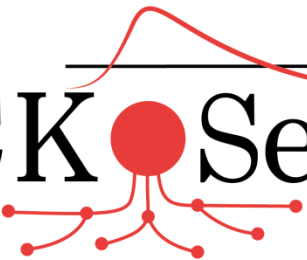




TRICK Service



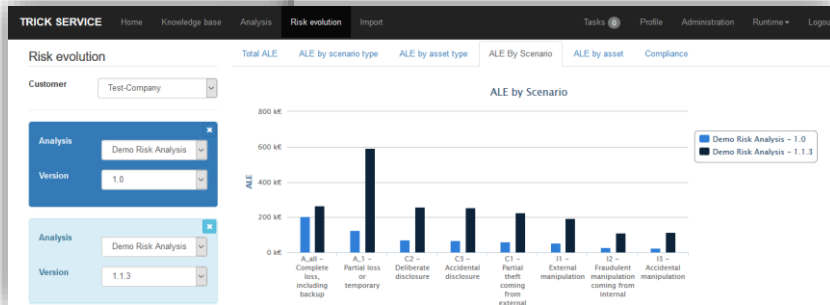
Product overview

TRICK Service

Tool for Risk management of an ISMS based on a Central Knowledge base



Welcome!



© 2016 itrust consulting - All Rights Reserved

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	Test 1	0	80	100	100	100	100
Test	Test 2	0	0	80	100	100	100
Test	Test 3	0	0	0	80	100	100
Test	Test 4	0	0	0	0	80	100
Test	Test 5	0	0	0	0	80	100
Test	Test 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

CISF parameters

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

Maximal efficiency rate per security maturity level

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

Implementation rate of SMT

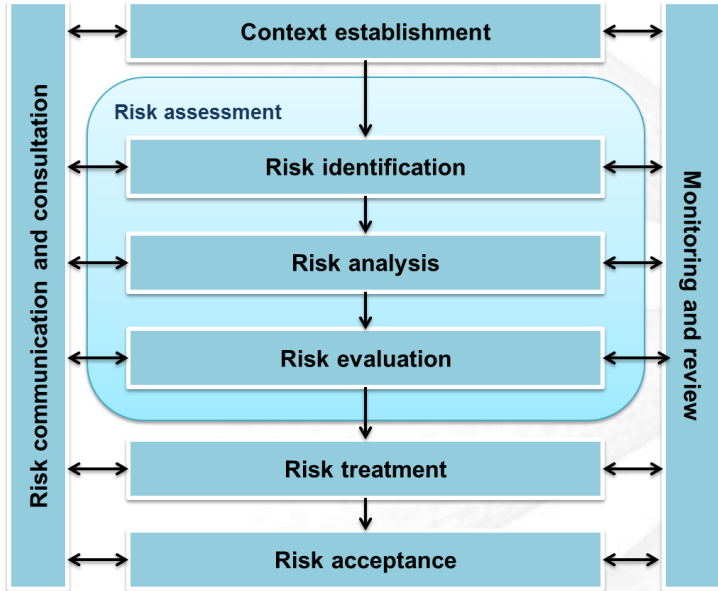
Level	Implementation (%)
Not achieved	0
Rudimentary achieved	20
Partially achieved	50
Largely achieved	80

TRICK Service 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 applied to selected assets;
7. Prepare a risk treatment plan, sorted by implementation phases and Return on Security Investment;
8. Prepare Statement of applicability for ISO/IEC 27001 certification;
9. Prepare risk analysis report compliant to CSSF circular 12/544
10. Assess security maturity.

TRICK Service

Methodology



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

Describe the context of 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;

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

+ Add Edit Estimation Select Unselect						
<input type="checkbox"/>	#	Name	Type	Value (k€)	ALE (k€)	Comment
<input type="checkbox"/>	1	ÉpStan application	SW	65	5,7	Application developed internally by itrust consulting.
<input type="checkbox"/>	2	ÉpStan data	Info	40	32,4	Information used in the business process
<input type="checkbox"/>	3	ÉpStan service	Busi	10	13,9	Value based on the yearly revenue generated from the service.
<input type="checkbox"/>	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).

