itrust
consulting

TRICK Service

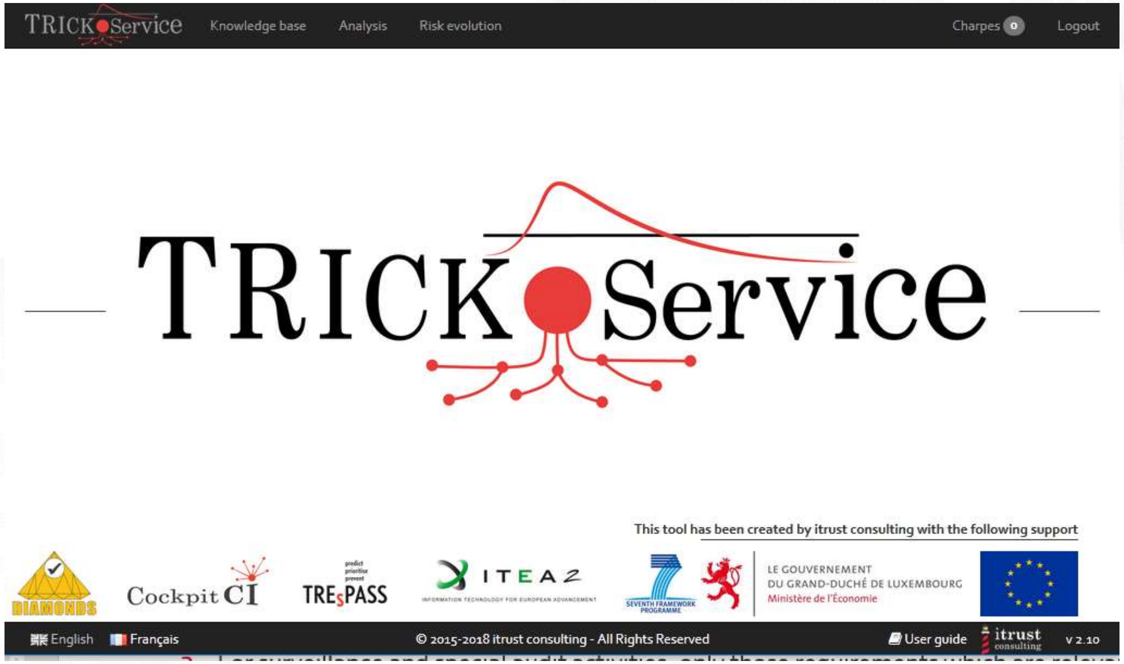
Product overview

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

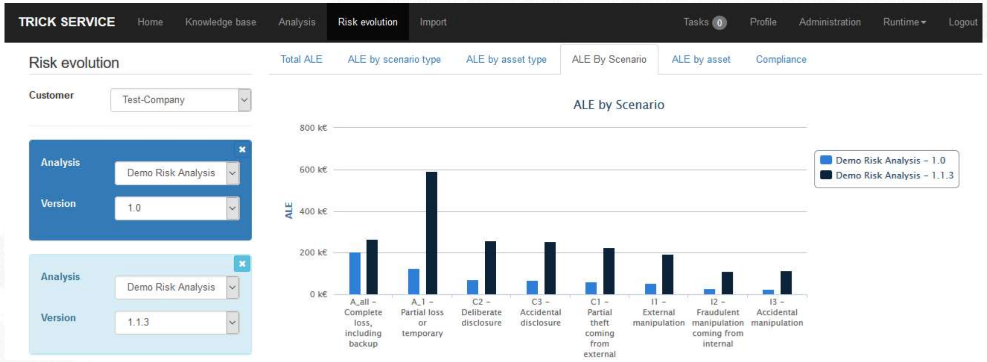
Tel: +352 26 176 212
Fax: +352 26 710 978
Web: www.itrust.lu

TRICK Service

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



This tool has been created by itrust consulting with the following support

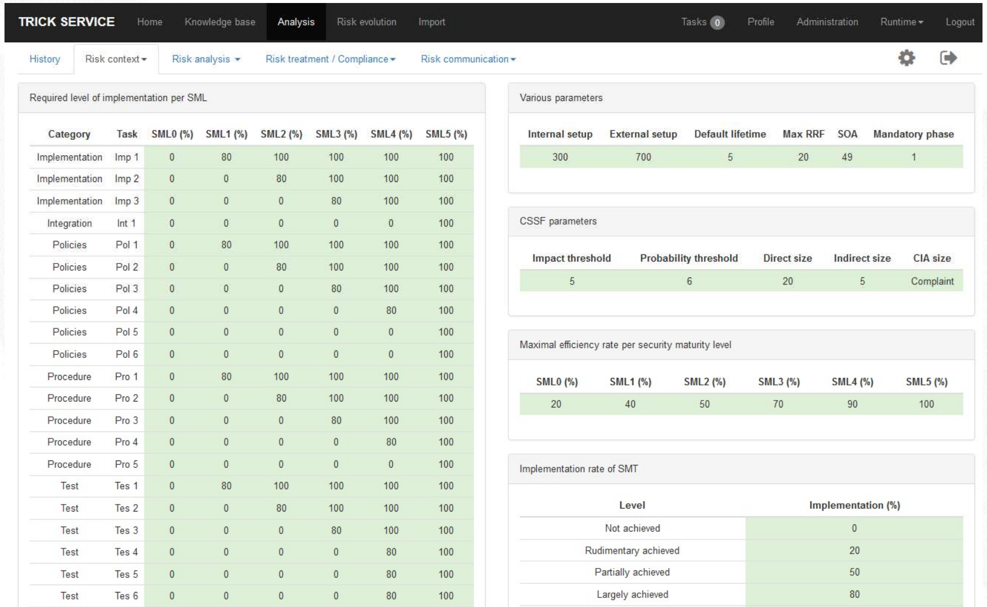

TRICK SERVICE
Home
Knowledge base
Analysis
Risk evolution
Import
Tasks 0
Profile
Administration
Runtime
Logout
Total ALE
ALE by scenario type
ALE by asset type
ALE By Scenario
ALE by asset
Compliance
ALE by Scenario
800 k€
600 k€
400 k€
200 k€
0 k€
ALE
A_all – Complete loss, including backup
A_1 – Partial loss or temporary
C2 – Deliberate disclosure
C3 – Accidental disclosure
C1 – Partial theft coming from external
I1 – External manipulation
I2 – Fraudulent manipulation coming from internal
I3 – Accidental manipulation
Demo Risk Analysis – 1.0
Demo Risk Analysis – 1.1.3

Risk evolution

Customer: Test-Company

Analysis: Demo Risk Analysis
Version: 1.0

Analysis: Demo Risk Analysis
Version: 1.1.3



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
Procedure	Pro 3	0	0	0	80	100	100
Procedure	Pro 4	0	0	0	0	80	100
Procedure	Pro 5	0	0	0	0	0	100
Test	Tes 1	0	80	100	100	100	100
Test	Tes 2	0	0	80	100	100	100
Test	Tes 3	0	0	0	80	100	100
Test	Tes 4	0	0	0	0	80	100
Test	Tes 5	0	0	0	0	80	100
Test	Tes 6	0	0	0	0	80	100

Various parameters

Internal setup	External setup	Default lifetime	Max RRF	SOA	Mandatory phase
300	700	5	20	49	1

CSSF parameters

Impact threshold	Probability threshold	Direct size	Indirect size	CIA size
5	6	20	5	Complaint

Maximal efficiency rate per security maturity level

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

Implementation rate of SMT

Level	Implementation (%)
Not achieved	0
Rudimentary achieved	20
Partially achieved	50
Largely achieved	80

TRICK Service

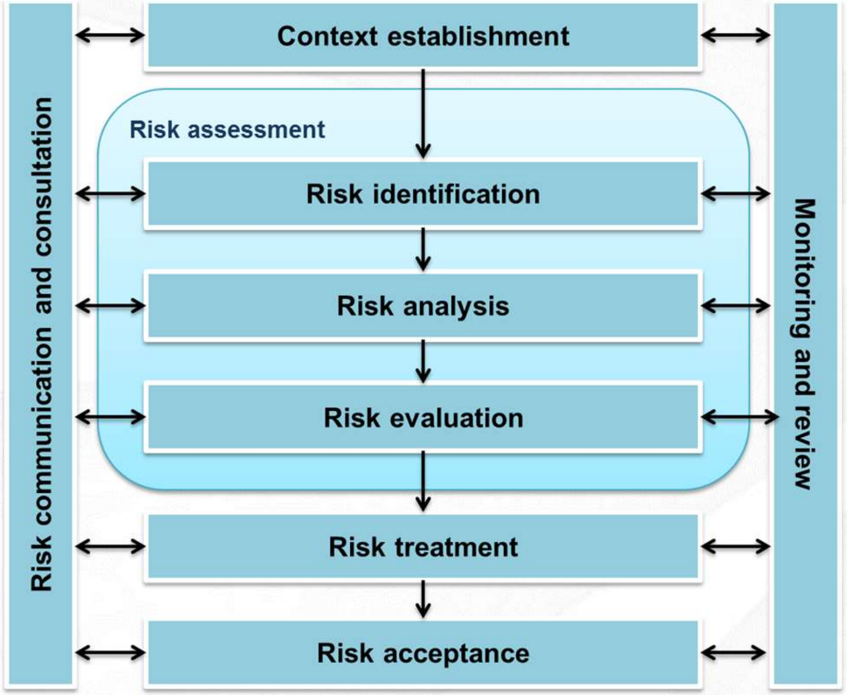
Overview

TRICK Service can be used to:

1. Document the organisational context & assets according to ISO/IEC **27005**;
2. Audit ISO/IEC **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 on selected **assets**;
7. Prepare a **risk treatment plan**, sorted by implementation phases and Return on Security Investment;
8. Generate **ILR-compliant JSON** file for Monarc, serima, and CSSF compliant reporting.
9. Prepare **Statement of applicability** for ISO/IEC 27001 certification;
10. Make a **Data protection impact assessment** (DPIA) compliant to GDPR.

TRICK Service

Methodology

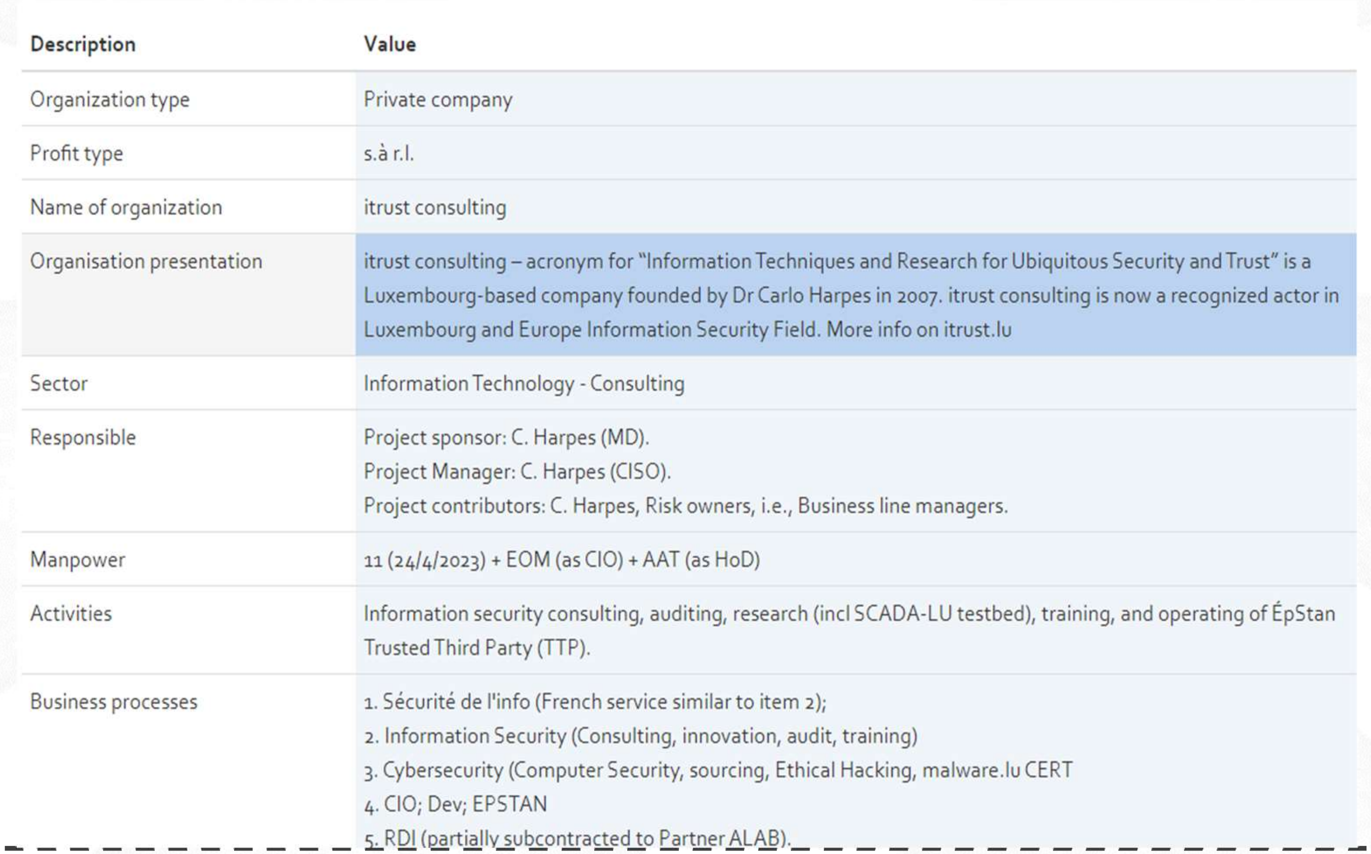


- **Follows the guidance of ISO/IEC 27005**
- **Is ISO/IEC 27001:2022 compliant**
- **Can be easily integrated in your Information Security Management System (ISMS)**
- **Prepares reporting to regulator (ILR, CSSF, CNPD, HCPN)**

TRICK Service

Context establishment – Risk analysis scope

Describe the context of your organisation

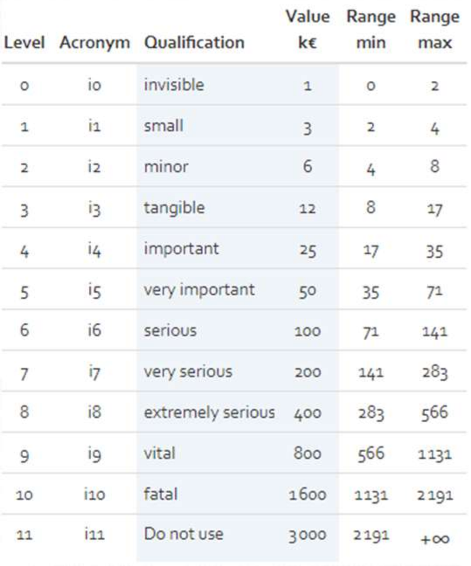


Description	Value
Organization type	Private company
Profit type	s.à r.l.
Name of organization	itrust consulting
Organisation presentation	itrust consulting – acronym for "Information Techniques and Research for Ubiquitous Security and Trust" is a Luxembourg-based company founded by Dr Carlo Harpes in 2007. itrust consulting is now a recognized actor in Luxembourg and Europe Information Security Field. More info on itrust.lu
Sector	Information Technology - Consulting
Responsible	Project sponsor: C. Harpes (MD). Project Manager: C. Harpes (CISO). Project contributors: C. Harpes, Risk owners, i.e., Business line managers.
Manpower	11 (24/4/2023) + EOM (as CIO) + AAT (as HoD)
Activities	Information security consulting, auditing, research (incl SCADA-LU testbed), training, and operating of ÉpStan Trusted Third Party (TTP).
Business processes	1. Sécurité de l'info (French service similar to item 2); 2. Information Security (Consulting, innovation, audit, training) 3. Cybersecurity (Computer Security, sourcing, Ethical Hacking, malware.lu CERT 4. CIO; Dev; EPSTAN 5. RDI (partially subcontracted to Partner ALAB).

