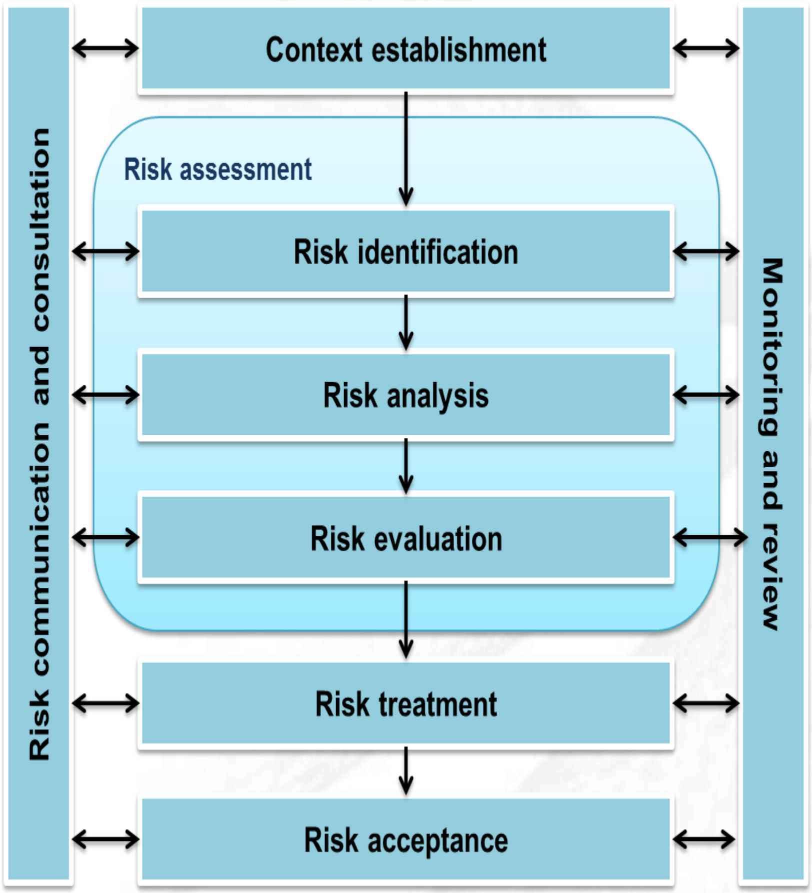
TRICK Service

Leassons Learned :

- Increased demande for formal Risk Assessments and Risk Management
- Not enough customer ask for security, i.e., insufficient deployment of security certification
- Need for effective security management
- Need for more communication and knowledge on cybersecurity
- Need for online risk monitoring
- Need for better tools, which are fully exploited...

2. Current status of ISO 27005

Methodology of RISK Service

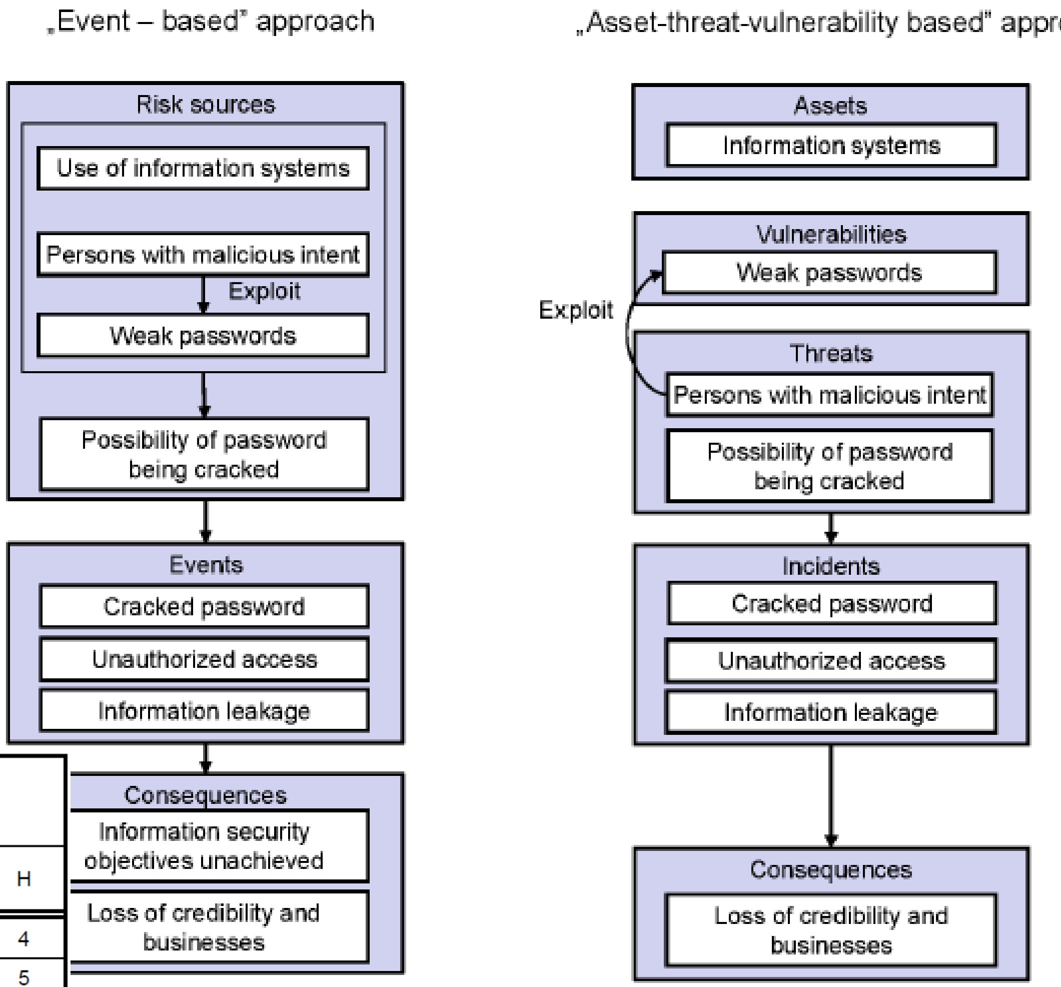


- **Follows the guidance of ISO 27005**
- **Is ISO 27001:2013 compliant**
- **Can be easily integrated in your Information Security Management System (ISMS)**
- **Prepares reporting to regulator (CSSF, CNPD)**

2. Current status of ISO 27005

Complicated ongoing discussion at SC27

- Need for future 27005 because of ISO 31000?
- Give up focus on assets
- Inconsistent illustation of qualitative assessments
- Risk = uncertainty on objecti i.e., can be an opportunity.



„Event – based“ approach

Risk sources: Use of information systems; Persons with malicious intent → Exploit → Weak passwords → Possibility of password being cracked

Events: Cracked password; Unauthorized access; Information leakage

Consequences: Information security objectives unachieved; Loss of credibility and businesses

„Asset-threat-vulnerability based“ appr

Assets: Information systems

Vulnerabilities: Weak passwords

Exploit

Threats: Persons with malicious intent; Possibility of password being cracked

Incidents: Cracked password; Unauthorized access; Information leakage

Consequences: Loss of credibility and businesses

	Likelihood of occurrence – Threat	Low			Medium			High		
	Ease of Exploitation	L	M	H	L	M	H	L	M	H
Asset Value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

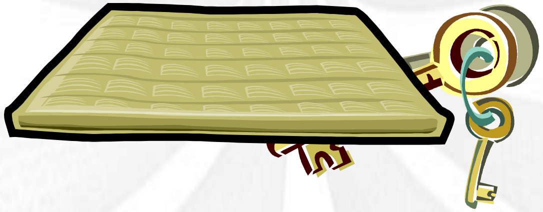
2. Current status of ISO 27005

Current status

- Current revision was cancelled last week in its 5th step, ie. 2 years lost.
- Current ISO 27005 will surview some more time.
- Ongoing need for Information Security guidance w.respect to the general 31000.
- New study period on the future of 27005.
- New study period on the creation of an IS Risk Handling Library as Standing Document (inventory of current and suggested IS risk related statements in different standards).
- LU/TREsPASS is co-rapporteur on the last study period.

2. Current status of ISO 27005

Useful to have common definitions



Threat

-> Risk source?

Vulnerability

Impact

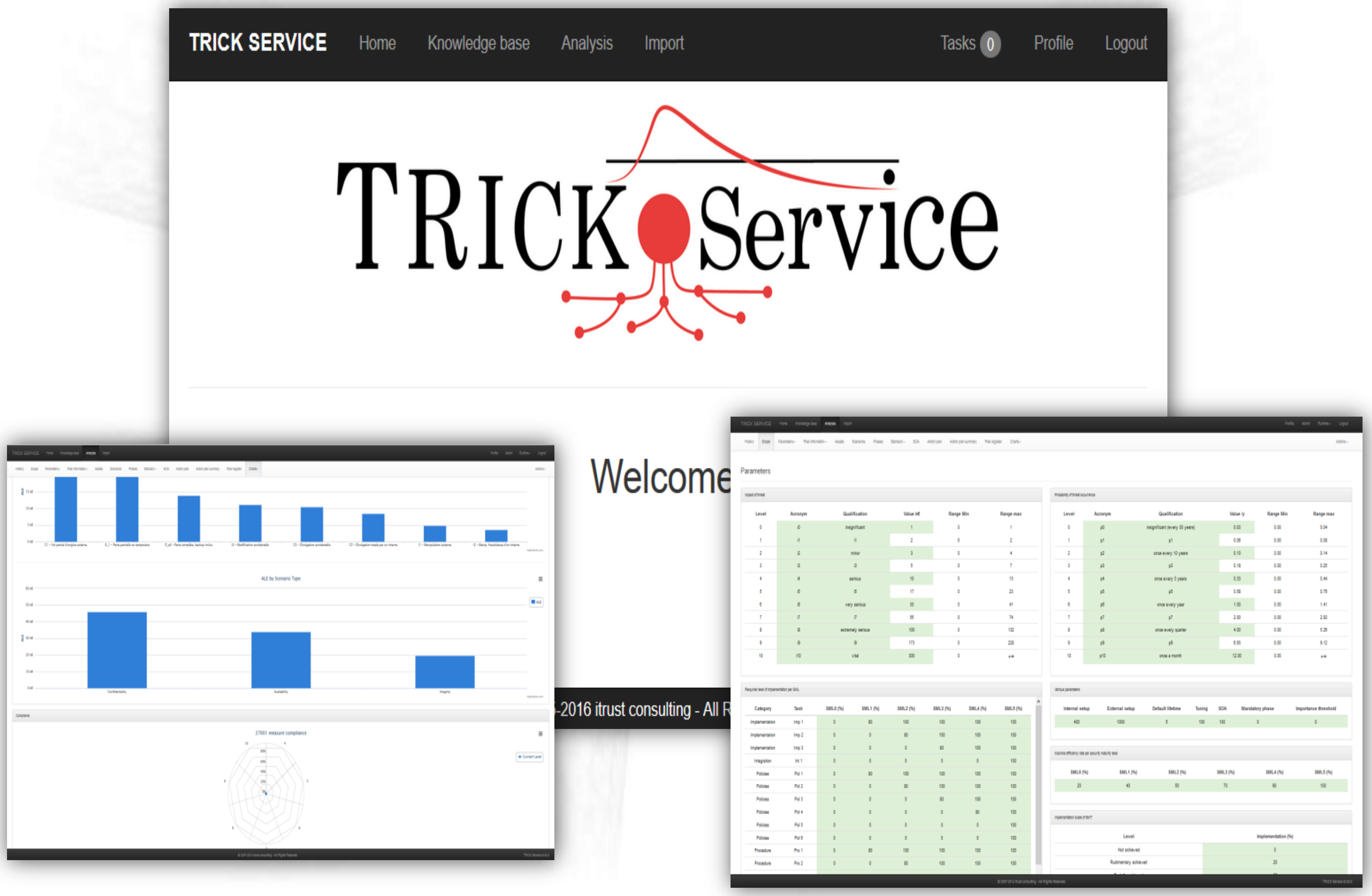
-> Consequences?