Select and estimate effectiveness and implementation cost of standardised and custom security 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, audits 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

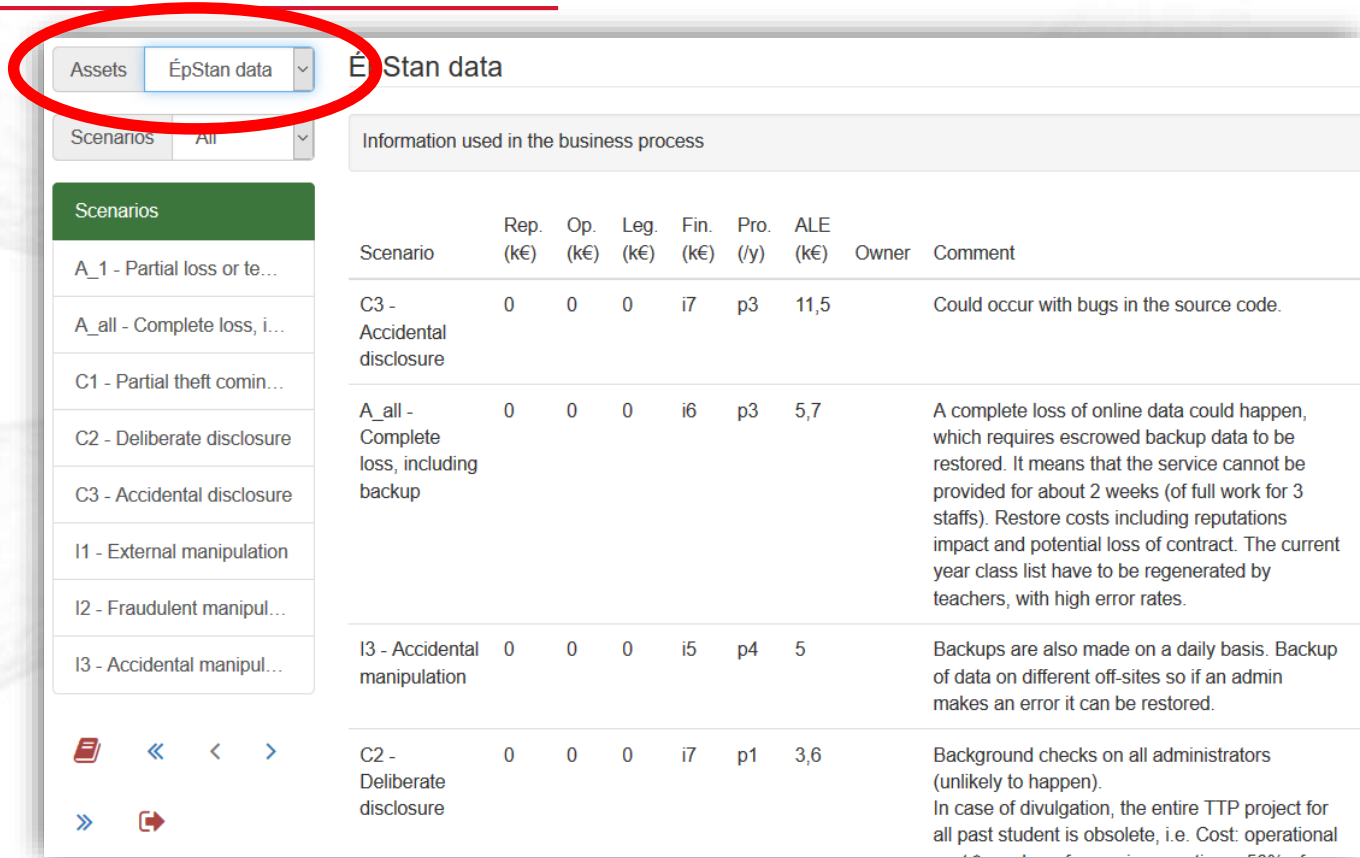
Qualitatively assess common threats and vulnerabilities, through structured brainstorming

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 Niederaanven or Berbourg.
1.0.2	Industrial origin	I	+		Petrol station in close proximity to Niederaanven 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).

Define risk scenarios

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

Estimate your risks by asset ...