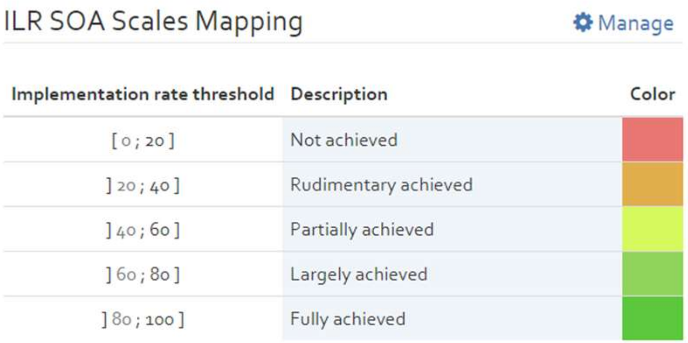
TRICK Service

Context establishment – Customisable parameters

Impact scale (CSSF compatible)



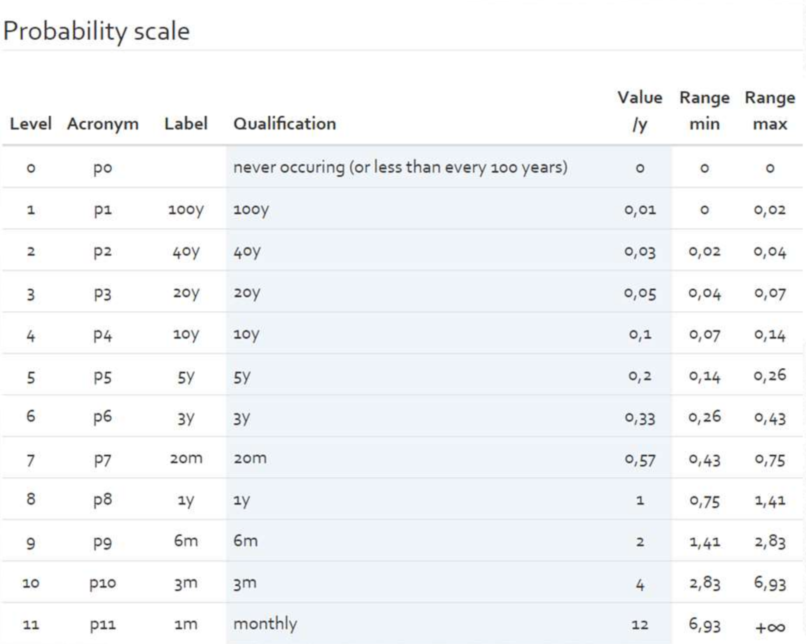
Level	Acronym	Qualification	Value k€	Range min	Range max
0	i0	invisible	1	0	2
1	i1	small	3	2	4
2	i2	minor	6	4	8
3	i3	tangible	12	8	17
4	i4	important	25	17	35
5	i5	very important	50	35	71
6	i6	serious	100	71	141
7	i7	very serious	200	141	283
8	i8	extremely serious	400	283	566
9	i9	vital	800	566	1131
10	i10	fatal	1600	1131	2191
11	i11	Do not use	3000	2191	+∞



ILR SOA Scales Mapping

Implementation rate threshold	Description	Color
[0 ; 20]	Not achieved	🟥
] 20 ; 40]	Rudimentary achieved	🟧
] 40 ; 60]	Partially achieved	🟨
] 60 ; 80]	Largely achieved	🟩
] 80 ; 100]	Fully achieved	🟩

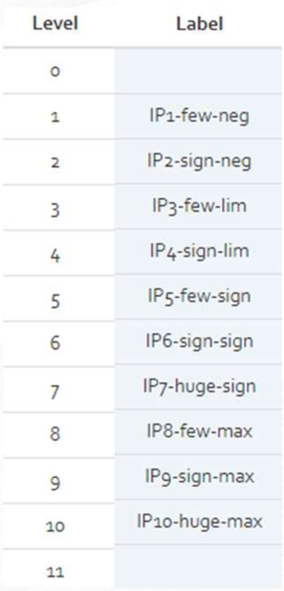
Probability scale (CSSF compatible)



Probability scale

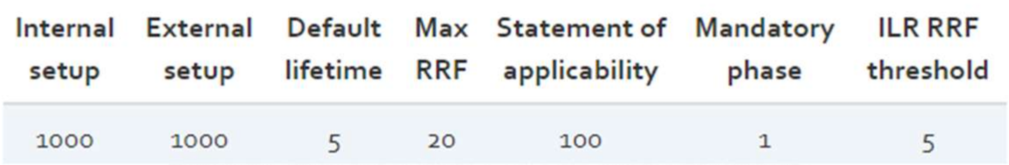
Level	Acronym	Label	Qualification	Value /y	Range min	Range max
0	p0		never occuring (or less than every 100 years)	0	0	0
1	p1	100y	100y	0,01	0	0,02
2	p2	40y	40y	0,03	0,02	0,04
3	p3	20y	20y	0,05	0,04	0,07
4	p4	10y	10y	0,1	0,07	0,14
5	p5	5y	5y	0,2	0,14	0,26
6	p6	3y	3y	0,33	0,26	0,43
7	p7	20m	20m	0,57	0,43	0,75
8	p8	1y	1y	1	0,75	1,41
9	p9	6m	6m	2	1,41	2,83
10	p10	3m	3m	4	2,83	6,93
11	p11	1m	monthly	12	6,93	+∞

Privacy scale



Level	Label
0	
1	IP1-few-neg
2	IP2-sign-neg
3	IP3-few-lim
4	IP4-sign-lim
5	IP5-few-sign
6	IP6-sign-sign
7	IP7-huge-sign
8	IP8-few-max
9	IP9-sign-max
10	IP10-huge-max
11	

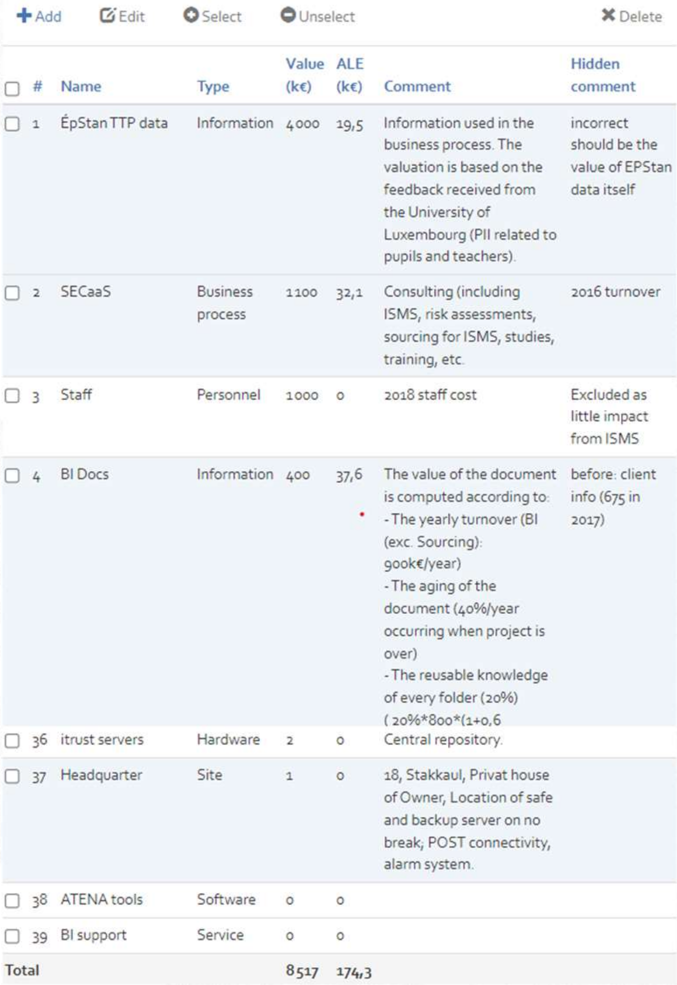
Various parameters



Internal setup	External setup	Default lifetime	Max RRF	Statement of applicability	Mandatory phase	ILR RRF threshold
1000	1000	5	20	100	1	5

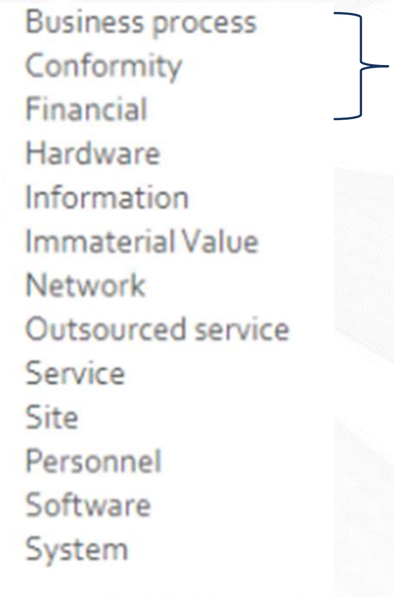
TRICK Service

Context establishment – Identification of assets to be considered



□	#	Name	Type	Value (k€)	ALE (k€)	Comment	Hidden comment
□	1	ÉpStan TTP data	Information	4000	19,5	Information used in the business process. The valuation is based on the feedback received from the University of Luxembourg (PII related to pupils and teachers).	incorrect should be the value of EPStan data itself
□	2	SECaaS	Business process	1100	32,1	Consulting (including ISMS, risk assessments, sourcing for ISMS, studies, training, etc.	2016 turnover
□	3	Staff	Personnel	1000	0	2018 staff cost	Excluded as little impact from ISMS
□	4	BI Docs	Information	400	37,6	The value of the document is computed according to: - The yearly turnover (BI (exc. Sourcing): 900k€/year) - The aging of the document (40%/year occurring when project is over) - The reusable knowledge of every folder (20%) (20%*800*(1+0,6	before: client info (675 in 2017)
□	36	itrust servers	Hardware	2	0	Central repository.	
□	37	Headquarter	Site	1	0	18, Stakkaul, Privat house of Owner, Location of safe and backup server on no break; POST connectivity, alarm system.	
□	38	ATENA tools	Software	0	0		
□	39	BI support	Service	0	0		
Total				8517	174,3		

Asset types



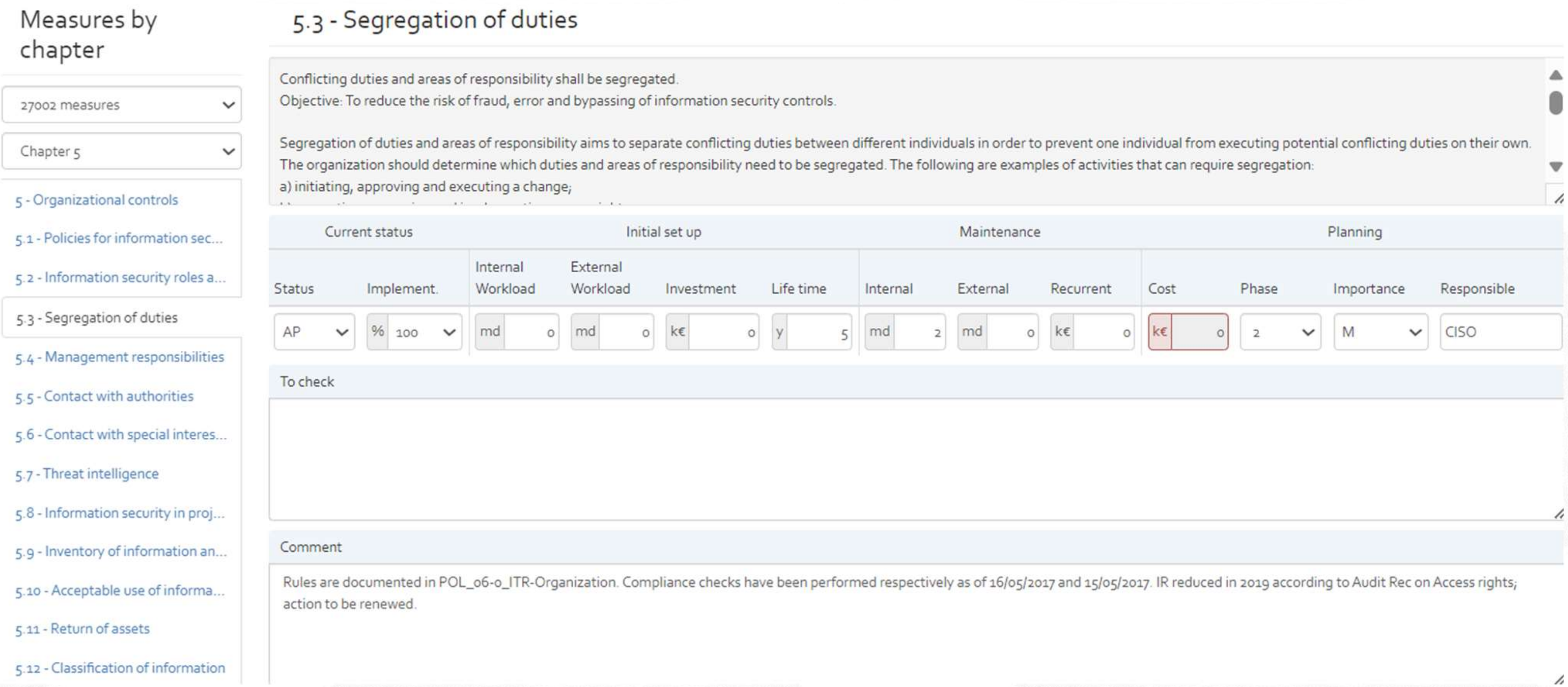
- Business process
- Conformity
- Financial
- Hardware
- Information
- Immaterial Value
- Network
- Outsourced service
- Service
- Site
- Personnel
- Software
- System

CSSF

TRICK Service

Security assessment

Select and estimate effectiveness and implementation cost of standardised and custom security controls



Measures by chapter

27002 measures

Chapter 5

5 - Organizational controls

5.1 - Policies for information sec...