Risk = Threat • Vulnerability • Impact

(€/year) = probability/year • conditional probability • €

3. The tool TRICK Service

Tool for **R**isk management of an **I**SMS based on a **C**entral **K**nowledge base



Parameters

Impact of threat

Level	Acronym	Qualification	Value k€	Range Min	Range max
0	i0	insignificant	1	0	1
1	i1	i1	2	0	2
2	i2	minor	3	0	4
3	i3	i3	5	0	7
4	i4	serious	10	0	13
5	i5	i5	17	0	23
6	i6	very serious	30	0	41
7	i7	i7	55	0	74
8	i8	extremely serious	100	0	132
9	i9	i9	173	0	228
10	i10	vital	300	0	+∞

Probability of threat occurrence

Level	Acronym	Qualification	Value /y	Range Min	Range max
0	p0	insignificant (every 30 years)	0.03	0.00	0.04
1	p1	p1	0.06	0.00	0.08
2	p2	once every 10 years	0.10	0.00	0.14
3	p3	p3	0.18	0.00	0.25
4	p4	once every 3 years	0.33	0.00	0.44
5	p5	p5	0.58	0.00	0.78
6	p6	once every year	1.00	0.00	1.41
7	p7	p7	2.00	0.00	2.83
8	p8	once every quarter	4.00	0.00	5.28
9	p9	p9	6.93	0.00	9.12
10	p10	once a month	12.00	0.00	+∞

Required level of implementation per SML

Category	Task	SML0 (%)	SML1 (%)	SML2 (%)	SML3 (%)	SML4 (%)	SML5 (%)
Implementation	Imp 1	0	80	100	100	100	100
Implementation	Imp 2	0	0	80	100	100	100
Implementation	Imp 3	0	0	0	80	100	100
Integration	Int 1	0	0	0	0	0	100
Policies	Pol 1	0	80	100	100	100	100
Policies	Pol 2	0	0	80	100	100	100
Policies	Pol 3	0	0	0	80	100	100
Policies	Pol 4	0	0	0	0	80	100
Policies	Pol 5	0	0	0	0	0	100
Policies	Pol 6	0	0	0	0	0	100
Procedure	Pro 1	0	80	100	100	100	100
Procedure	Pro 2	0	0	80	100	100	100

Various parameters

Internal setup	External setup	Default lifetime	Tuning	SOA	Mandatory phase	Importance threshold
400	1000	5	100	100	0	0

Maximal efficiency rate per security maturity level

SML0 (%)	SML1 (%)	SML2 (%)	SML3 (%)	SML4 (%)	SML5 (%)
20	40	50	70	90	100

Implementation scale of SMT

Level	Implementation (%)
Not achieved	0
Rudimentary achieved	20

© 2007-2014 itrust consulting - All Rights Reserved

TRICK Service v0.9.0

TRICK Service

Overview

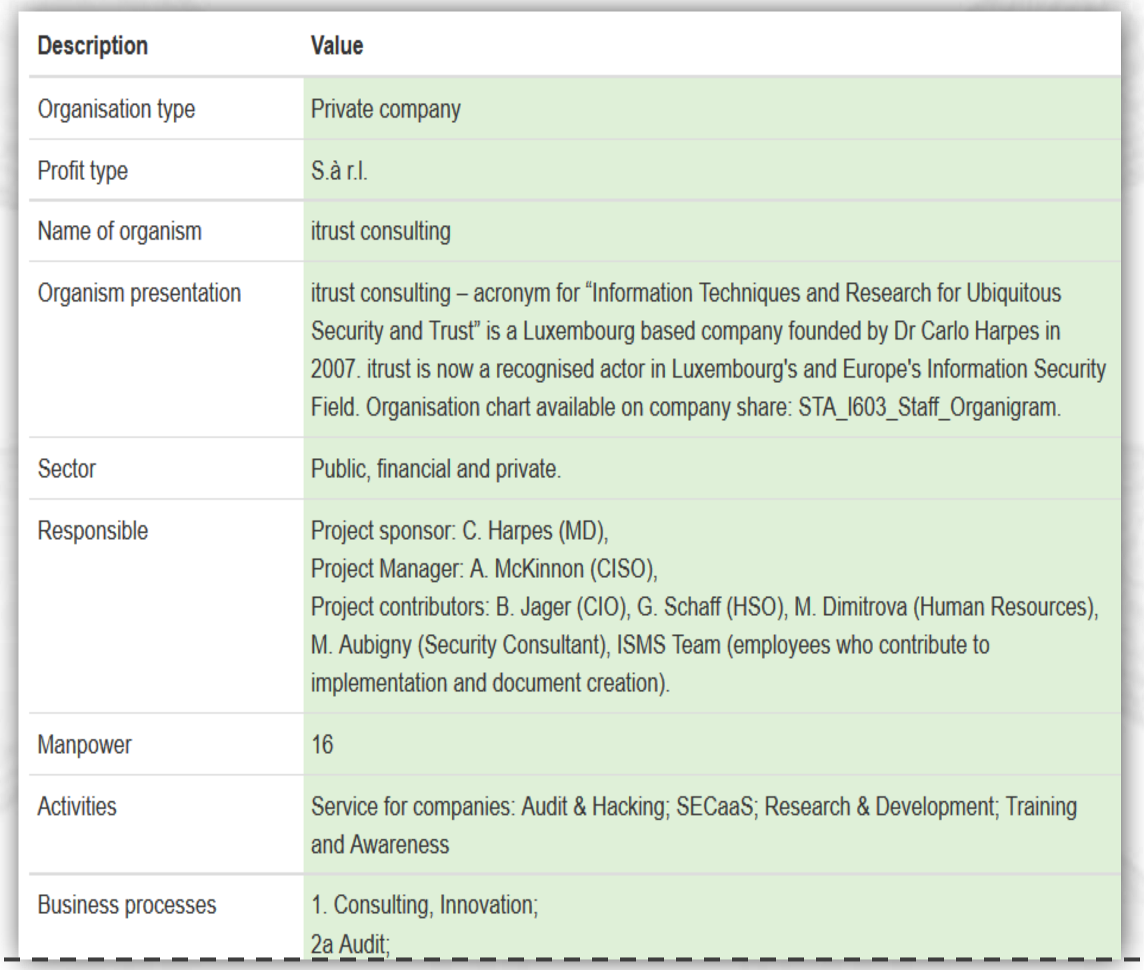
TRICK Service is a risk assessment & treatment tool by itrust consulting used to:

1. Document the organisational context & assets according to ISO 27005;
2. Audit 27002 compliance and assess resources needed for missing security;
3. Qualitatively assess threats, vulnerabilities, risks, through structured brainstorming;
4. Guide through quantified assessment of risk scenarios;
5. Model dependencies between assets, risk scenarios, and security;
6. Quantitatively assess impact and likelihood of risk scenarios applied to selected assets;
7. Prepare risk treatment plan, sorted by implementation phases and ROSI;
8. Prepare Statement of applicability for ISO 27001 certification;
9. Prepare risk analysis report compliant to CSSF circular 12/544
10. Assess security maturity.

TRICK Service

Step 1. Context establishment

Define the scope and your organisation

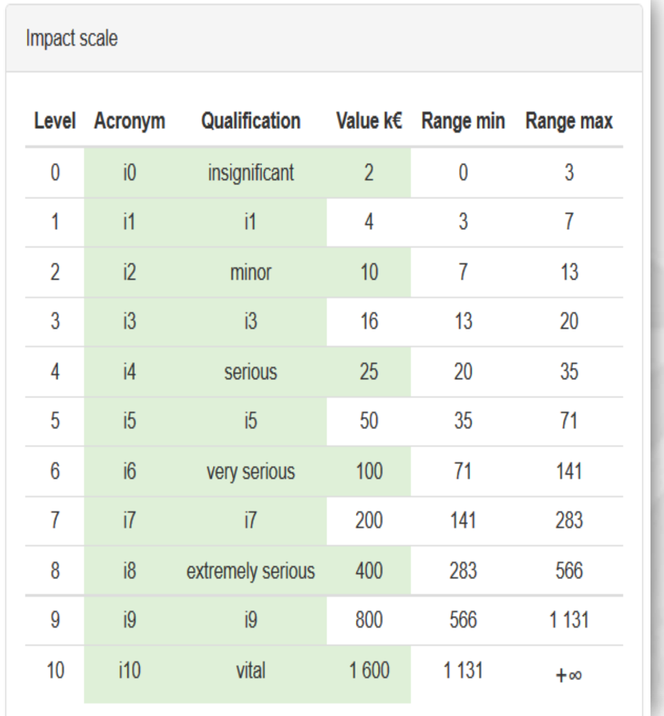


Description	Value
Organisation type	Private company
Profit type	S.à r.l.
Name of organism	itrust consulting
Organism presentation	itrust consulting – acronym for "Information Techniques and Research for Ubiquitous Security and Trust" is a Luxembourg based company founded by Dr Carlo Harpes in 2007. itrust is now a recognised actor in Luxembourg's and Europe's Information Security Field. Organisation chart available on company share: STA_I603_Staff_Organigram.
Sector	Public, financial and private.
Responsible	Project sponsor: C. Harpes (MD), Project Manager: A. McKinnon (CISO), Project contributors: B. Jager (CIO), G. Schaff (HSO), M. Dimitrova (Human Resources), M. Aubigny (Security Consultant), ISMS Team (employees who contribute to implementation and document creation).
Manpower	16
Activities	Service for companies: Audit & Hacking; SECaaS; Research & Development; Training and Awareness
Business processes	1. Consulting, Innovation; 2a Audit;

TRICK Service

Define the scale and the standard of best practices

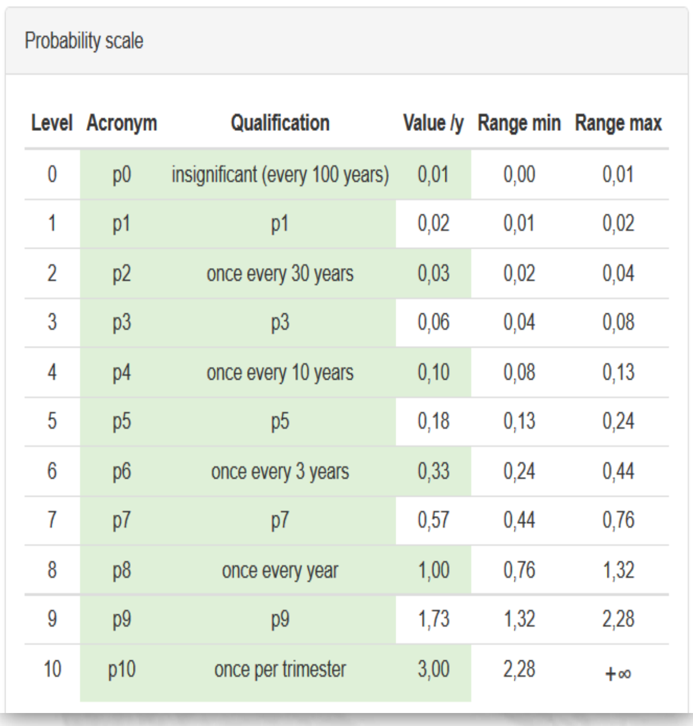
Impact scale (CSSF compatible)