Assets ÉpStan data É Stan data

Scenarios All

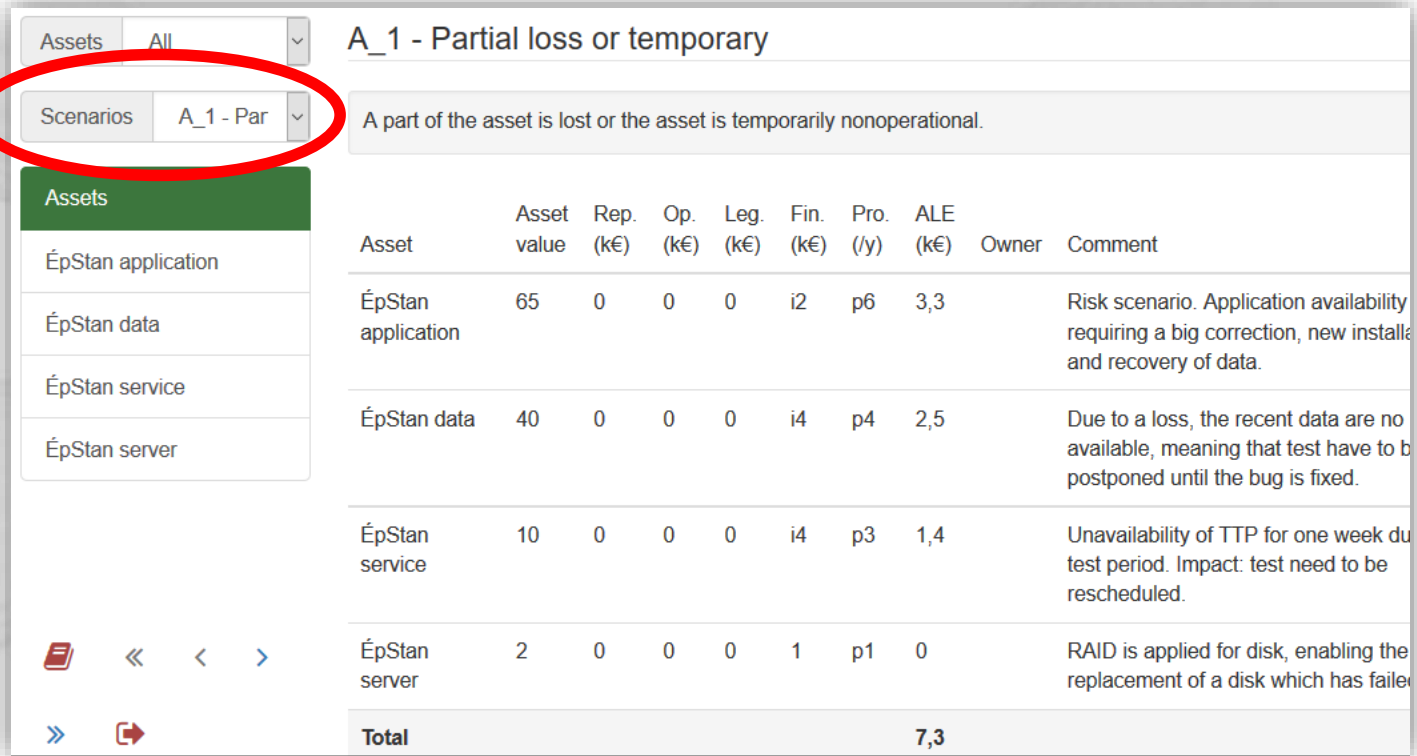
Information used in the business process

Scenario	Rep. (k€)	Op. (k€)	Leg. (k€)	Fin. (k€)	Pro. (/y)	ALE (k€)	Owner	Comment
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...								
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

Assess your risks in term of impact & likelihood

... Or estimate your risk by risk 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.

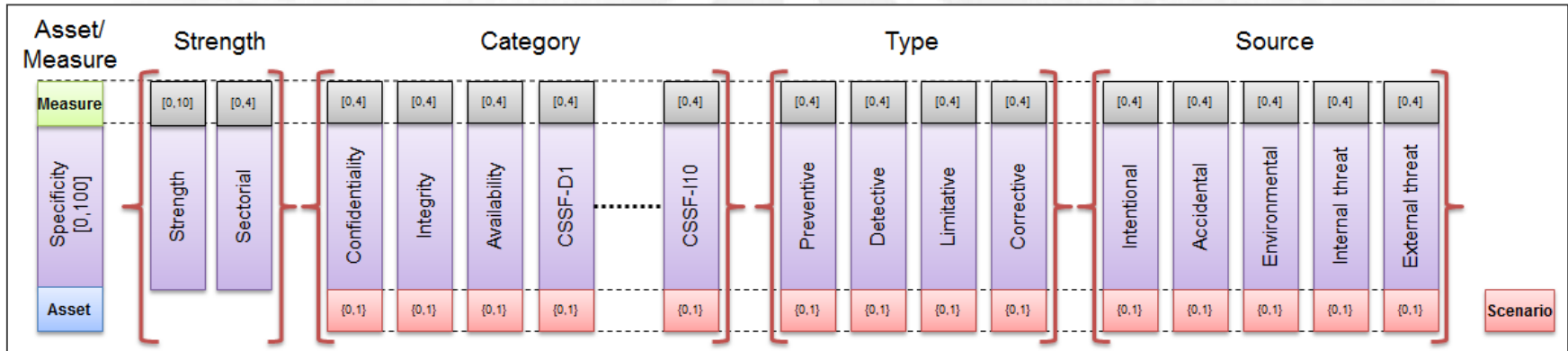
Asset	Asset value	Rep. (k€)	Op. (k€)	Leg. (k€)	Fin. (k€)	Pro. (/y)	ALE (k€)	Owner	Comment
ÉpStan application	65	0	0	0	i2	p6	3,3		Risk scenario. Application availability requiring a big correction, new installation and recovery of data.
ÉpStan data	40	0	0	0	i4	p4	2,5		Due to a loss, the recent data are no available, meaning that test have to be postponed until the bug is fixed.
ÉpStan service	10	0	0	0	i4	p3	1,4		Unavailability of TTP for one week during 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 failed.
Total							7,3		