5.2 - Information security roles a...

5.3 - Segregation of duties

5.4 - Management responsibilities

5.5 - Contact with authorities

5.6 - Contact with special interes...

5.7 - Threat intelligence

5.8 - Information security in proj...

5.9 - Inventory of information an...

5.10 - Acceptable use of informa...

5.11 - Return of assets

5.12 - Classification of information

5.3 - Segregation of duties

Conflicting duties and areas of responsibility shall be segregated.
Objective: To reduce the risk of fraud, error and bypassing of information security controls.

Segregation of duties and areas of responsibility aims to separate conflicting duties between different individuals in order to prevent one individual from executing potential conflicting duties on their own. The organization should determine which duties and areas of responsibility need to be segregated. The following are examples of activities that can require segregation:
a) initiating, approving and executing a change;

Current status		Initial set up				Maintenance			Planning			
Status	Implement.	Internal Workload	External Workload	Investment	Life time	Internal	External	Recurrent	Cost	Phase	Importance	Responsible
AP	% 100	md 0	md 0	k€ 0	y 5	md 2	md 0	k€ 0	k€ 0	2	M	CISO

To check

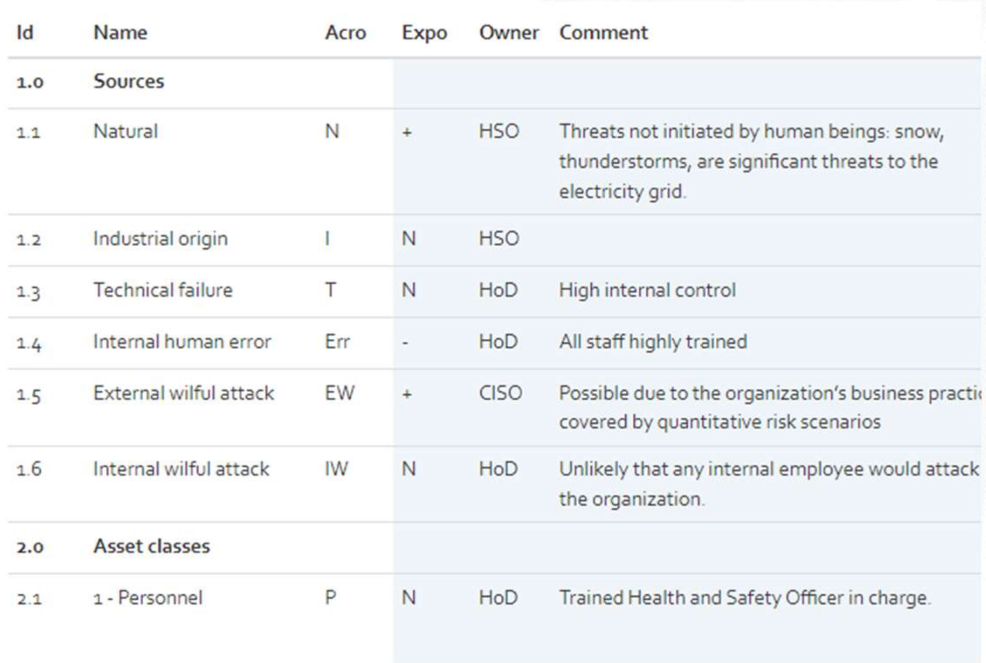
Comment

Rules are documented in POL_06-0_ITR-Organization. Compliance checks have been performed respectively as of 16/05/2017 and 15/05/2017. IR reduced in 2019 according to Audit Rec on Access rights; action to be renewed.

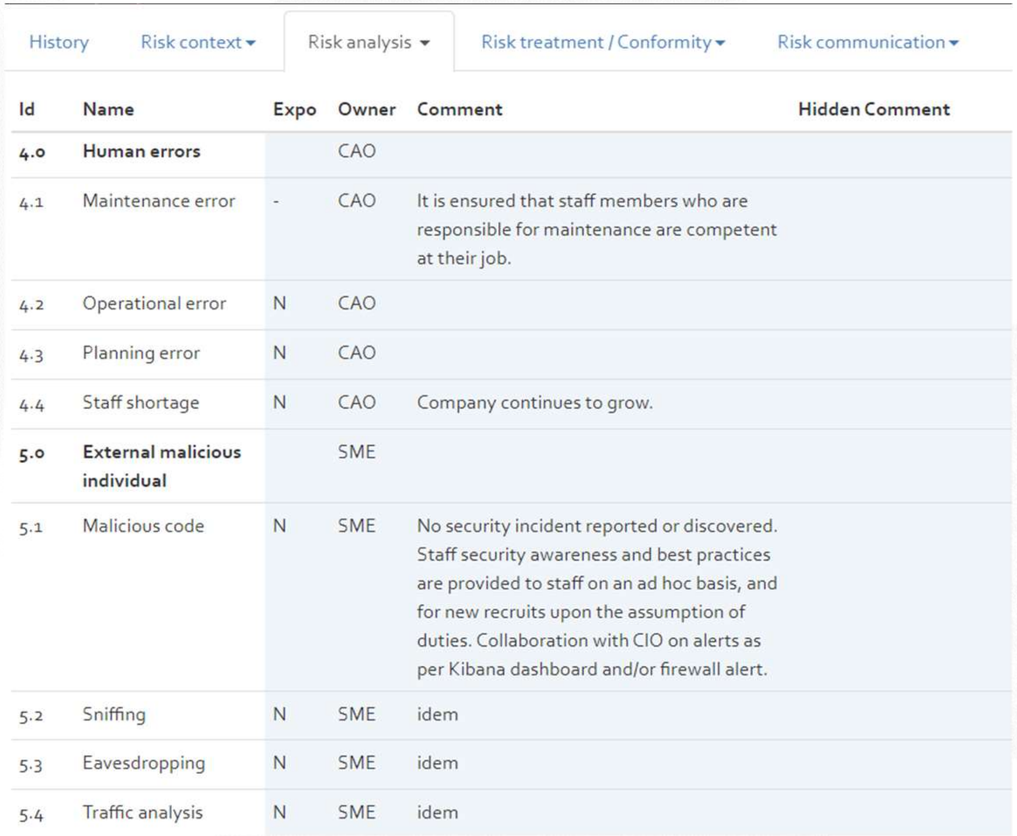
TRICK Service

Qualitative risk analysis

Qualitatively assess common threats, vulnerabilities, risks through structured brainstorming



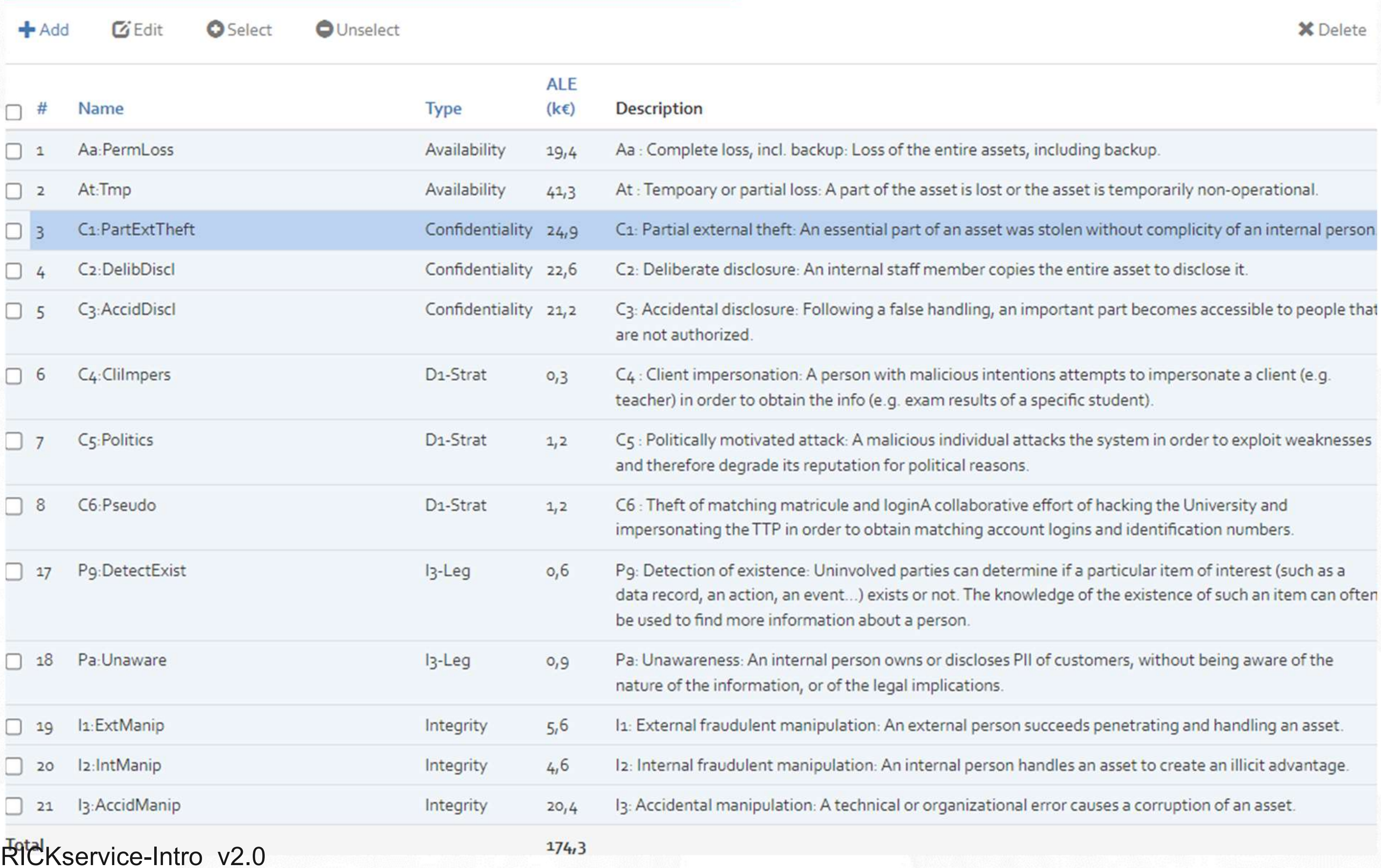
Id	Name	Acro	Expo	Owner	Comment
1.0	**Sources**				
1.1	Natural	N	+	HSO	Threats not initiated by human beings: snow, thunderstorms, are significant threats to the electricity grid.
1.2	Industrial origin	I	N	HSO	
1.3	Technical failure	T	N	HoD	High internal control
1.4	Internal human error	Err	-	HoD	All staff highly trained
1.5	External wilful attack	EW	+	CISO	Possible due to the organization's business practi covered by quantitative risk scenarios
1.6	Internal wilful attack	IW	N	HoD	Unlikely that any internal employee would attack the organization.
2.0	**Asset classes**				
2.1	1 - Personnel	P	N	HoD	Trained Health and Safety Officer in charge.