Impact scale

Level	Acronym	Qualification	Value k€	Range min	Range max
0	i0	insignificant	2	0	3
1	i1	i1	4	3	7
2	i2	minor	10	7	13
3	i3	i3	16	13	20
4	i4	serious	25	20	35
5	i5	i5	50	35	71
6	i6	very serious	100	71	141
7	i7	i7	200	141	283
8	i8	extremely serious	400	283	566
9	i9	i9	800	566	1 131
10	i10	vital	1 600	1 131	+∞

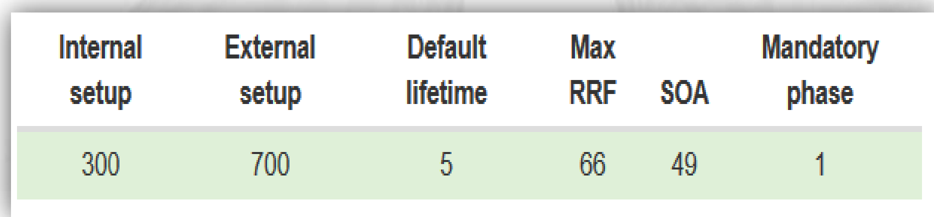
Probability scale (CSSF compatible)



Probability scale

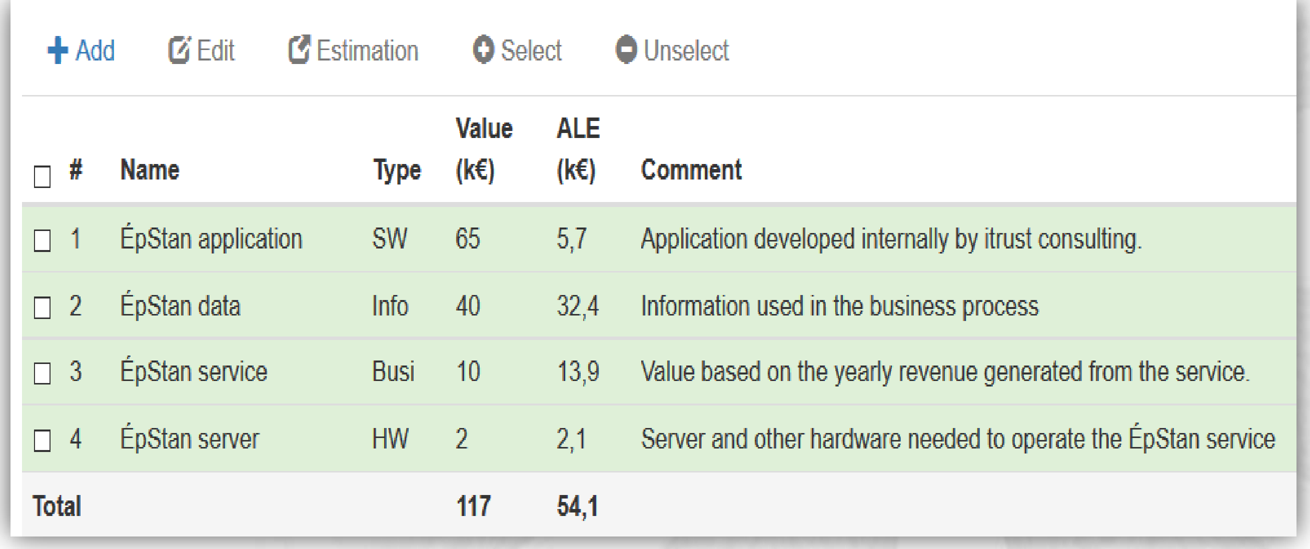
Level	Acronym	Qualification	Value /y	Range min	Range max
0	p0	insignificant (every 100 years)	0,01	0,00	0,01
1	p1	p1	0,02	0,01	0,02
2	p2	once every 30 years	0,03	0,02	0,04
3	p3	p3	0,06	0,04	0,08
4	p4	once every 10 years	0,10	0,08	0,13
5	p5	p5	0,18	0,13	0,24
6	p6	once every 3 years	0,33	0,24	0,44
7	p7	p7	0,57	0,44	0,76
8	p8	once every year	1,00	0,76	1,32
9	p9	p9	1,73	1,32	2,28
10	p10	once per trimester	3,00	2,28	+∞

Various parameters



Internal setup	External setup	Default lifetime	Max RRF	SOA	Mandatory phase
300	700	5	66	49	1

Context establishment: Identify and estimate assets



□	#	Name	Type	Value (k€)	ALE (k€)	Comment
□	1	ÉpStan application	SW	65	5,7	Application developed internally by itrust consulting.
□	2	ÉpStan data	Info	40	32,4	Information used in the business process
□	3	ÉpStan service	Busi	10	13,9	Value based on the yearly revenue generated from the service.
□	4	ÉpStan server	HW	2	2,1	Server and other hardware needed to operate the ÉpStan service
Total				117	54,1	

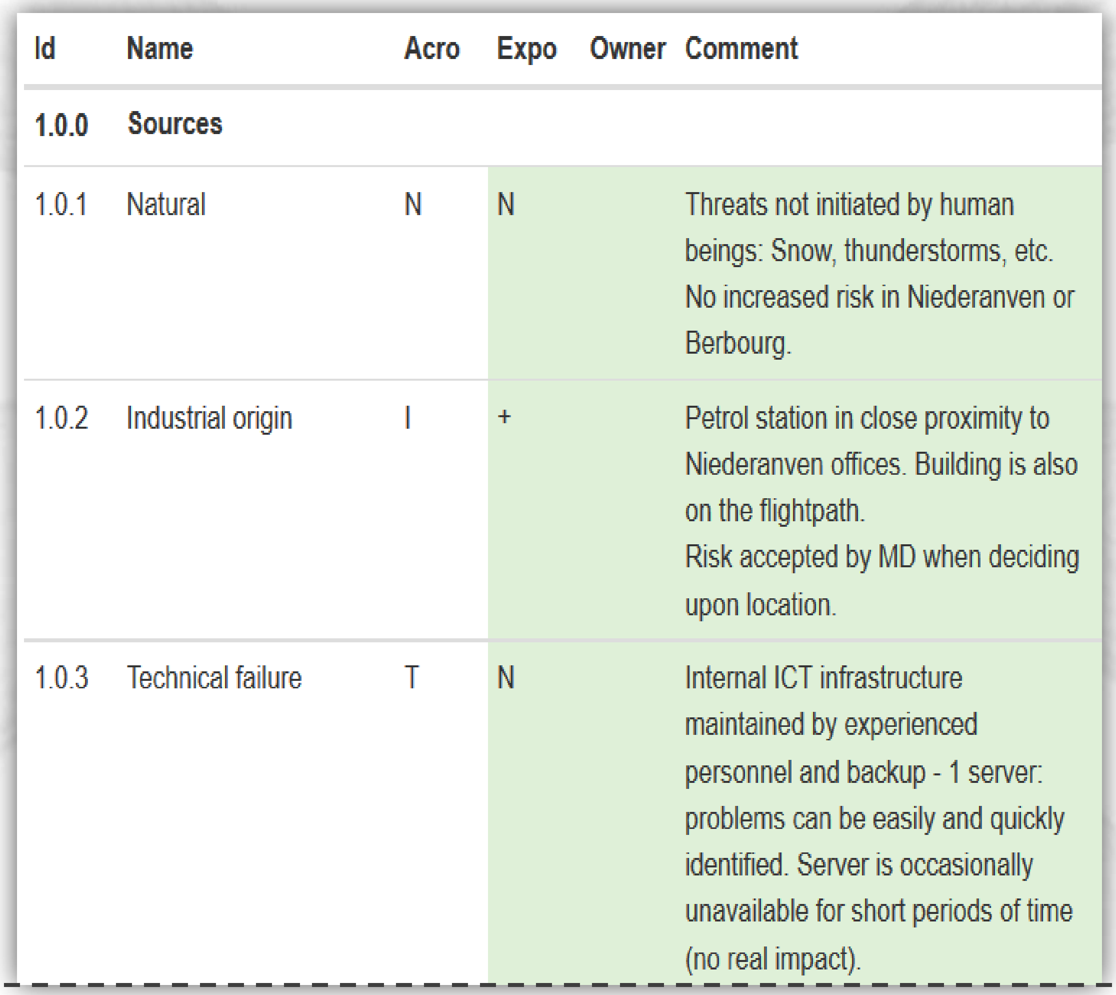
Asset types:

- Service;
- Information;
- Software;
- Hardware;
- Network;
- Staff;
- Not material value;
- Business (CSSF);
- Financial (CSSF);
- Compliance (CSSF).

TRICK Service

Step 2: Qualitative risk analysis

Qualitatively assess threats, vulnerabilities, and risks, through structured brainstorming