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:



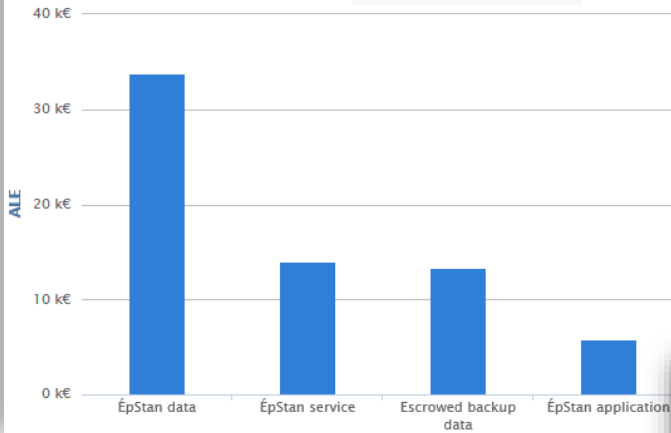
Risk treatment plan, sorted by implementation phase and ROSI

#	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

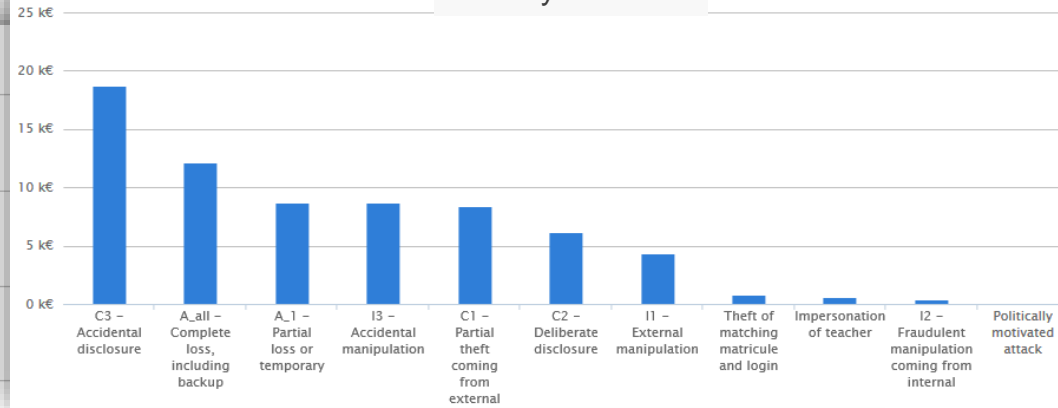
TRICK Service

Output: Key indicators

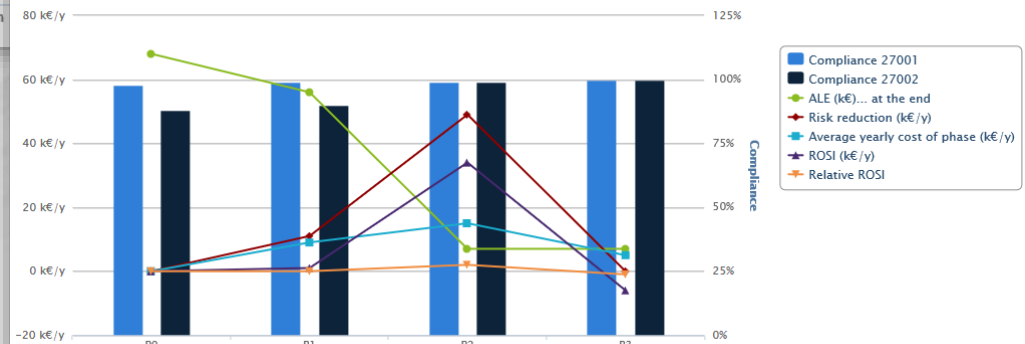
ALE by asset



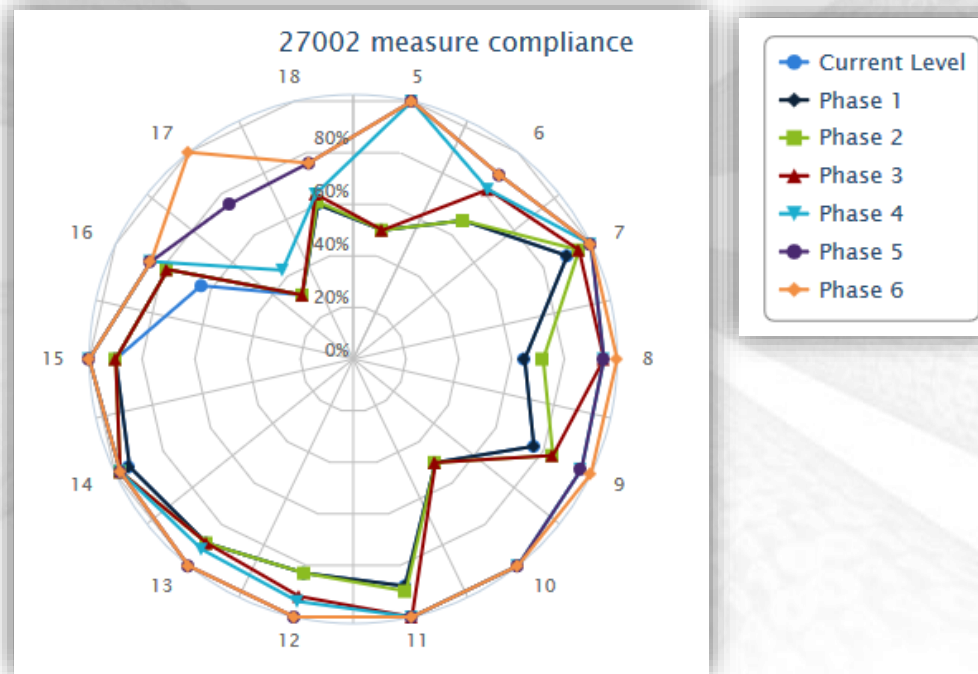
ALE by scenario



Evolution of profitability and ISO compliance for APPN



Compliance evolution towards best practices and international standards



CSSF compliant risk register

#	ID	Category	Risk title	Asset	Raw Eval.			Net Eval.			Exp Eval.			Response	Owner
					P.	I.	Imp.	P.	I.	Imp.	P.	I.	Imp.		
1	C1	Availability	A_1 - Partial loss or temporary	Staff	7	2	14	7	2	14	7	2	14	Transfer	User 1
2	C2	Integrity	I1 - External manipulation	malware.lu	6	2	12	6	2	12	6	2	12	Reduce	User 2

Automatically export 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

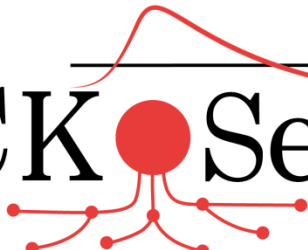
Annexes:

Statement of applicability

State of implementation of ISO 27002 security measures



TRICK Service

The logo for TRICK Service features the word "TRICK" in a large, black, serif font, followed by a red circle, and then the word "Service" in a smaller, black, serif font. A red line starts above the red circle, curves upwards and to the right, then downwards and to the left, ending above the "Service" part. Below the red circle, several red lines radiate outwards, each ending in a small red dot, resembling a network or a stylized tree structure.

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



Acknowledgments

itrust consulting has participated in several research projects funded by the Ministry of Economics or the European Commission, including BUGYO Beyond, CockpitCI and TREsPASS. These projects allowed us to build up our risk analysis tool that was first designed as Excel tool, then as web application.

TRICK Service obtained useful features since then: be it the calculation of profitability, the structuring of threats and risks, the costs of the security process (after ISO 27001) and security measures (of ISO 27002), the Luxembourgish requirements of dematerialisation and archiving, the thresholds and registers of CSSF, the evolution of security maturity, and many more.