Id	Name	Expo	Owner	Comment	Hidden Comment
4.0	**Human errors**		CAO		
4.1	Maintenance error	-	CAO	It is ensured that staff members who are responsible for maintenance are competent at their job.	
4.2	Operational error	N	CAO		
4.3	Planning error	N	CAO		
4.4	Staff shortage	N	CAO	Company continues to grow.	
5.0	**External malicious individual**		SME		
5.1	Malicious code	N	SME	No security incident reported or discovered. Staff security awareness and best practices are provided to staff on an ad hoc basis, and for new recruits upon the assumption of duties. Collaboration with CIO on alerts as per Kibana dashboard and/or firewall alert.	
5.2	Sniffing	N	SME	idem	
5.3	Eavesdropping	N	SME	idem	
5.4	Traffic analysis	N	SME	idem	

TRICK Service

Risk identification for quantitative risk analysis

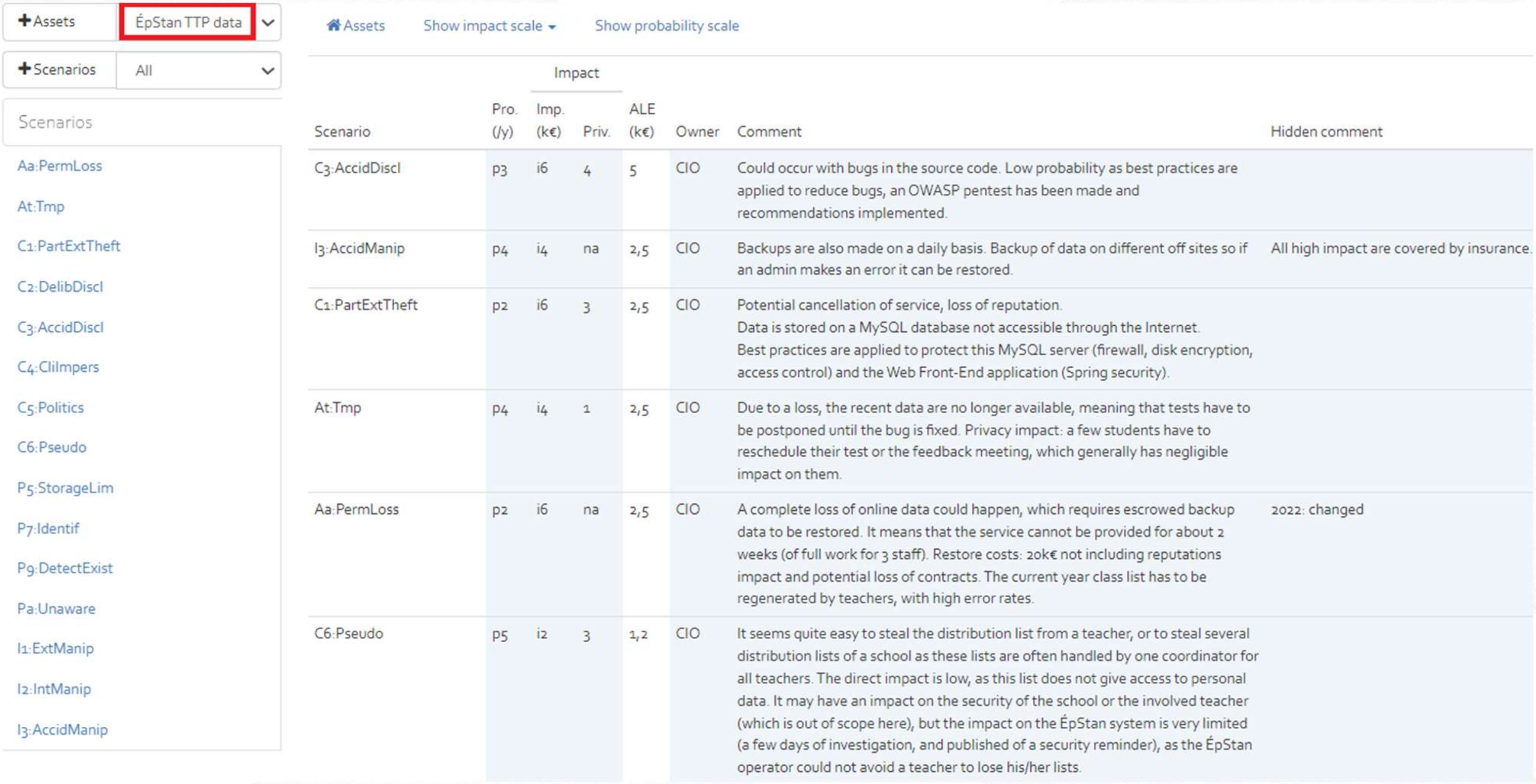


□	#	Name	Type	ALE (k€)	Description
□	1	Aa:PermLoss	Availability	19,4	Aa : Complete loss, incl. backup: Loss of the entire assets, including backup.
□	2	At:Tmp	Availability	41,3	At : Tempoary or partial loss: A part of the asset is lost or the asset is temporarily non-operational.
□	3	C1:PartExtTheft	Confidentiality	24,9	C1: Partial external theft: An essential part of an asset was stolen without complicity of an internal person
□	4	C2:DelibDiscl	Confidentiality	22,6	C2: Deliberate disclosure: An internal staff member copies the entire asset to disclose it.
□	5	C3:AccidDiscl	Confidentiality	21,2	C3: Accidental disclosure: Following a false handling, an important part becomes accessible to people that are not authorized.
□	6	C4:Clilmpers	D1-Strat	0,3	C4 : Client impersonation: A person with malicious intentions attempts to impersonate a client (e.g. teacher) in order to obtain the info (e.g. exam results of a specific student).
□	7	C5:Politics	D1-Strat	1,2	C5 : Politically motivated attack: A malicious individual attacks the system in order to exploit weaknesses and therefore degrade its reputation for political reasons.
□	8	C6:Pseudo	D1-Strat	1,2	C6 : Theft of matching matricule and loginA collaborative effort of hacking the University and impersonating the TTP in order to obtain matching account logins and identification numbers.
□	17	P9:DetectExist	I3-Leg	0,6	P9: Detection of existence: Uninvolved parties can determine if a particular item of interest (such as a data record, an action, an event...) exists or not. The knowledge of the existence of such an item can often be used to find more information about a person.
□	18	Pa:Unaware	I3-Leg	0,9	Pa: Unawareness: An internal person owns or discloses PII of customers, without being aware of the nature of the information, or of the legal implications.
□	19	I1:ExtManip	Integrity	5,6	I1: External fraudulent manipulation: An external person succeeds penetrating and handling an asset.
□	20	I2:IntManip	Integrity	4,6	I2: Internal fraudulent manipulation: An internal person handles an asset to create an illicit advantage.
□	21	I3:AccidManip	Integrity	20,4	I3: Accidental manipulation: A technical or organizational error causes a corruption of an asset.
Total				174,3	

TRICK Service

Assess your risks in term of impact & likelihood

Estimate your risks by asset ...



Scenarios

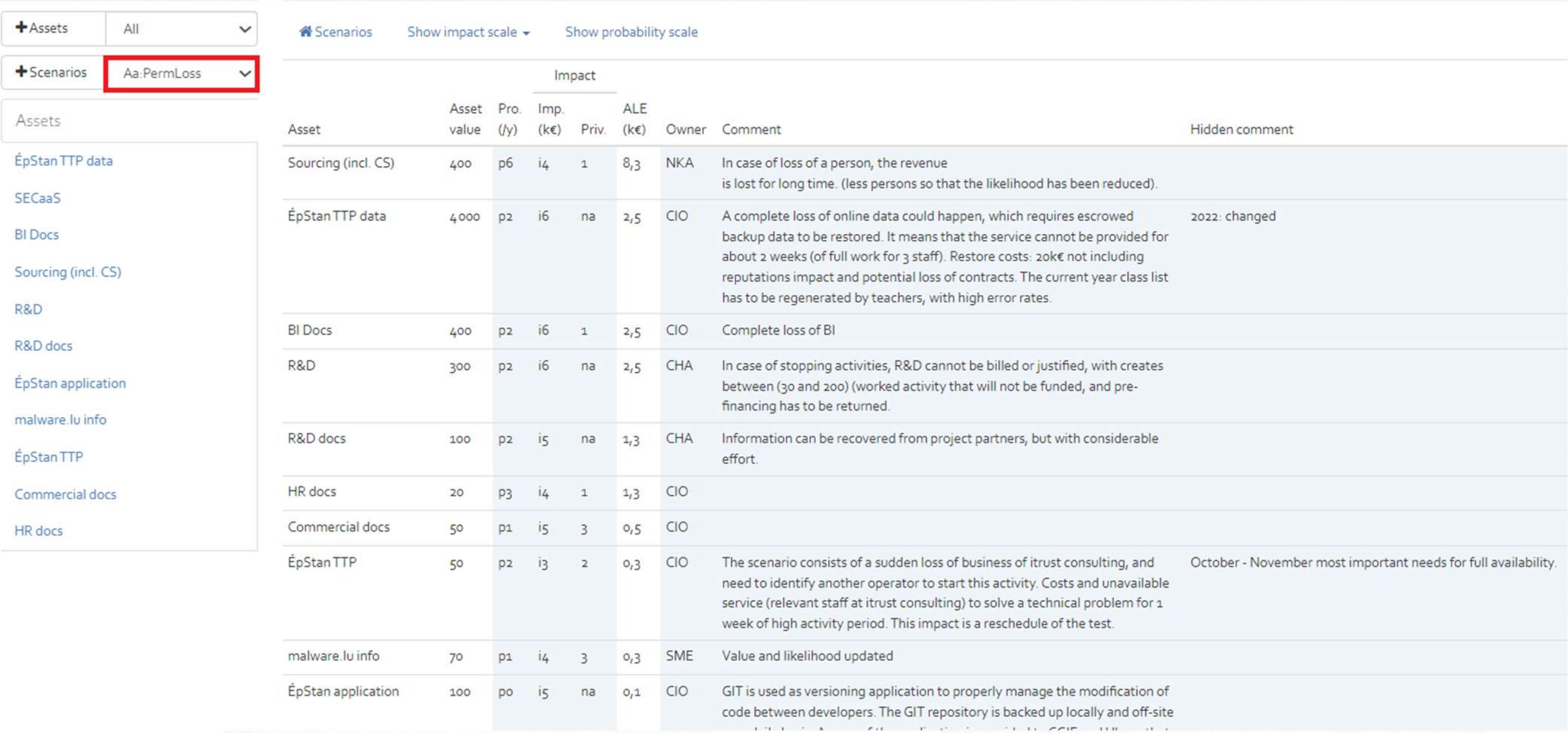
- Aa:PermLoss
- At:Tmp
- C1:PartExtTheft
- C2:DelibDiscl
- C3:AccidDiscl
- C4:CliImpers
- C5:Politics
- C6:Pseudo
- P5:StorageLim
- P7:Identif
- P9:DetectExist
- Pa:Unaware
- I1:ExtManip
- I2:IntManip
- I3:AccidManip

		Impact					
Scenario	Pro. (/y)	Imp. (k€)	Priv.	ALE (k€)	Owner	Comment	Hidden comment
C3:AccidDiscl	p3	i6	4	5	CIO	Could occur with bugs in the source code. Low probability as best practices are applied to reduce bugs, an OWASP pentest has been made and recommendations implemented.	
I3:AccidManip	p4	i4	na	2,5	CIO	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.	All high impact are covered by insurance.
C1:PartExtTheft	p2	i6	3	2,5	CIO	Potential cancellation of service, loss of reputation. Data is stored on a MySQL database not accessible through the Internet. Best practices are applied to protect this MySQL server (firewall, disk encryption, access control) and the Web Front-End application (Spring security).	
At:Tmp	p4	i4	1	2,5	CIO	Due to a loss, the recent data are no longer available, meaning that tests have to be postponed until the bug is fixed. Privacy impact: a few students have to reschedule their test or the feedback meeting, which generally has negligible impact on them.	
Aa:PermLoss	p2	i6	na	2,5	CIO	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 staff). Restore costs: 20k€ not including reputations impact and potential loss of contracts. The current year class list has to be regenerated by teachers, with high error rates.	2022: changed
C6:Pseudo	p5	i2	3	1,2	CIO	It seems quite easy to steal the distribution list from a teacher, or to steal several distribution lists of a school as these lists are often handled by one coordinator for all teachers. The direct impact is low, as this list does not give access to personal data. It may have an impact on the security of the school or the involved teacher (which is out of scope here), but the impact on the ÉpStan system is very limited (a few days of investigation, and published of a security reminder), as the ÉpStan operator could not avoid a teacher to lose his/her lists.	

TRICK Service

Assess your risks in term of impact & likelihood

... Or estimate your risk by risk scenario



			Impact					
Asset	Asset value	Pro. (/y)	Imp. (k€)	Priv.	ALE (k€)	Owner	Comment	Hidden comment
Sourcing (incl. CS)	400	p6	i4	1	8,3	NKA	In case of loss of a person, the revenue is lost for long time. (less persons so that the likelihood has been reduced).	
ÉpStan TTP data	4000	p2	i6	na	2,5	CIO	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 staff). Restore costs: 20k€ not including reputations impact and potential loss of contracts. The current year class list has to be regenerated by teachers, with high error rates.	2022: changed
BI Docs	400	p2	i6	1	2,5	CIO	Complete loss of BI	
R&D	300	p2	i6	na	2,5	CHA	In case of stopping activities, R&D cannot be billed or justified, with creates between (30 and 200) (worked activity that will not be funded, and pre-financing has to be returned.	
R&D docs	100	p2	i5	na	1,3	CHA	Information can be recovered from project partners, but with considerable effort.	
HR docs	20	p3	i4	1	1,3	CIO		
Commercial docs	50	p1	i5	3	0,5	CIO		
ÉpStan TTP	50	p2	i3	2	0,3	CIO	The scenario consists of a sudden loss of business of itrust consulting, and need to identify another operator to start this activity. Costs and unavailable service (relevant staff at itrust consulting) to solve a technical problem for 1 week of high activity period. This impact is a reschedule of the test.	October - November most important needs for full availability.
malware.lu info	70	p1	i4	3	0,3	SME	Value and likelihood updated	
ÉpStan application	100	p0	i5	na	0,1	CIO	GIT is used as versioning application to properly manage the modification of code between developers. The GIT repository is backed up locally and off-site	

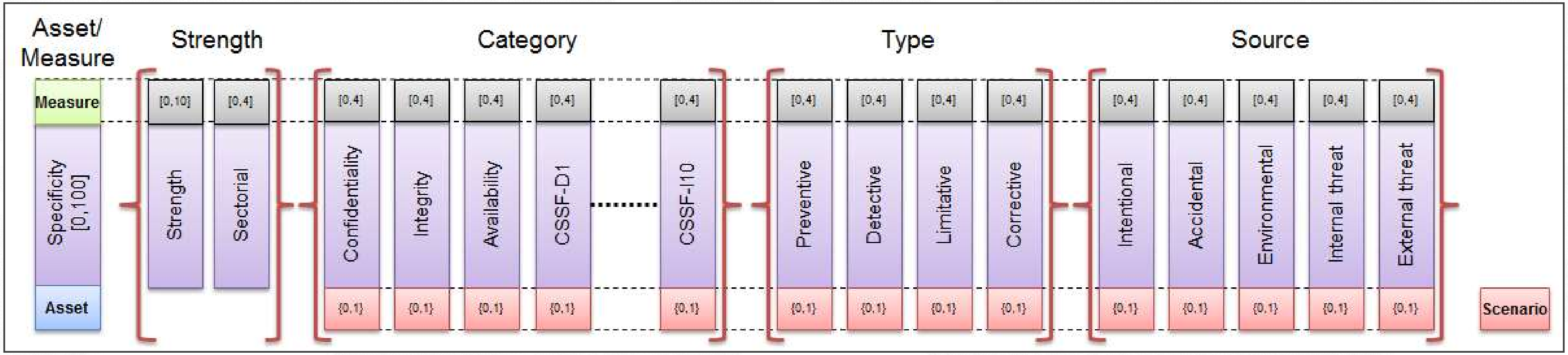
TRICK Service

Risk Reduction Factor

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.