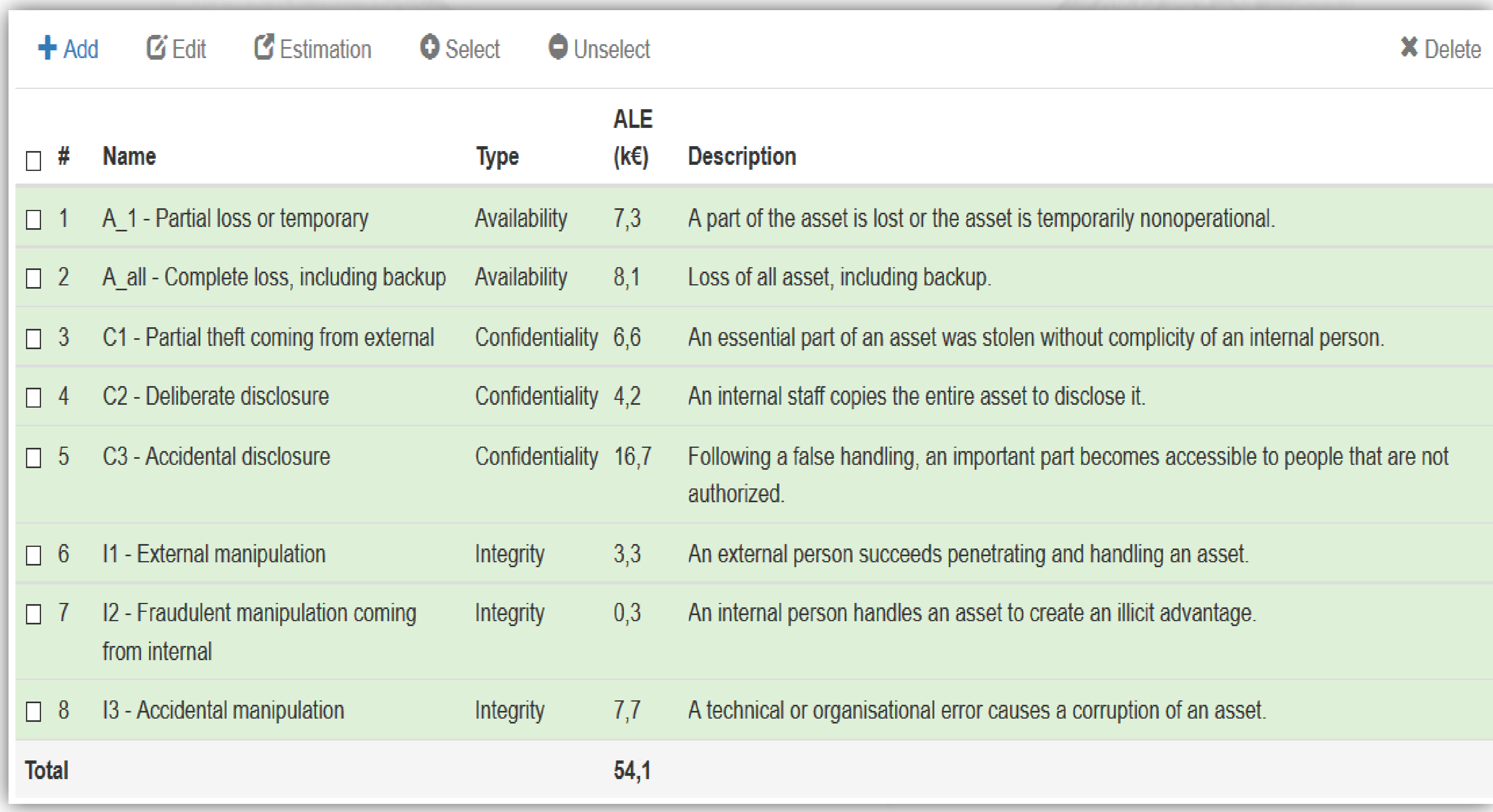


Id	Name	Acro	Expo	Owner	Comment
1.0.0	**Sources**				
1.0.1	Natural	N	N		Threats not initiated by human beings: Snow, thunderstorms, etc. No increased risk in Niederanven or Berbourg.
1.0.2	Industrial origin	I	+		Petrol station in close proximity to Niederanven offices. Building is also on the flightpath. Risk accepted by MD when deciding upon location.
1.0.3	Technical failure	T	N		Internal ICT infrastructure maintained by experienced personnel and backup - 1 server: problems can be easily and quickly identified. Server is occasionally unavailable for short periods of time (no real impact).

TRICK Service

Risk identification for quantitative risk analysis

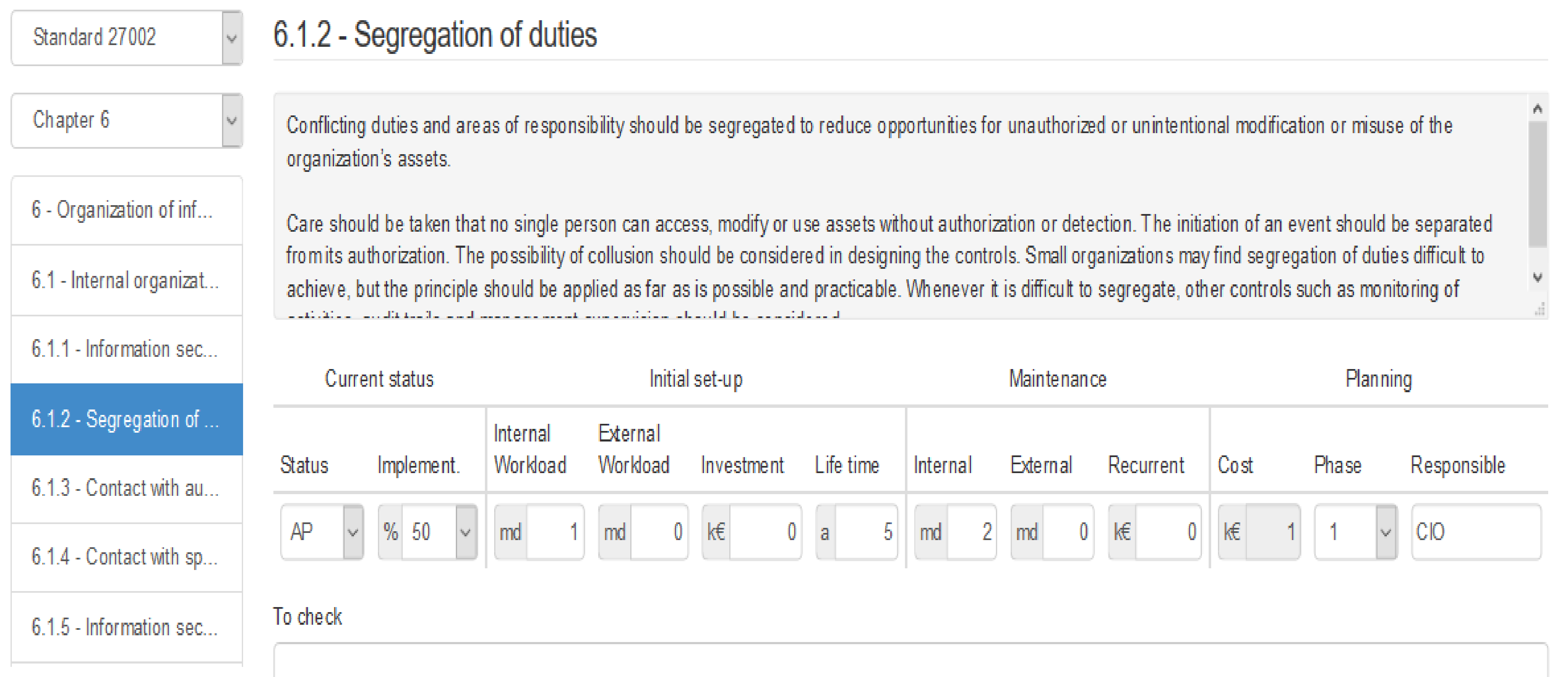
Definition of risk scenarios



□	#	Name	Type	ALE (k€)	Description
□	1	A_1 - Partial loss or temporary	Availability	7,3	A part of the asset is lost or the asset is temporarily nonoperational.
□	2	A_all - Complete loss, including backup	Availability	8,1	Loss of all asset, including backup.
□	3	C1 - Partial theft coming from external	Confidentiality	6,6	An essential part of an asset was stolen without complicity of an internal person.
□	4	C2 - Deliberate disclosure	Confidentiality	4,2	An internal staff copies the entire asset to disclose it.
□	5	C3 - Accidental disclosure	Confidentiality	16,7	Following a false handling, an important part becomes accessible to people that are not authorized.
□	6	I1 - External manipulation	Integrity	3,3	An external person succeeds penetrating and handling an asset.
□	7	I2 - Fraudulent manipulation coming from internal	Integrity	0,3	An internal person handles an asset to create an illicit advantage.
□	8	I3 - Accidental manipulation	Integrity	7,7	A technical or organisational error causes a corruption of an asset.
Total				**54,1**	

Step 3: Security assessment

Identify, estimate effectiveness and required cost of standardised and custom controls



Standard 27002

Chapter 6

6 - Organization of inf...

6.1 - Internal organizat...

6.1.1 - Information sec...

6.1.2 - Segregation of ...

6.1.3 - Contact with au...

6.1.4 - Contact with sp...

6.1.5 - Information sec...

6.1.2 - Segregation of duties

Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

Care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered in designing the controls. Small organizations may find segregation of duties difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered.

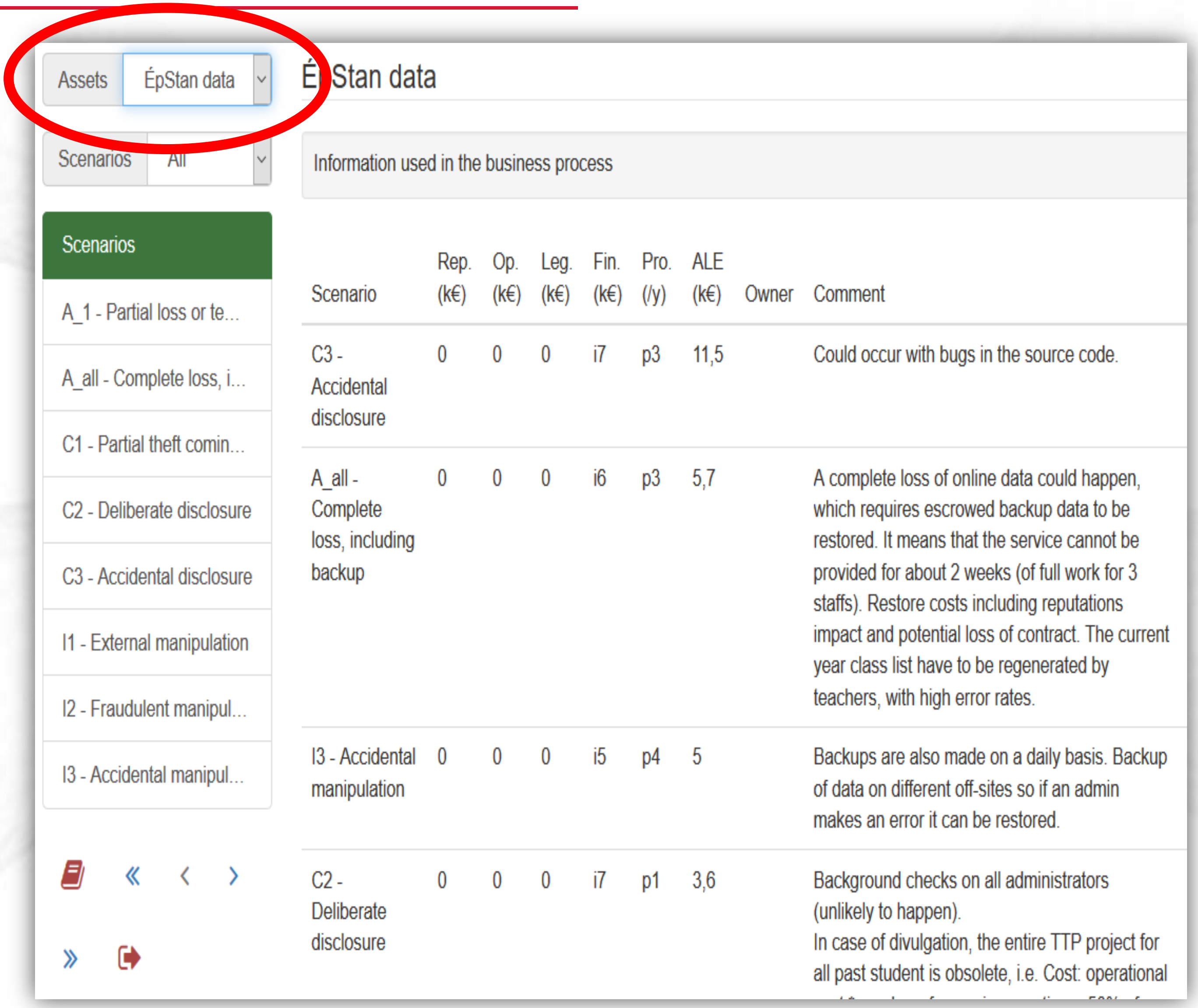
Current status		Initial set-up				Maintenance			Planning		
Status	Implement.	Internal Workload	External Workload	Investment	Life time	Internal	External	Recurrent	Cost	Phase	Responsible
AP	% 50	md 1	md 0	k€ 0	a 5	md 2	md 0	k€ 0	k€ 1	1	CIO

To check

TRICK Service

Step 4: Assess your risks in term of impact, likelihood…

Estimation of an asset


Assets
ÉpStan data
Scenarios
All
Scenarios
A_1 - Partial loss or te...
A_all - Complete loss, i...
C1 - Partial theft comin...
C2 - Deliberate disclosure
C3 - Accidental disclosure
I1 - External manipulation
I2 - Fraudulent manipul...
I3 - Accidental manipul...