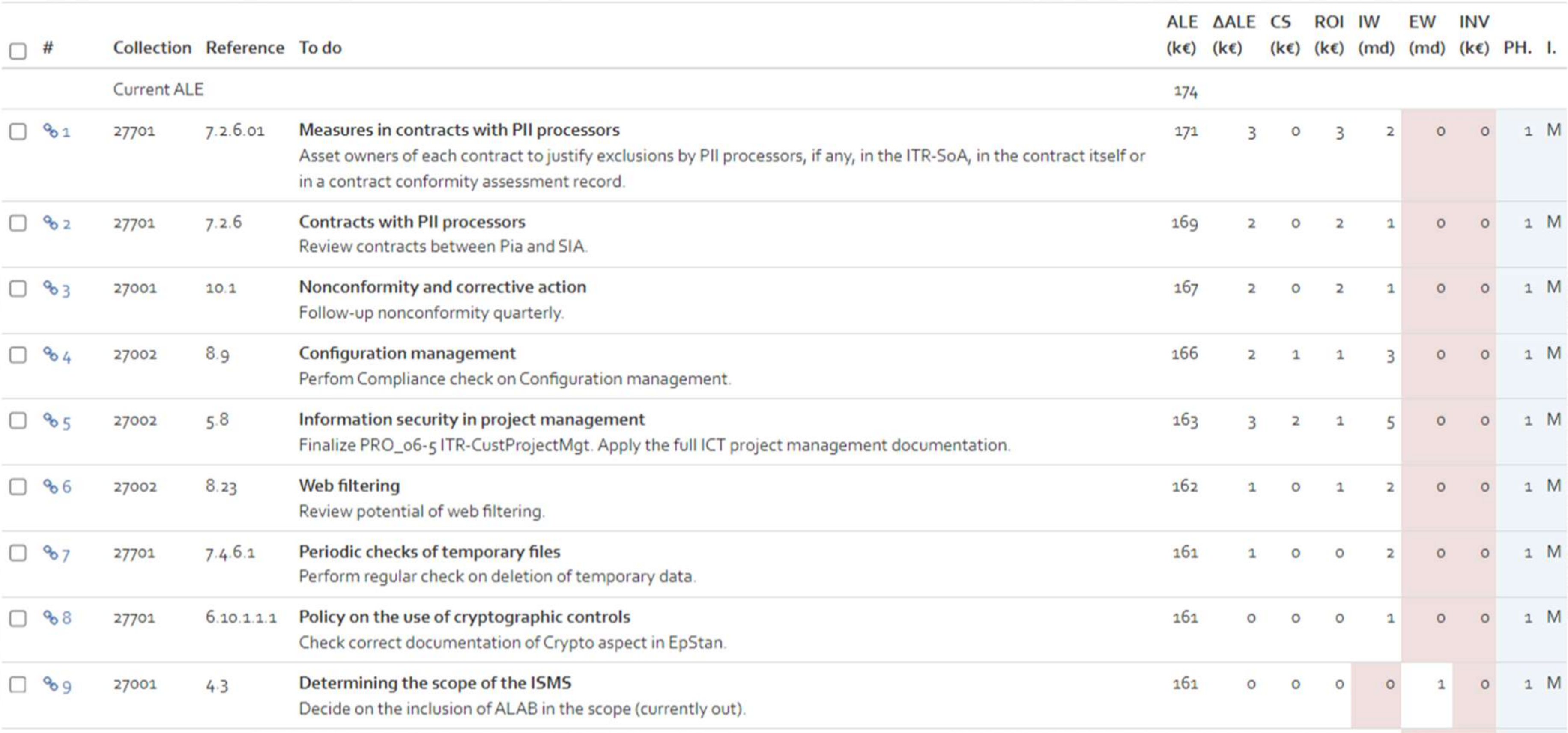
TRICK Service contains an estimate of RRF for each security measure, each risk, each asset type, which can be fine-tuned if needed.
Those estimates are based on properties of scenario, measures, and assets:



TRICK Service

Output: Risk treatment plan & Statement of Applicability

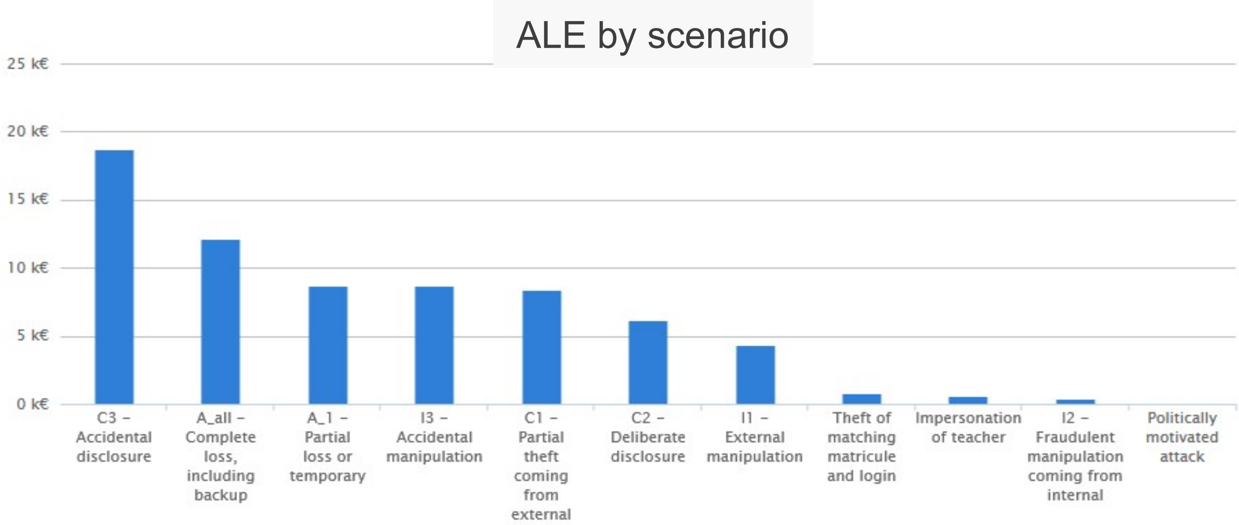
Risk treatment plan, sorted by implementation phase and ROSI

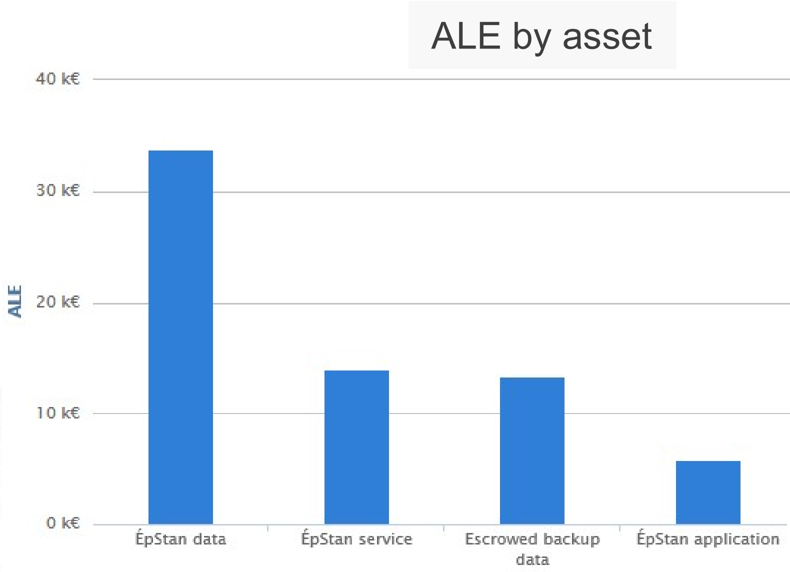


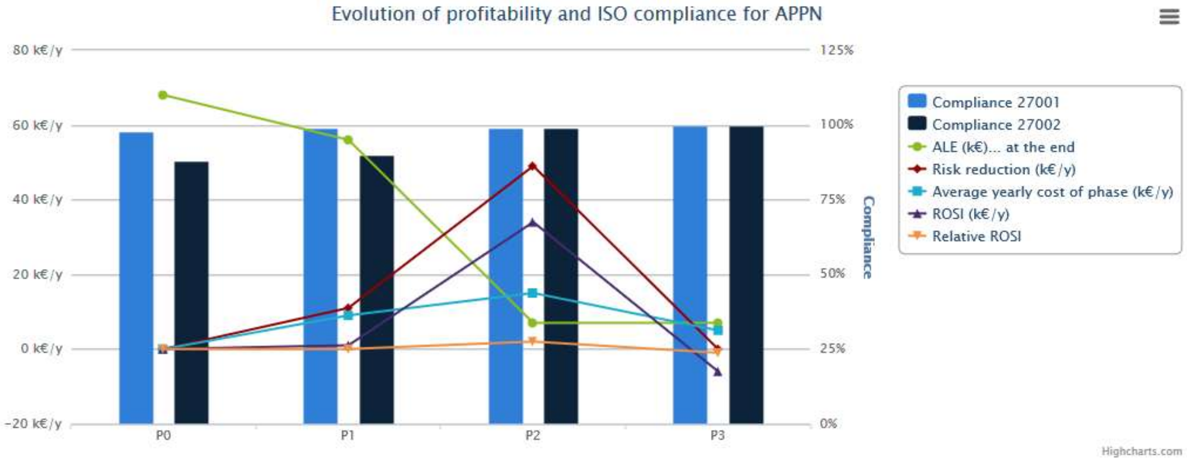
☐	#	Collection	Reference	To do	ALE	ΔALE	CS	ROI	IW	EW	INV	PH.	I.
					(k€)	(k€)	(k€)	(k€)	(md)	(md)	(k€)		
		Current ALE			174								
☐	1	27701	7.2.6.01	**Measures in contracts with PII processors** Asset owners of each contract to justify exclusions by PII processors, if any, in the ITR-SoA, in the contract itself or in a contract conformity assessment record.	171	3	0	3	2	0	0	1	M
☐	2	27701	7.2.6	**Contracts with PII processors** Review contracts between Pia and SIA.	169	2	0	2	1	0	0	1	M
☐	3	27001	10.1	**Nonconformity and corrective action** Follow-up nonconformity quarterly.	167	2	0	2	1	0	0	1	M
☐	4	27002	8.9	**Configuration management** Perfom Compliance check on Configuration management.	166	2	1	1	3	0	0	1	M
☐	5	27002	5.8	**Information security in project management** Finalize PRO_06-5 ITR-CustProjectMgt. Apply the full ICT project management documentation.	163	3	2	1	5	0	0	1	M
☐	6	27002	8.23	**Web filtering** Review potential of web filtering.	162	1	0	1	2	0	0	1	M
☐	7	27701	7.4.6.1	**Periodic checks of temporary files** Perform regular check on deletion of temporary data.	161	1	0	0	2	0	0	1	M
☐	8	27701	6.10.1.1.1	**Policy on the use of cryptographic controls** Check correct documentation of Crypto aspect in EpStan.	161	0	0	0	1	0	0	1	M
☐	9	27001	4.3	**Determining the scope of the ISMS** Decide on the inclusion of ALAB in the scope (currently out).	161	0	0	0	0	1	0	1	M

TRICK Service

Output: Key indicators







TRICK Service

Output: Privacy risks

Privacy risk heat map

Impact

11											
10-IP10-huge-max											
9-IP9-sign-max											
8-IP8-few-max											
7-IP7-huge-sign											
6-IP6-sign-sign			1								
5-IP5-few-sign			2	1							
4-IP4-sign-lim	1	1	1	1							
3-IP3-few-lim		1	3	8	5			1			
2-IP2-sign-neg	3	2		5		1					
1-IP1-few-neg		5	14	7	3	2		1	2		
	1-100y	2-40y	3-20y	4-10y	5-5y	6-3y	7-20m	8-12m	9-6m	10-3m	11-1m

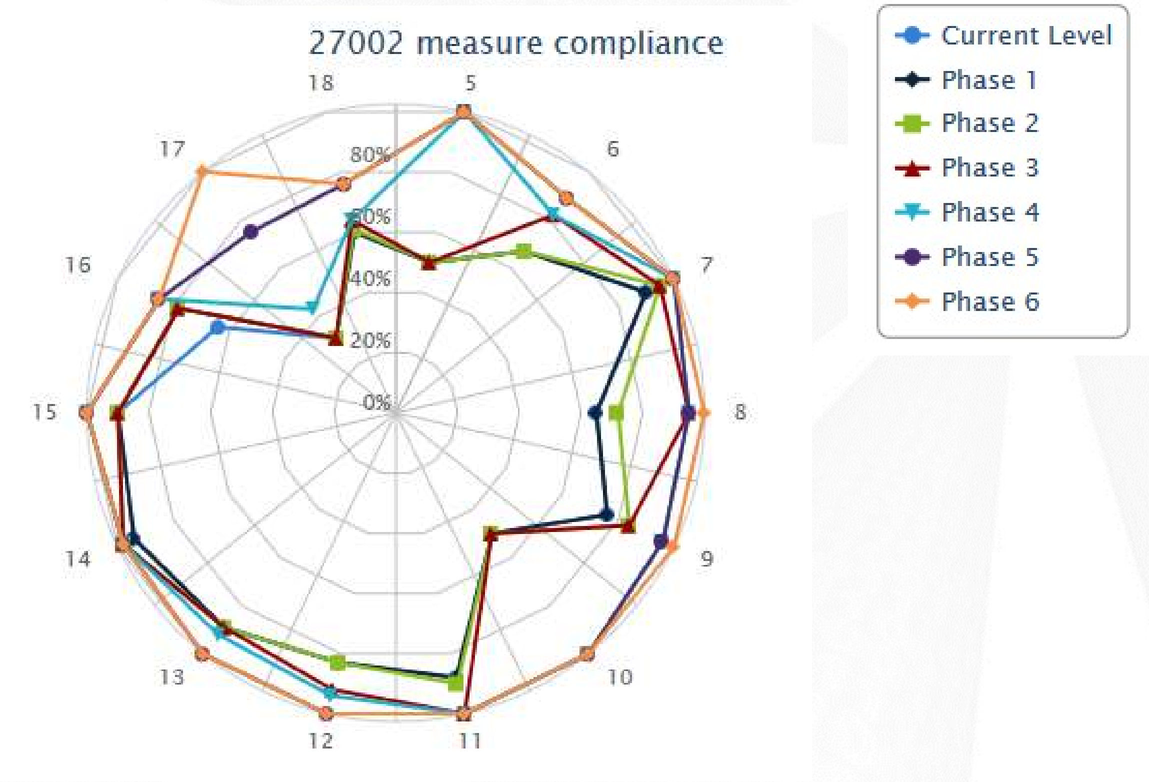
1/Probability

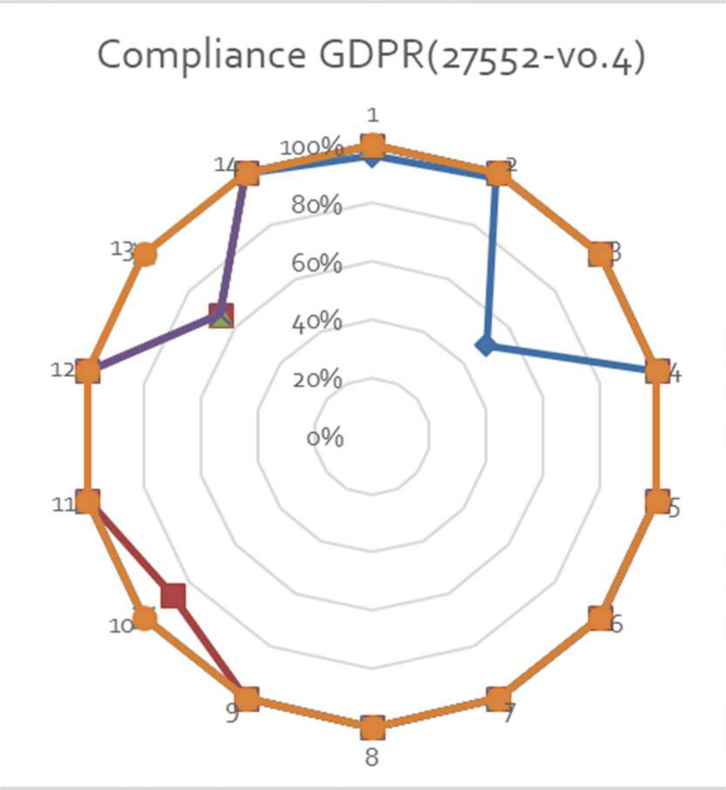
TRICK Service

Output: Key indicators

itrust consulting

Compliance evolution towards best practices and international standards

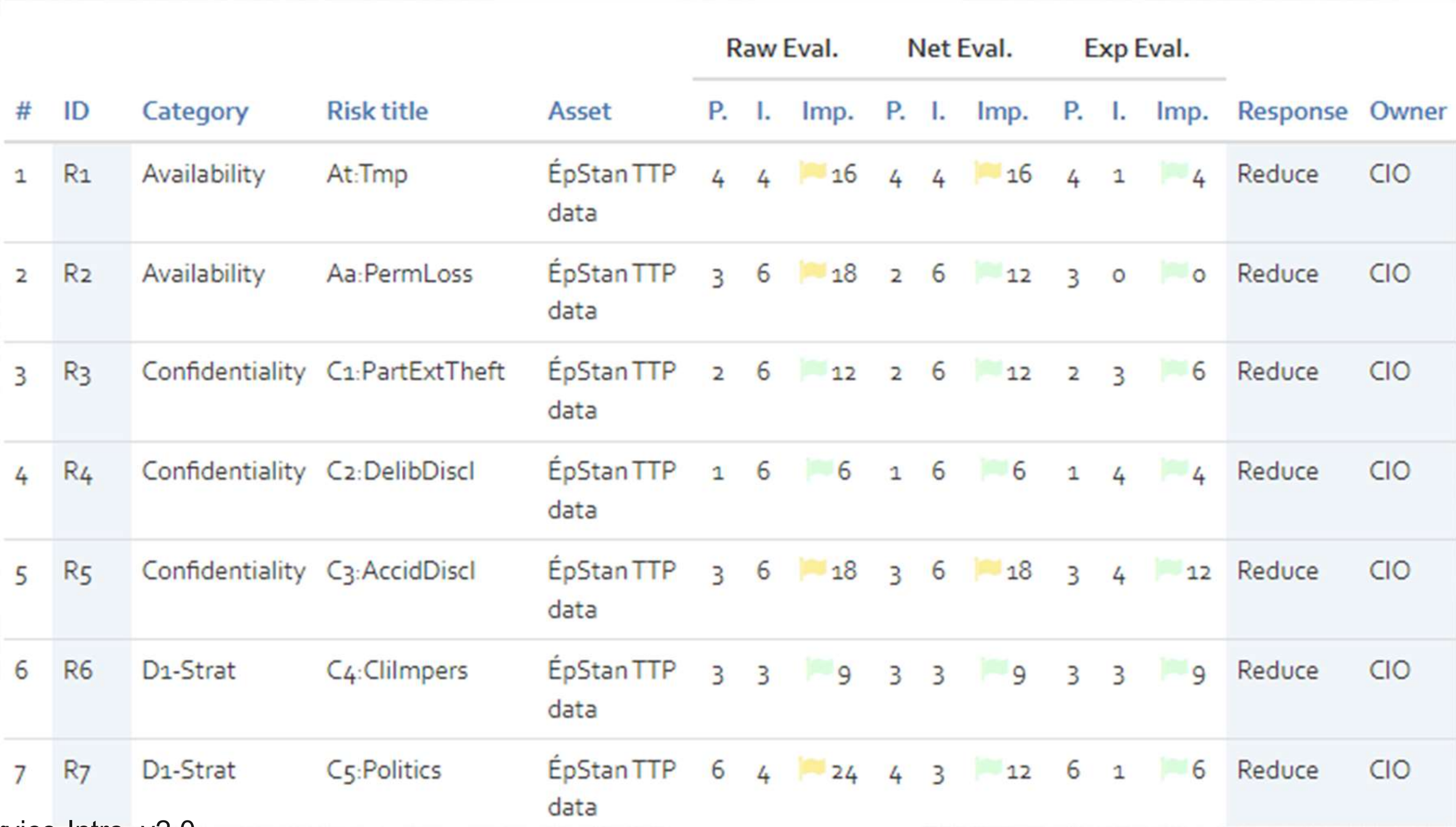




TRICK Service

Output

CSSF 12/544 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	R1	Availability	At:Tmp	ÉpStan TTP data	4	4	🟨 16	4	4	🟨 16	4	1	🟩 4	Reduce	CIO
2	R2	Availability	Aa:PermLoss	ÉpStan TTP data	3	6	🟨 18	2	6	🟩 12	3	0	🟩 0	Reduce	CIO
3	R3	Confidentiality	C1:PartExtTheft	ÉpStan TTP data	2	6	🟩 12	2	6	🟩 12	2	3	🟩 6	Reduce	CIO
4	R4	Confidentiality	C2:DelibDiscl	ÉpStan TTP data	1	6	🟩 6	1	6	🟩 6	1	4	🟩 4	Reduce	CIO
5	R5	Confidentiality	C3:AccidDiscl	ÉpStan TTP data	3	6	🟨 18	3	6	🟨 18	3	4	🟩 12	Reduce	CIO
6	R6	D1-Strat	C4:CliImpers	ÉpStan TTP data	3	3	🟩 9	3	3	🟩 9	3	3	🟩 9	Reduce	CIO
7	R7	D1-Strat	C5:Politics	ÉpStan TTP data	6	4	🟨 24	4	3	🟩 12	6	1	🟩 6	Reduce	CIO

TRICK Service

Output

Automatically export all results in a structured report

Management summary

1 Introduction

Context, Document objectives, Scope, Audience, Document structure, References, Acronyms, Glossary

2 Methodology and proceeding

2.1 Methodology

Context establishment

Risk assessment

Risk identification

Risk analysis

Risk evaluation

Risks treatment

Risk acceptance

2.2 Proceeding during the analysis

3 Context establishment

3.1 General considerations

3.2 Basic criteria

General risk assessment criteria

Impact criterion

Risk acceptance criterion

3.3 Description of the target

4 Risk assessment

4.1 Risk assessment meetings

4.2 Risk identification

Asset identification

Brainstorming

Threats exposure mapping

Vulnerabilities exposure mapping

Risk exposure mapping

4.3 Risk analysis

Risk scenarios and likelihood & impact scales

Overview of the risk analysis results

Typology of estimated risks

4.4 Risk evaluation

5 Risk treatment

5.1 General consideration regarding the identification of measures

Parameter tuning and outcome’s validation

A methodology based on profitability

5.2 Summary of treatment plan

5.3 Increase of compliance rate and profitability of the phases

5.4 Detailed risk treatment plan

6 Risk acceptance

7 Feedback loops of risk assessment process

7.1 Risk communication

7.2 Risk monitoring and review

8 Implementation level of security measures

8.1 Modus operandi

8.2 Evolution of the organisation’s compliance

Compliance level for ISO/IEC 27001

Compliance level for ISO/IEC 27002

Annexes: List of security measures applicable to the TOE

TRICK Service

ILR compliance

ILR compliant - Risk Analysis

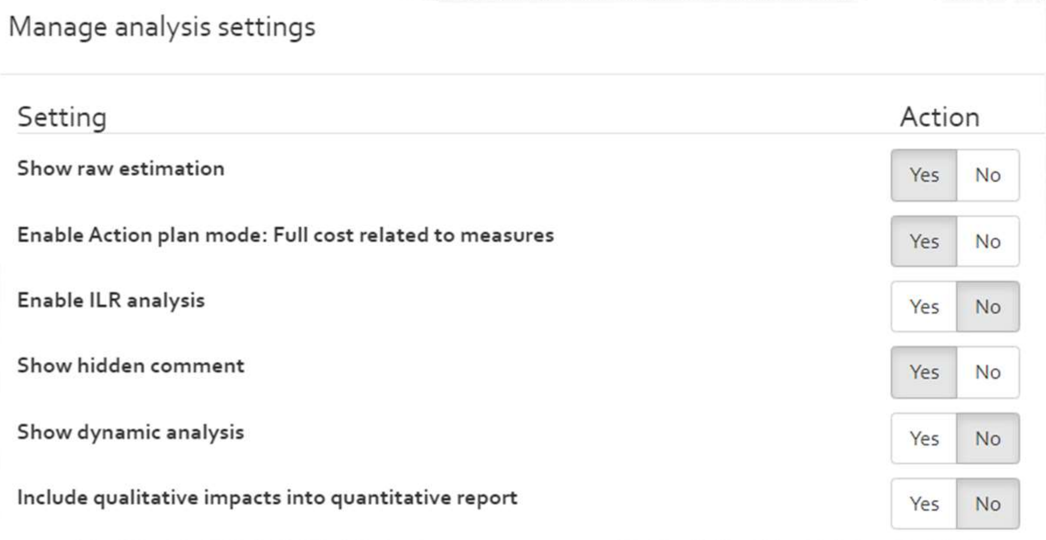
Trick Service has been enhanced for ILR compatible Risk Analysis export file generation by enhancing tool features such as:

- **Enabling** - ILR analysis in analysis settings.
- **Updating -** Likelihood and probability scales for ILR
- **Adding –** ILR compatible Export Format (JSON)
- **Enabling** – Export of JSON file for Serima
- **Supporting** – ILR Asset Dependency Model
- **Supporting** - ILR compliant Risk Assessment

TRICK Service

ILR compliance

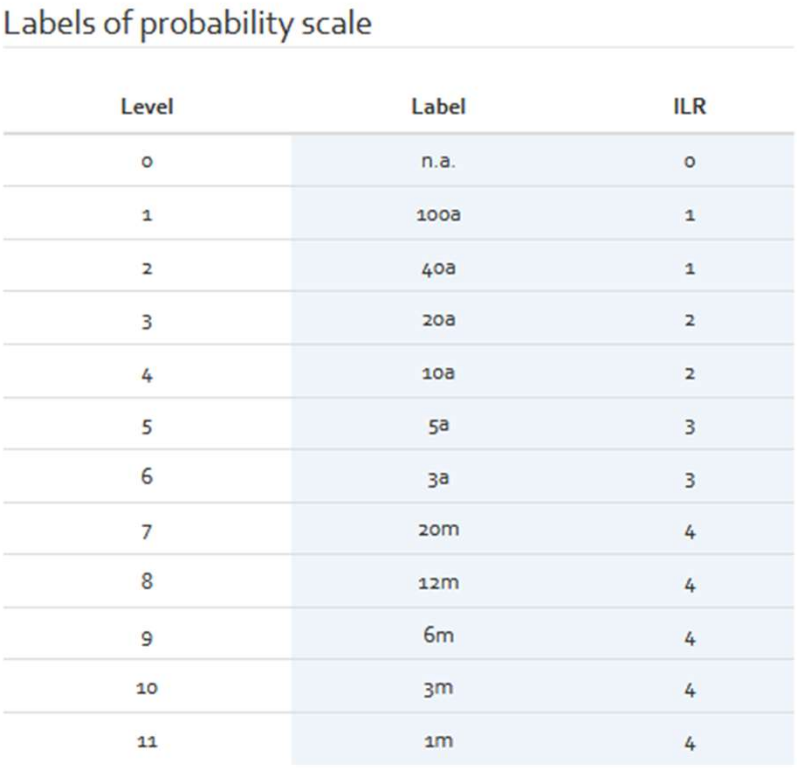
Enable ILR Analysis and Likelihood and probability scales