ÉpStan data

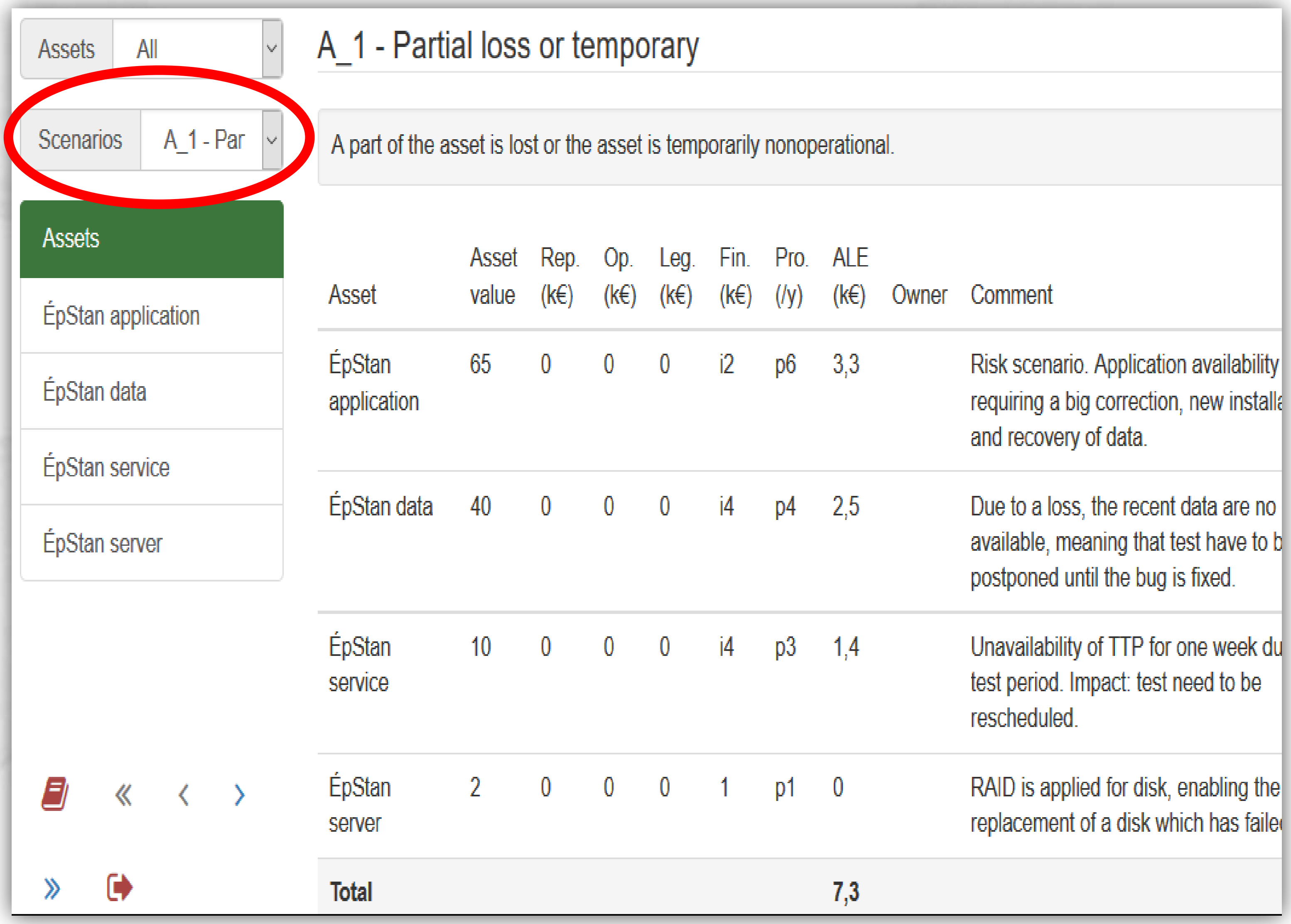
Information used in the business process

Scenario	Rep. (k€)	Op. (k€)	Leg. (k€)	Fin. (k€)	Pro. (/y)	ALE (k€)	Owner	Comment
C3 - Accidental disclosure	0	0	0	i7	p3	11,5		Could occur with bugs in the source code.
A_all - Complete loss, including backup	0	0	0	i6	p3	5,7		A complete loss of online data could happen, which requires escrowed backup data to be restored. It means that the service cannot be provided for about 2 weeks (of full work for 3 staffs). Restore costs including reputations impact and potential loss of contract. The current year class list have to be regenerated by teachers, with high error rates.
I3 - Accidental manipulation	0	0	0	i5	p4	5		Backups are also made on a daily basis. Backup of data on different off-sites so if an admin makes an error it can be restored.
C2 - Deliberate disclosure	0	0	0	i7	p1	3,6		Background checks on all administrators (unlikely to happen). In case of divulgation, the entire TTP project for all past student is obsolete, i.e. Cost: operational

TRICK Service

Step 4: Assess your risks in term of impact, likelihood…

Estimation of a scenario



Assets All

Scenarios A_1 - Par

Assets

ÉpStan application

ÉpStan data

ÉpStan service

ÉpStan server

A_1 - Partial loss or temporary

A part of the asset is lost or the asset is temporarily nonoperational.

Asset	Asset value	Rep. (k€)	Op. (k€)	Leg. (k€)	Fin. (k€)	Pro. (/y)	ALE (k€)	Owner	Comment
ÉpStan application	65	0	0	0	i2	p6	3,3		Risk scenario. Application availability requiring a big correction, new installa and recovery of data.
ÉpStan data	40	0	0	0	i4	p4	2,5		Due to a loss, the recent data are no available, meaning that test have to b postponed until the bug is fixed.
ÉpStan service	10	0	0	0	i4	p3	1,4		Unavailability of TTP for one week du test period. Impact: test need to be rescheduled.
ÉpStan server	2	0	0	0	1	p1	0		RAID is applied for disk, enabling the replacement of a disk which has faile
Total							**7,3**		

TRICK Service

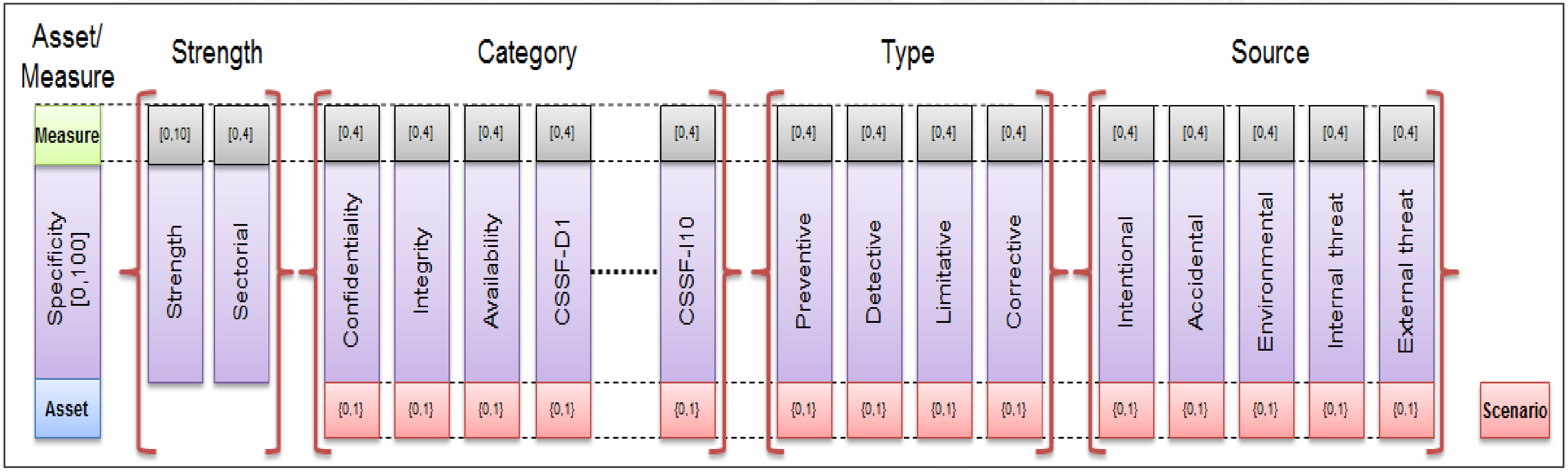
Step 5: Finetune “Risk Reduction Factor” if needed

TRICK Service: a tool based on the profitability of security measures (ROSI)

Risk Reduction Factor (RRF) = relative reduction of a given risk by implementing a given security measures.

TRICK Service contains an estimate of RRF for each security measure, each risk, each asset type, which can be fine-tuned if needed.

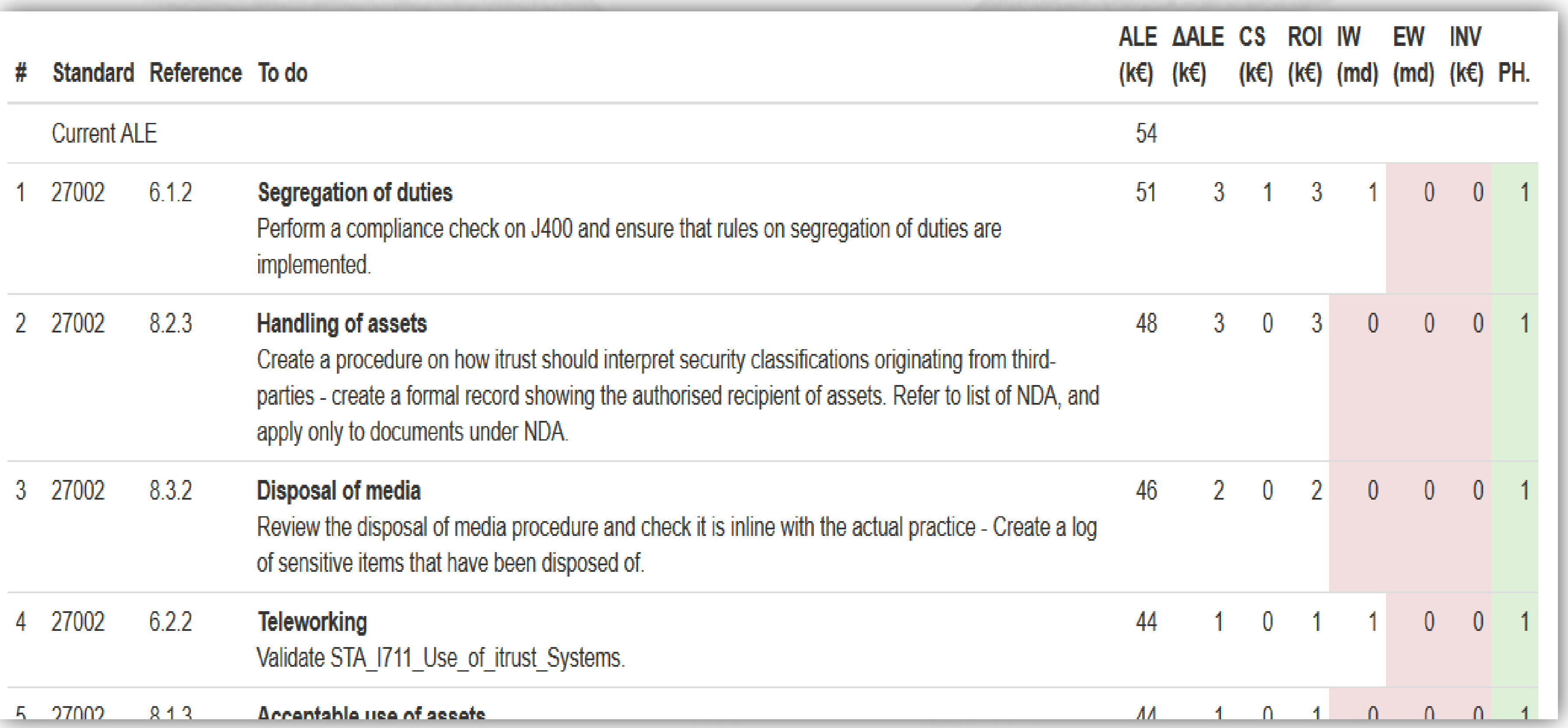
Those estimates are based on properties of scenario, measures, and assets:



TRICK Service

Step 6: Risk Treatment: Create Action Plan, change plans, ...

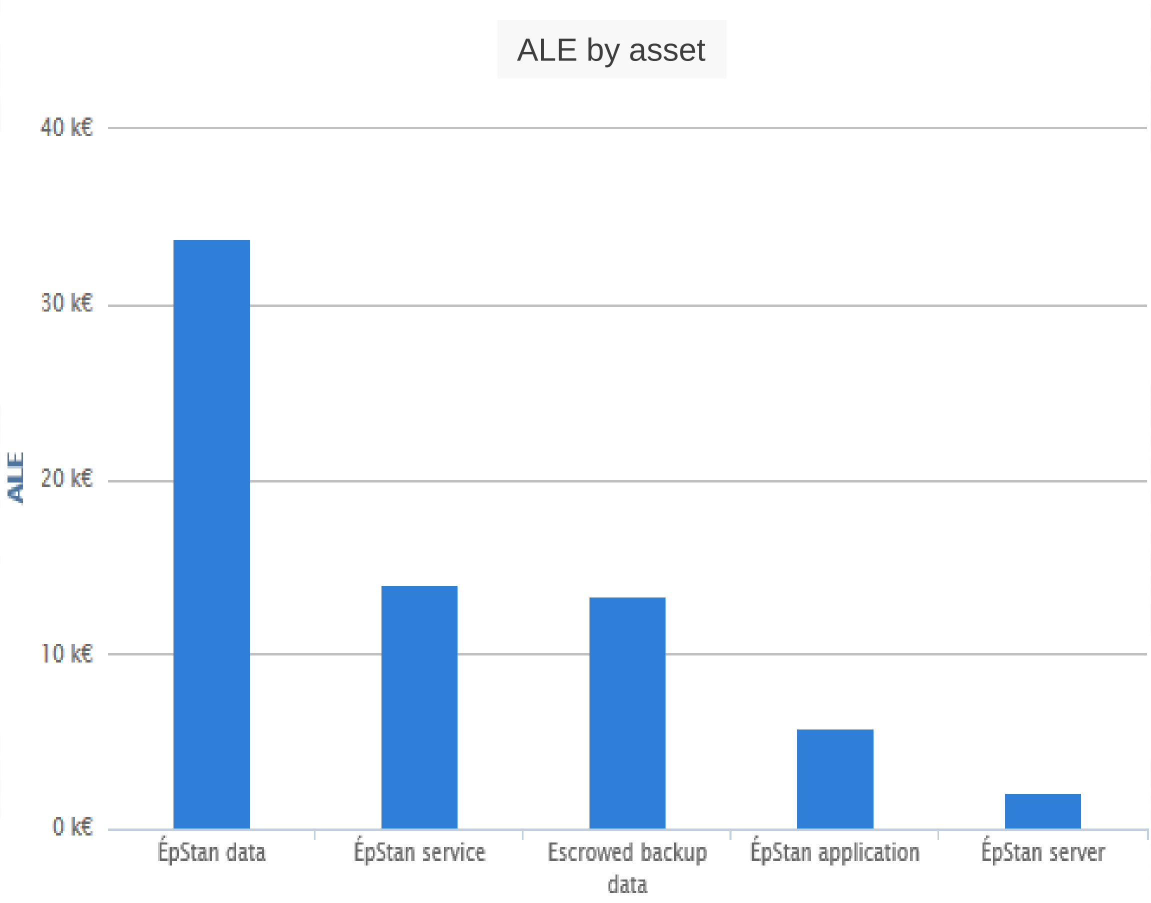
- **Assign implementation phase, check budget constraints and acceptance criteria, review…**
- **Risk treatment plan, sorted by implementation phase and ROSI**



#	Standard	Reference	To do	ALE (k€)	ΔALE (k€)	CS (k€)	ROI (k€)	IW (md)	EW (md)	INV (k€)	PH.
	Current ALE			54							
1	27002	6.1.2	**Segregation of duties** Perform a compliance check on J400 and ensure that rules on segregation of duties are implemented.	51	3	1	3	1	0	0	1
2	27002	8.2.3	**Handling of assets** Create a procedure on how itrust should interpret security classifications originating from third-parties - create a formal record showing the authorised recipient of assets. Refer to list of NDA, and apply only to documents under NDA.	48	3	0	3	0	0	0	1
3	27002	8.3.2	**Disposal of media** Review the disposal of media procedure and check it is inline with the actual practice - Create a log of sensitive items that have been disposed of.	46	2	0	2	0	0	0	1
4	27002	6.2.2	**Teleworking** Validate STA_I711_Use_of_itrust_Systems.	44	1	0	1	1	0	0	1
5	27002	8.1.3	**Acceptable use of assets**	44	1	0	1	0	0	0	1