Manage analysis settings

Setting	Action
Show raw estimation	[✓ Yes] No
Enable Action plan mode: Full cost related to measures	[✓ Yes] No
Enable ILR analysis	Yes [✓ No]
Show hidden comment	[✓ Yes] No
Show dynamic analysis	Yes [✓ No]
Include qualitative impacts into quantitative report	Yes [✓ No]

Enable ILR Analysis



Labels of probability scale

Level	Label	ILR
0	n.a.	0
1	100a	1
2	40a	1
3	20a	2
4	10a	2
5	5a	3
6	3a	3
7	20m	4
8	12m	4
9	6m	4
10	3m	4
11	1m	4

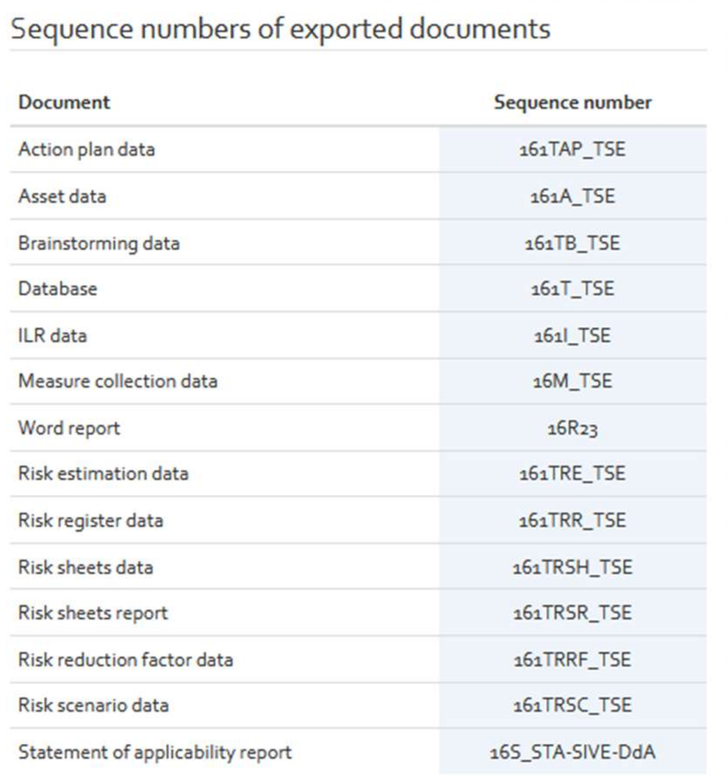
Likelihood and probability scales for ILR

TRICK Service

ILR compliance

ILR compatible Export Format

ILR compatible Export Format (ILR data)



Sequence numbers of exported documents

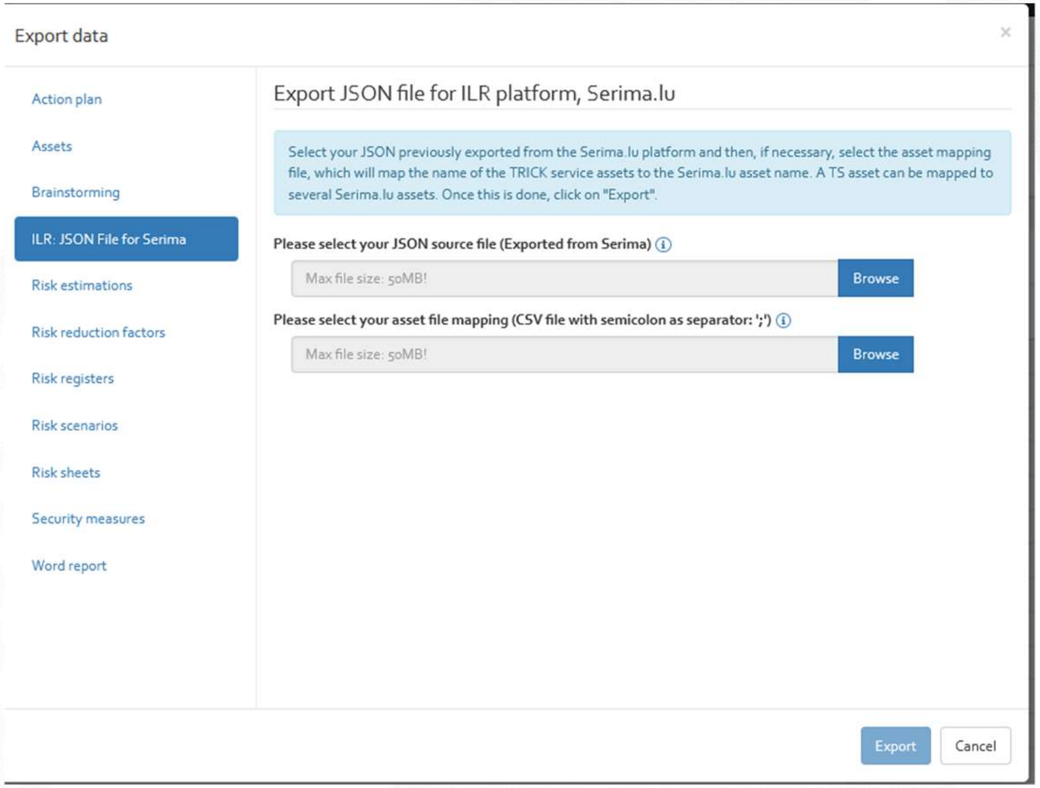
Document	Sequence number
Action plan data	161TAP_TSE
Asset data	161A_TSE
Brainstorming data	161TB_TSE
Database	161T_TSE
ILR data	161I_TSE
Measure collection data	16M_TSE
Word report	16R23
Risk estimation data	161TRE_TSE
Risk register data	161TRR_TSE
Risk sheets data	161TRSH_TSE
Risk sheets report	161TRSR_TSE
Risk reduction factor data	161TRRF_TSE
Risk scenario data	161TRSC_TSE
Statement of applicability report	16S_STA-SIVE-DdA

Work Flow:

- **Generate empty model of JSON file with scenarios assets etc.**
- **Trick injects information into empty model**
- **Export JSON from Trick**
- **Import JSON to Monarc**

Export of JSON file for Serima

Export Interface



Export data

Export JSON file for ILR platform, Serima.lu

Select your JSON previously exported from the Serima.lu platform and then, if necessary, select the asset mapping file, which will map the name of the TRICK service assets to the Serima.lu asset name. A TS asset can be mapped to several Serima.lu assets. Once this is done, click on "Export".

Please select your JSON source file (Exported from Serima) ⓘ

Max file size: 50MB!

Please select your asset file mapping (CSV file with semicolon as separator: ';') ⓘ

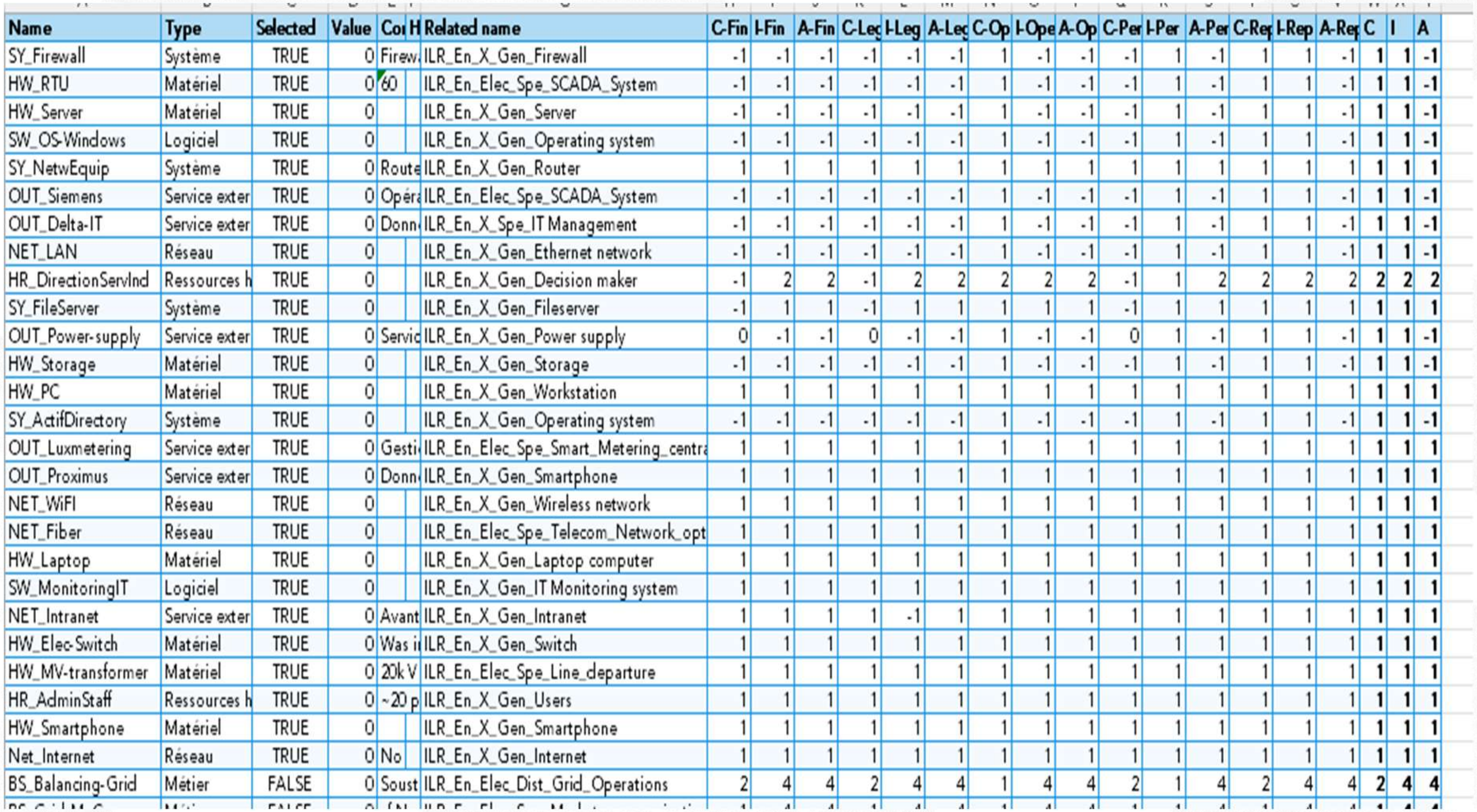
Max file size: 50MB!

Provide JSON file for Serima as input and additional CSV asset mapping file to generate the JSON file which can be imported to Monarc/Serima platform.

TRICK Service

ILR compliance

ILR Asset Dependency Model



Name	Type	Selected	Value	Coı	H	Related name	C-Fin	I-Fin	A-Fin	C-Leg	I-Leg	A-Leg	C-Op	I-Ope	A-Op	C-Per	I-Per	A-Per	C-Rep	I-Rep	A-Rep	C	I	A
SY_Firewall	Système	TRUE	0	Firew:		ILR_En_X_Gen_Firewall	-1	-1	-1	-1	-1	-1	1	-1	-1	-1	1	-1	1	1	-1	**1**	**1**	**-1**
HW_RTU	Matériel	TRUE	0	60		ILR_En_Elec_Spe_SCADA_System	-1	-1	-1	-1	-1	-1	1	-1	-1	-1	1	-1	1	1	-1	**1**	**1**	**-1**
HW_Server	Matériel	TRUE	0			ILR_En_X_Gen_Server	-1	-1	-1	-1	-1	-1	1	-1	-1	-1	1	-1	1	1	-1	**1**	**1**	**-1**
SW_OS-Windows	Logiciel	TRUE	0			ILR_En_X_Gen_Operating system	-1	-1	-1	-1	-1	-1	1	-1	-1	-1	1	-1	1	1	-1	**1**	**1**	**-1**
SY_NetwEquip	Système	TRUE	0	Route		ILR_En_X_Gen_Router	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**1**	**1**	**1**
OUT_Siemens	Service exter	TRUE	0	Opéra		ILR_En_Elec_Spe_SCADA_System	-1	-1	-1	-1	-1	-1	1	-1	-1	-1	1	-1	1	1	-1	**1**	**1**	**-1**
OUT_Delta-IT	Service exter	TRUE	0	Donn		ILR_En_X_Spe_IT Management	-1	-1	-1	-1	-1	-1	1	-1	-1	-1	1	-1	1	1	-1	**1**	**1**	**-1**
NET_LAN	Réseau	TRUE	0			ILR_En_X_Gen_Ethernet network	-1	-1	-1	-1	-1	-1	1	-1	-1	-1	1	-1	1	1	-1	**1**	**1**	**-1**
HR_DirectionServInd	Ressources h	TRUE	0			ILR_En_X_Gen_Decision maker	-1	2	2	-1	2	2	2	2	2	-1	1	2	2	2	2	**2**	**2**	**2**
SY_FileServer	Système	TRUE	0			ILR_En_X_Gen_Fileserver	-1	1	1	-1	1	1	1	1	1	-1	1	1	1	1	1	**1**	**1**	**1**
OUT_Power-supply	Service exter	TRUE	0	Servic		ILR_En_X_Gen_Power supply	0	-1	-1	0	-1	-1	1	-1	-1	0	1	-1	1	1	-1	**1**	**1**	**-1**
HW_Storage	Matériel	TRUE	0			ILR_En_X_Gen_Storage	-1	-1	-1	-1	-1	-1	1	-1	-1	-1	1	-1	1	1	-1	**1**	**1**	**-1**
HW_PC	Matériel	TRUE	0			ILR_En_X_Gen_Workstation	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**1**	**1**	**1**
SY_ActifDirectory	Système	TRUE	0			ILR_En_X_Gen_Operating system	-1	-1	-1	-1	-1	-1	1	-1	-1	-1	1	-1	1	1	-1	**1**	**1**	**-1**
OUT_Luxmetering	Service exter	TRUE	0	Gesti		ILR_En_Elec_Spe_Smart_Metering_centra	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**1**	**1**	**1**
OUT_Proximus	Service exter	TRUE	0	Donn		ILR_En_X_Gen_Smartphone	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**1**	**1**	**1**
NET_WiFI	Réseau	TRUE	0			ILR_En_X_Gen_Wireless network	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**1**	**1**	**1**
NET_Fiber	Réseau	TRUE	0			ILR_En_Elec_Spe_Telecom_Network_opt	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**1**	**1**	**1**
HW_Laptop	Matériel	TRUE	0			ILR_En_X_Gen_Laptop computer	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**1**	**1**	**1**
SW_MonitoringIT	Logiciel	TRUE	0			ILR_En_X_Gen_IT Monitoring system	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**1**	**1**	**1**
NET_Intranet	Service exter	TRUE	0	Avant		ILR_En_X_Gen_Intranet	1	1	1	1	-1	1	1	1	1	1	1	1	1	1	1	**1**	**1**	**1**
HW_Elec-Switch	Matériel	TRUE	0	Was i		ILR_En_X_Gen_Switch	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**1**	**1**	**1**
HW_MV-transformer	Matériel	TRUE	0	20k V		ILR_En_Elec_Spe_Line_departure	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**1**	**1**	**1**
HR_AdminStaff	Ressources h	TRUE	0	~20 p		ILR_En_X_Gen_Users	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**1**	**1**	**1**
HW_Smartphone	Matériel	TRUE	0			ILR_En_X_Gen_Smartphone	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**1**	**1**	**1**
Net_Internet	Réseau	TRUE	0	No		ILR_En_X_Gen_Internet	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**1**	**1**	**1**
BS_Balancing-Grid	Métier	FALSE	0	Soust		ILR_En_Elec_Dist_Grid_Operations	2	4	4	2	4	4	1	4	4	2	1	4	2	4	4	**2**	**4**	**4**