Step 7: Risk assessment and treatment report

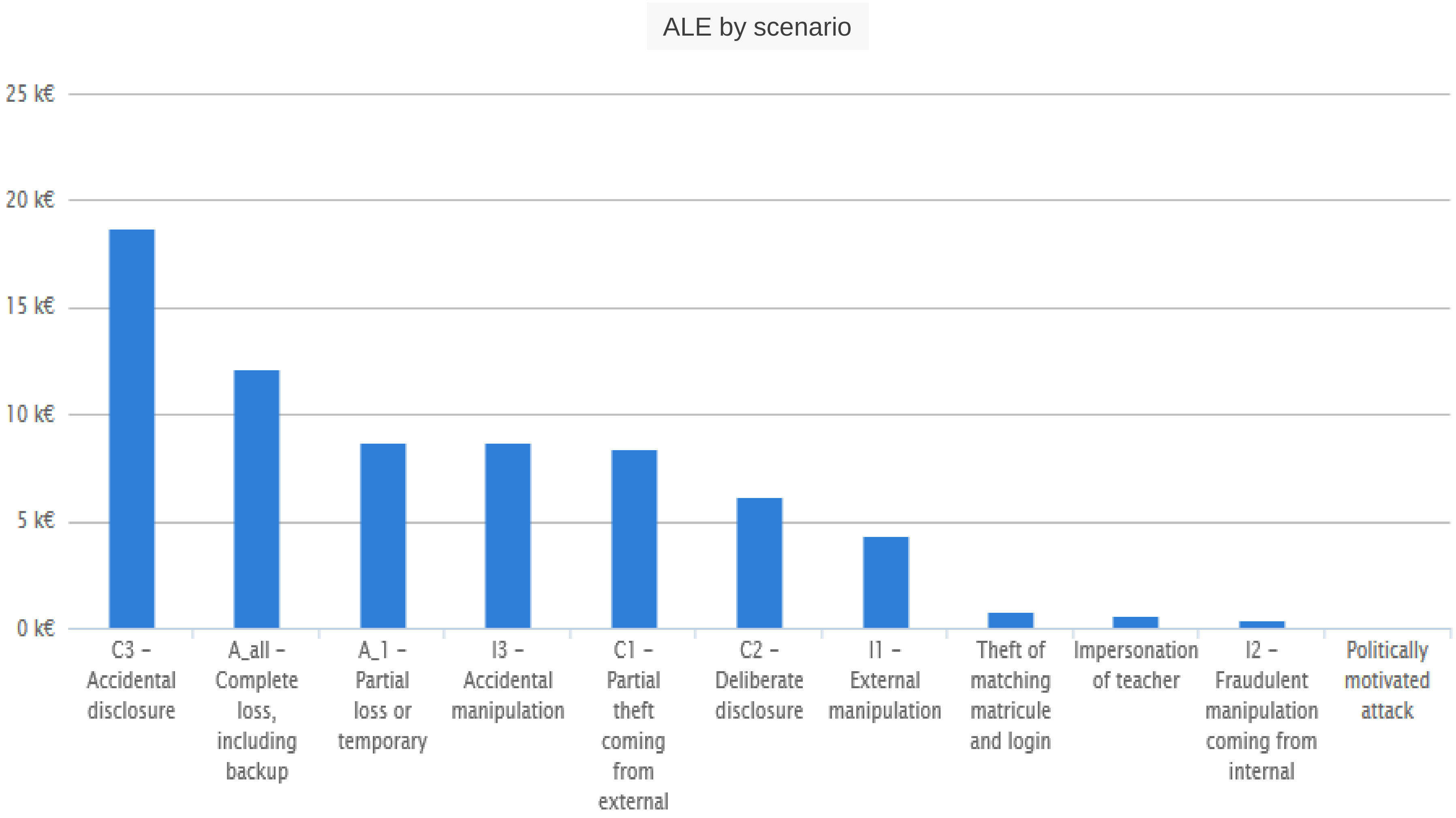
Indicators and management view on risks



TRICK Service

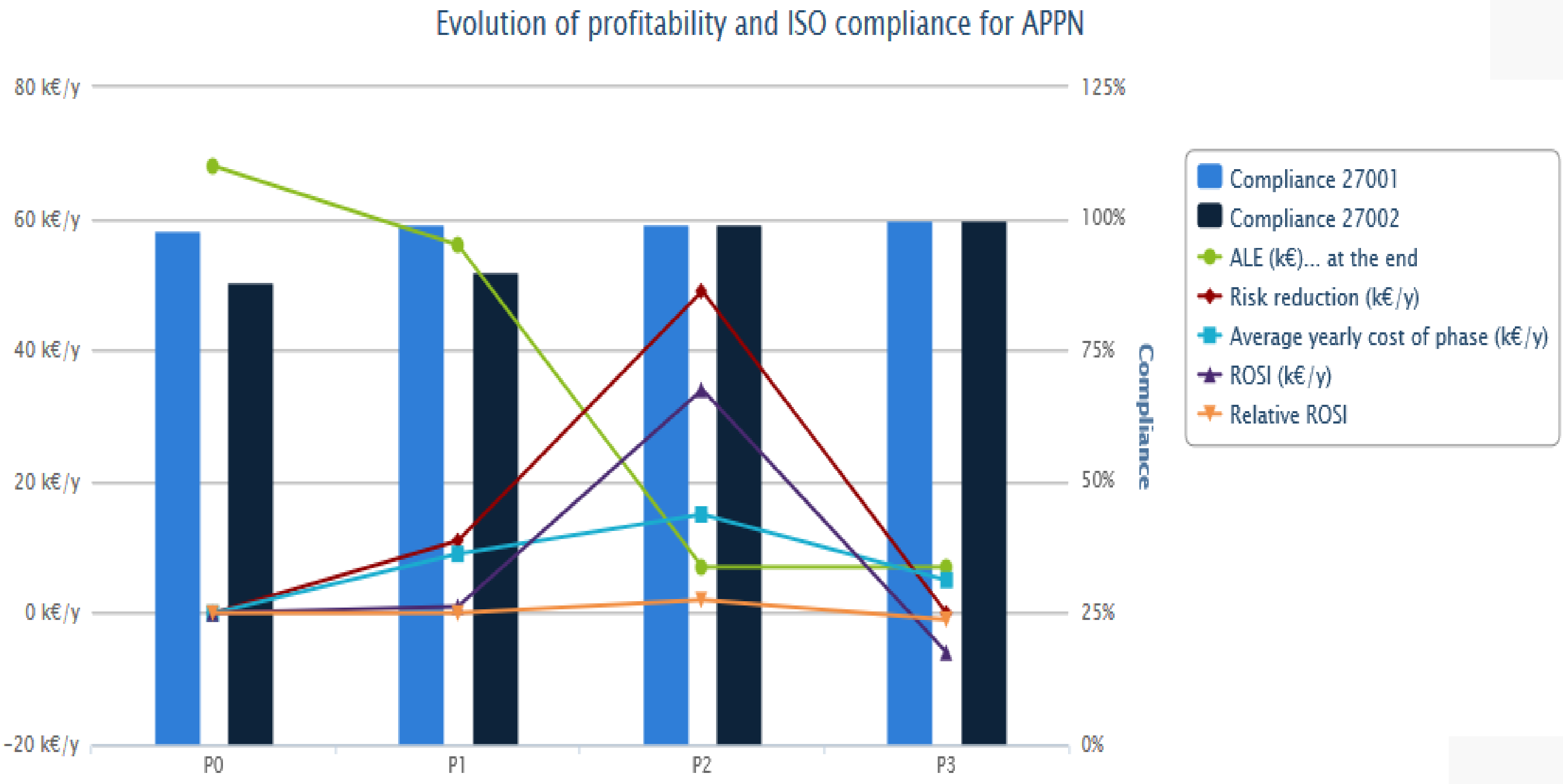
Step 7: Risk assessment and treatment report

Indicators and management view on risks



Step 7: Risk assessment and treatment report

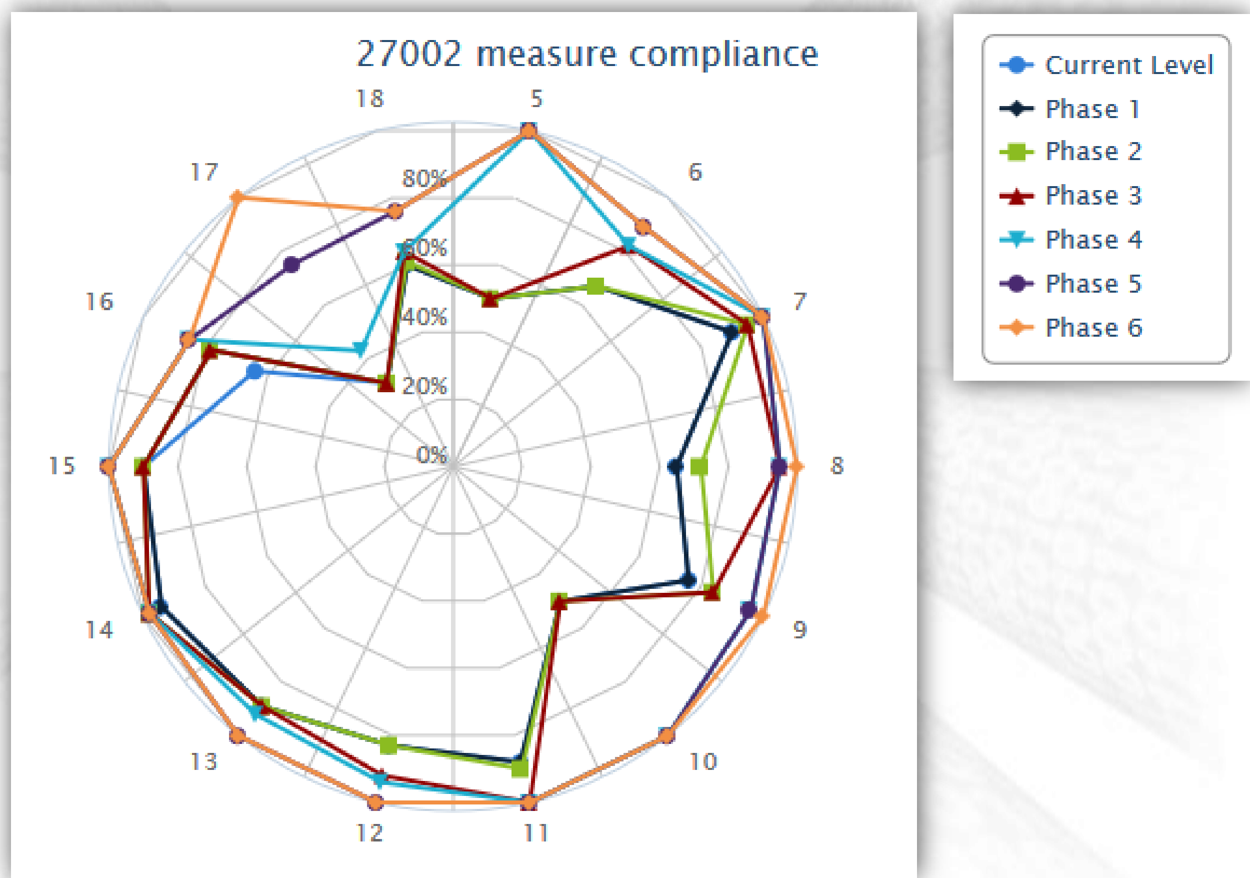
Management view of implementation phases



TRICK Service

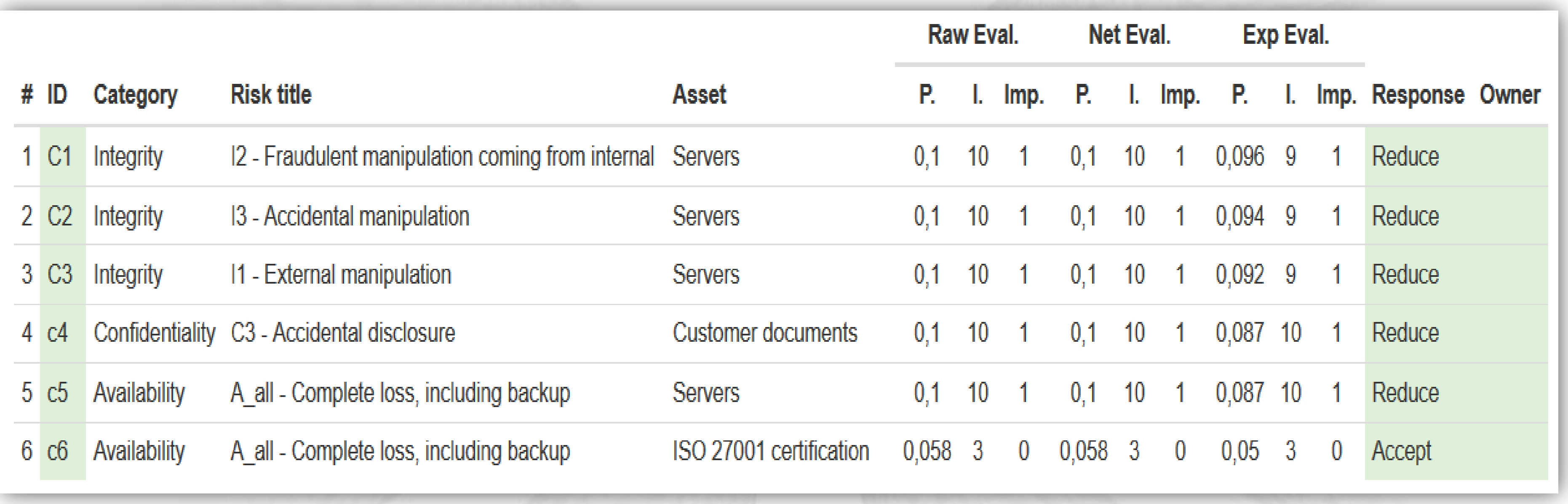
Step 7: Risk assessment and treatment report

27002 Compliance evolution with risk treatment plan



Step 7: Risk assessment and treatment report

CSSF compliant risk register



					Raw Eval.			Net Eval.			Exp Eval.				
#	ID	Category	Risk title	Asset	P.	I.	Imp.	P.	I.	Imp.	P.	I.	Imp.	Response	Owner
1	C1	Integrity	I2 - Fraudulent manipulation coming from internal	Servers	0,1	10	1	0,1	10	1	0,096	9	1	Reduce	
2	C2	Integrity	I3 - Accidental manipulation	Servers	0,1	10	1	0,1	10	1	0,094	9	1	Reduce	
3	C3	Integrity	I1 - External manipulation	Servers	0,1	10	1	0,1	10	1	0,092	9	1	Reduce	
4	c4	Confidentiality	C3 - Accidental disclosure	Customer documents	0,1	10	1	0,1	10	1	0,087	10	1	Reduce	
5	c5	Availability	A_all - Complete loss, including backup	Servers	0,1	10	1	0,1	10	1	0,087	10	1	Reduce	
6	c6	Availability	A_all - Complete loss, including backup	ISO 27001 certification	0,058	3	0	0,058	3	0	0,05	3	0	Accept	

TRICK Service

Step 7: Risk assessment and treatment report

Get all results in a structured report

Management summary
1 Introduction
Context, Document objectives, Scope, Audience, Document structure, References, Acronyms, Glossary
2 Methodology
2.1 Phases of risk management
Risk context
Risk identification
Risks estimation
Risks treatment
Risk acceptance
3 Risk context
3.1 General considerations
3.2 Basic criteria
Risk assessment criterion
Impact criterion
Risk acceptance criterion
3.3 The target
General considerations
Organisation chart
Table of assets
3.4 Organisation of risk management

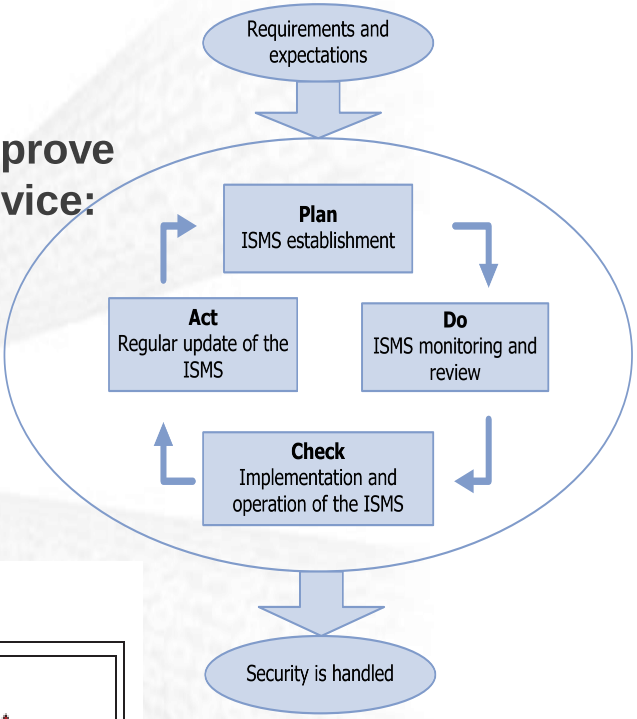
4 Risk assessment
4.1 General aspect of the security
4.2 Threats mapping
Approach
Details
Conclusion
4.3 Specific Risks
Approach
Details
Conclusion
4.4 Risk estimation
Introduction
Table of estimated risks for each asset
Summary of the current level of risk
5 Implementation level of ISO 27002
6 Risk treatment plan
6.1 Introduction
6.2 Specific recommendations
6.3 General ISO 27002 related recommendations
7 Risk evaluation and conclusions
Annexes:
Statement of applicability
State of implementation of ISO 27002 security measures

TRICK Service

Contineous improvement

Update and fine-tune yearly your Risk Assessment

Continously improve with TRICK Service:


Requirements and expectations

Plan
ISMS establishment

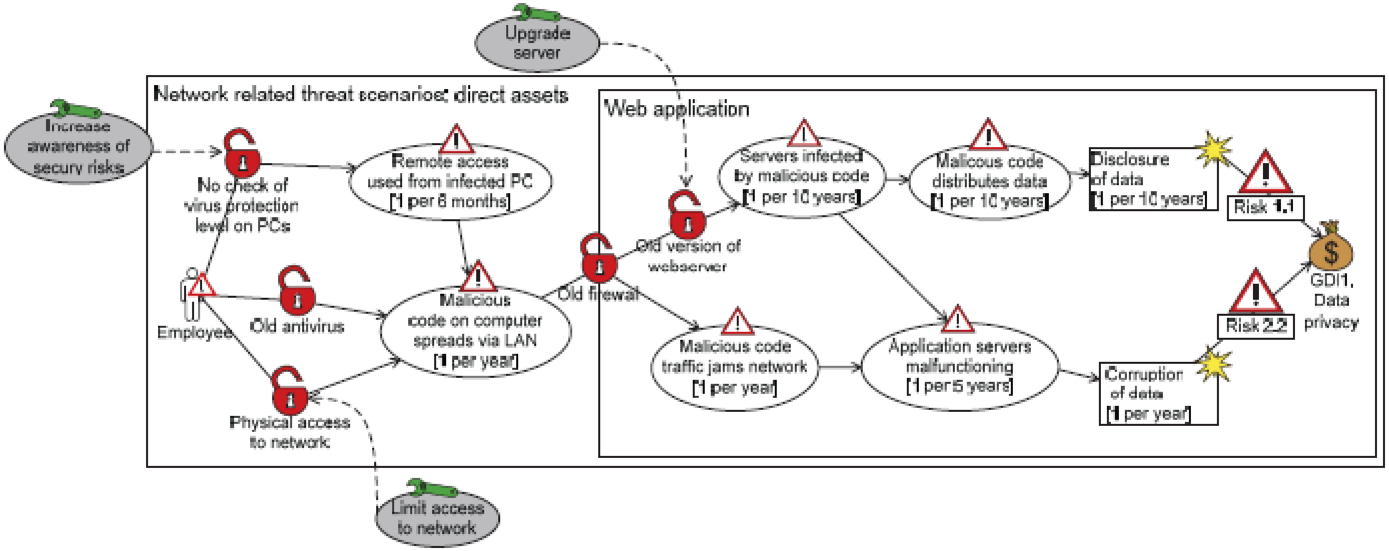
Do
ISMS monitoring and review

Check
Implementation and operation of the ISMS

Act
Regular update of the ISMS

Security is handled

Improve by detailed modelling of critical parts, e.g. with CORAS, Attack-Defence-trees or other ISO 31010 techniques:


Upgrade server
Network related threat scenarios: direct assets
Web application
Increase awareness of secury risks
No check of virus protection level on PCs
Remote access used from infected PC [1 per 6 months]
Employee
Old antivirus
Malicious code on computer spreads via LAN [1 per year]
Physical access to network
Limit access to network
Old firewall
Old version of webserver
Servers infected by malicious code [1 per 10 years]
Malicous code distributes data [1 per 10 years]
Disclosure of data [1 per 10 years]
Risk 1.1
GDI1, Data privacy
Risk 2.2
Malicious code traffic jams network [1 per year]
Application servers malfunctioning [1 per 5 years]
Corruption of data [1 per year]

4. Ongoing TREsPASS contribution towards TRICK Cockpit

There is a need for

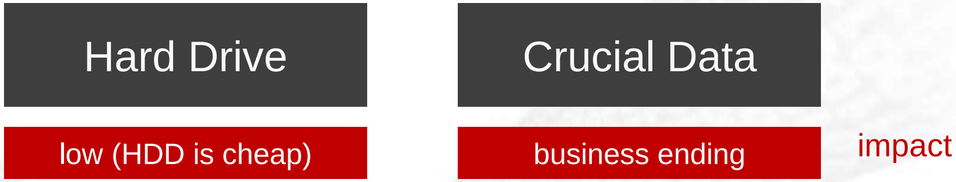
- Fine-tuning with attack-defence trees
- Better assessment of socio-technical risks.

  -> which leads to TREsPASS.
- Asset dependency model
- Real time update of TRICK service parameter
- Visualisation for real time system -> TRICK Cockpit
- Integration of IDS, Incident Handling, Vulnerability management to update the correspondign parameter of the risk model (either the linear TRICK Service model, or the fine-tuned ATTACK-DEFENCE-TREE.

Asset Dependencies

Why Asset Dependencies?

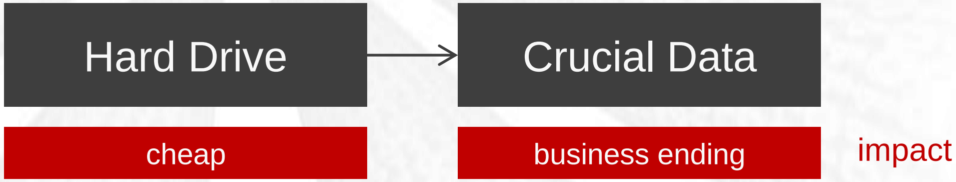
Traditional risk analysis



«HDD crash» scenario: HDD needs to be replaced

→ low overall impact

With dependencies:



«HDD crash» scenario: HDD needs to be replaced *and* data is lost

→ high overall impact

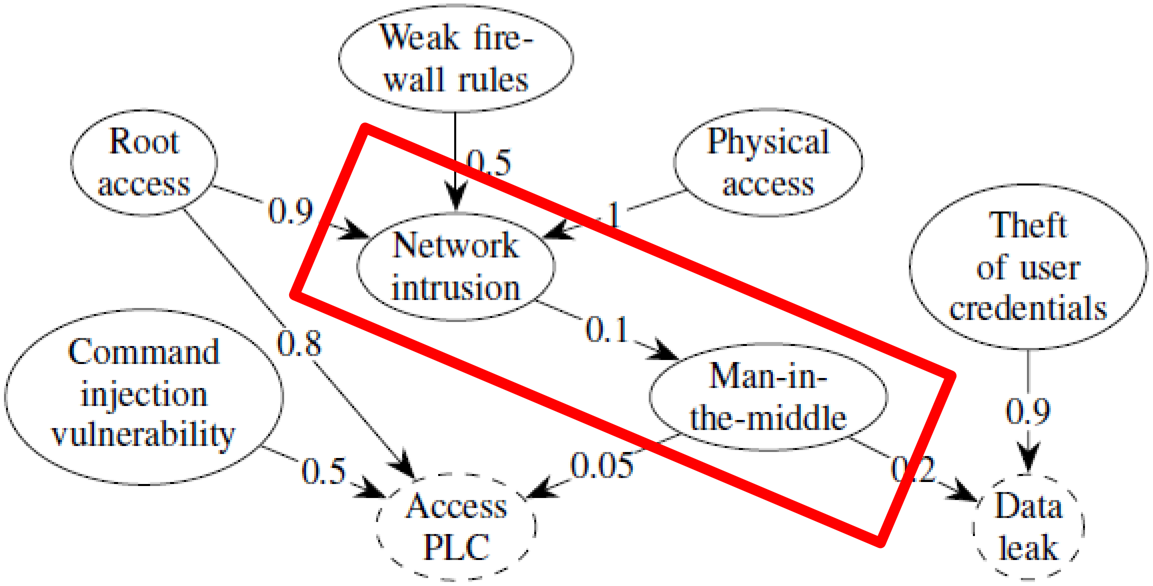
Dependency-aware risk analysis highly encourages disk health monitoring, whereas traditional does not.

Asset Dependencies

How to describe dependencies?

- Express dependencies between *assets* as cause/consequence of *incidents*

- (Sample) Dependency graph:

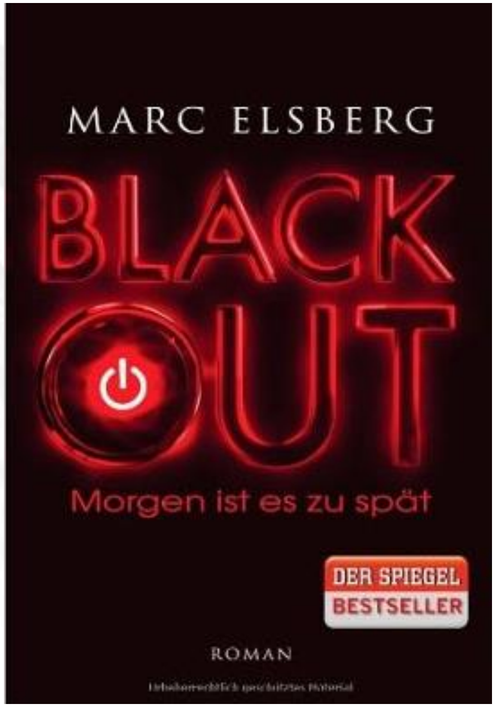


IF there is a network intrusion,
THEN there is a 10% chance of a Man-In-The-Middle attack

Conclusion

<u>Leassons Learned by cofunded R&D project:</u>

- For itrust consulting, R&D is THE enabler of growth.
- Knowledge of several research projets contributed to tool, in particular TRICK service.
- Users do not pay the full price for the required security;
  co-funded R&D is mandatory to create the required knowledge to protect against cybersecurity
- Missing concerns by operators of critical societal or economic activities.



itrust
consulting

Thank you for your attention!