Alignment of Monarc dependency model

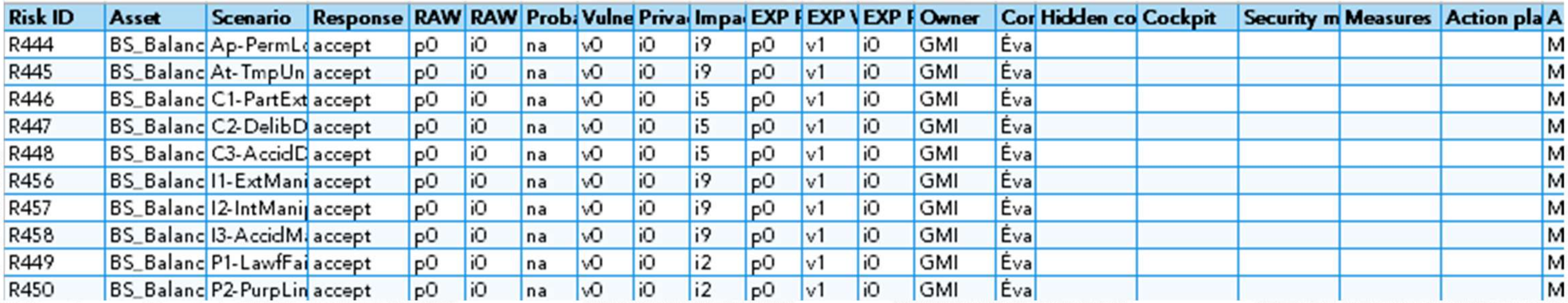
- **Adding parameters to asset import file**
- **Mapping of Trick Name to Monarc name is configurable**

TRICK Service

ILR compliance

ILR compliant Risk Assessment

Defining the threat and vulnerability for the ILR risk assessment.



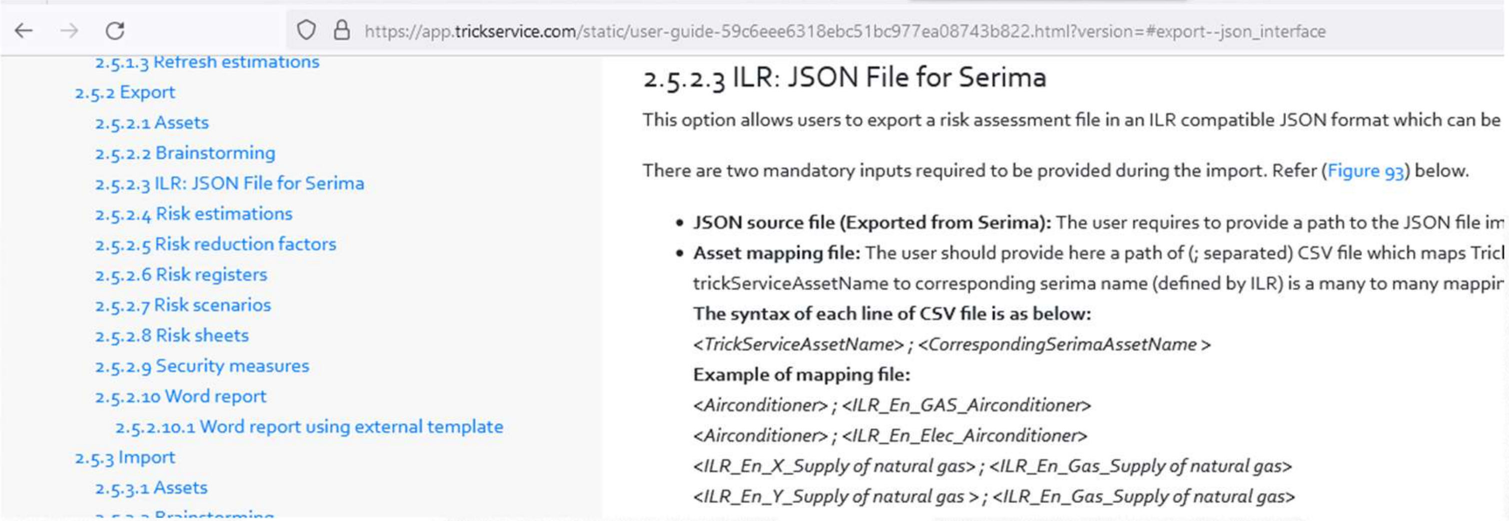
Risk ID	Asset	Scenario	Response	RAW	RAW	Proba	Vulne	Priva	Impa	EXP P	EXP V	EXP I	Owner	Cor	Hidden co	Cockpit	Security m	Measures	Action pla	A
R444	BS_Balanc	Ap-PermL	accept	p0	i0	na	v0	i0	i9	p0	v1	i0	GMI	Éva						M
R445	BS_Balanc	At-TmpUn	accept	p0	i0	na	v0	i0	i9	p0	v1	i0	GMI	Éva						M
R446	BS_Balanc	C1-PartExt	accept	p0	i0	na	v0	i0	i5	p0	v1	i0	GMI	Éva						M
R447	BS_Balanc	C2-DelibD	accept	p0	i0	na	v0	i0	i5	p0	v1	i0	GMI	Éva						M
R448	BS_Balanc	C3-AccidD	accept	p0	i0	na	v0	i0	i5	p0	v1	i0	GMI	Éva						M
R456	BS_Balanc	I1-ExtMani	accept	p0	i0	na	v0	i0	i9	p0	v1	i0	GMI	Éva						M
R457	BS_Balanc	I2-IntMani	accept	p0	i0	na	v0	i0	i9	p0	v1	i0	GMI	Éva						M
R458	BS_Balanc	I3-AccidM	accept	p0	i0	na	v0	i0	i9	p0	v1	i0	GMI	Éva						M
R449	BS_Balanc	P1-LawfFai	accept	p0	i0	na	v0	i0	i2	p0	v1	i0	GMI	Éva						M
R450	BS_Balanc	P2-PurpLin	accept	p0	i0	na	v0	i0	i2	p0	v1	i0	GMI	Éva						M

TRICK Service

ILR compliance

ILR compliance – Additional information in User Guide.

All these features have been explained in a comprehensive user guide included in the product.



https://app.trickservice.com/static/user-guide-59c6eee6318ebc51bc977ea08743b822.html?version=#export--json_interface

2.5.1.3 Refresh estimations
2.5.2 Export
2.5.2.1 Assets
2.5.2.2 Brainstorming
2.5.2.3 ILR: JSON File for Serima
2.5.2.4 Risk estimations
2.5.2.5 Risk reduction factors
2.5.2.6 Risk registers
2.5.2.7 Risk scenarios
2.5.2.8 Risk sheets
2.5.2.9 Security measures
2.5.2.10 Word report
2.5.2.10.1 Word report using external template
2.5.3 Import
2.5.3.1 Assets
2.5.3.2 Brainstorming

2.5.2.3 ILR: JSON File for Serima

This option allows users to export a risk assessment file in an ILR compatible JSON format which can be

There are two mandatory inputs required to be provided during the import. Refer (Figure 93) below.

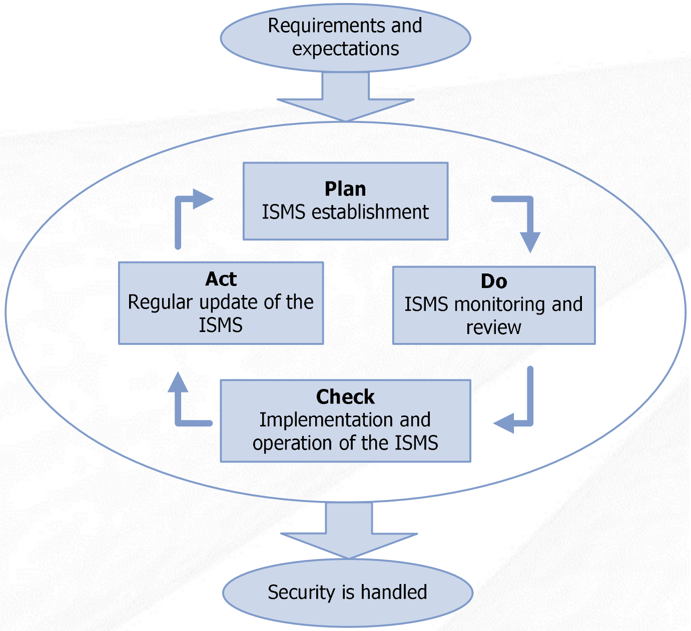
- **JSON source file (Exported from Serima):** The user requires to provide a path to the JSON file im
- **Asset mapping file:** The user should provide here a path of (; separated) CSV file which maps Tricl trickServiceAssetName to corresponding serima name (defined by ILR) is a many to many mappir
  The syntax of each line of CSV file is as below:
  <TrickServiceAssetName> ; <CorrespondingSerimaAssetName >
  Example of mapping file:
  <Airconditioner> ; <ILR_En_GAS_Airconditioner>
  <Airconditioner> ; <ILR_En_Elec_Airconditioner>
  <ILR_En_X_Supply of natural gas> ; <ILR_En_Gas_Supply of natural gas>
  <ILR_En_Y_Supply of natural gas > ; <ILR_En_Gas_Supply of natural gas>

TRICK Service

Continuous improvement

Update and fine-tune yearly your Risk Assessment

Continously improve with TRICK Service:



Requirements and expectations

Plan
ISMS establishment

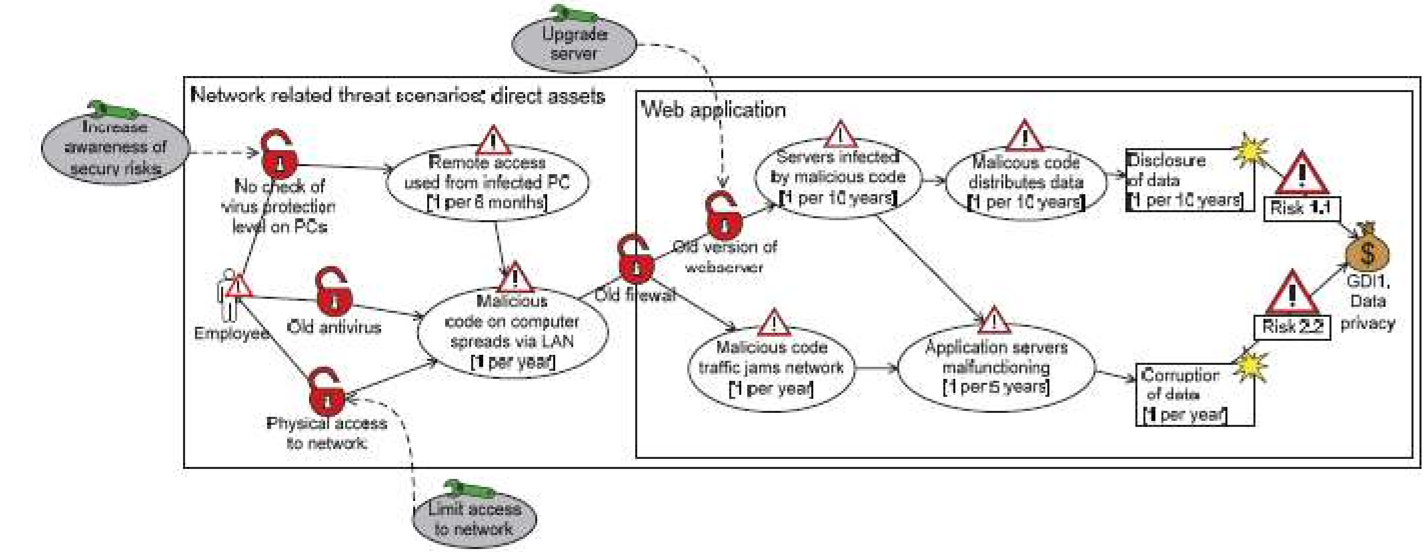
Do
ISMS monitoring and review

Check
Implementation and operation of the ISMS

Act
Regular update of the ISMS

Security is handled

Improve by modeling critical parts, e.g. with CORAS, attack 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
Malicious code traffic jams network [1 per year]
Application servers malfunctioning [1 per 5 years]
Corruption of data [1 per year]
Risk 2.2
$
GDI1, Data privacy

itrust consulting

TRICK Service

For further information on TRICK Service, please do not hesitate to contact us.

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

Tel: +352 26 176 212
Fax: +352 26 710 978
Web: www.itrust.lu