Kost-nytte innen sikkerhet: Hva er prisen, hva er verdien, og hvordan prioritere blant tiltak?

Aida Omerovic

Seminar om kost-nytte analyse i en risikoevaluering

18. Feb. 2015

SINTEF

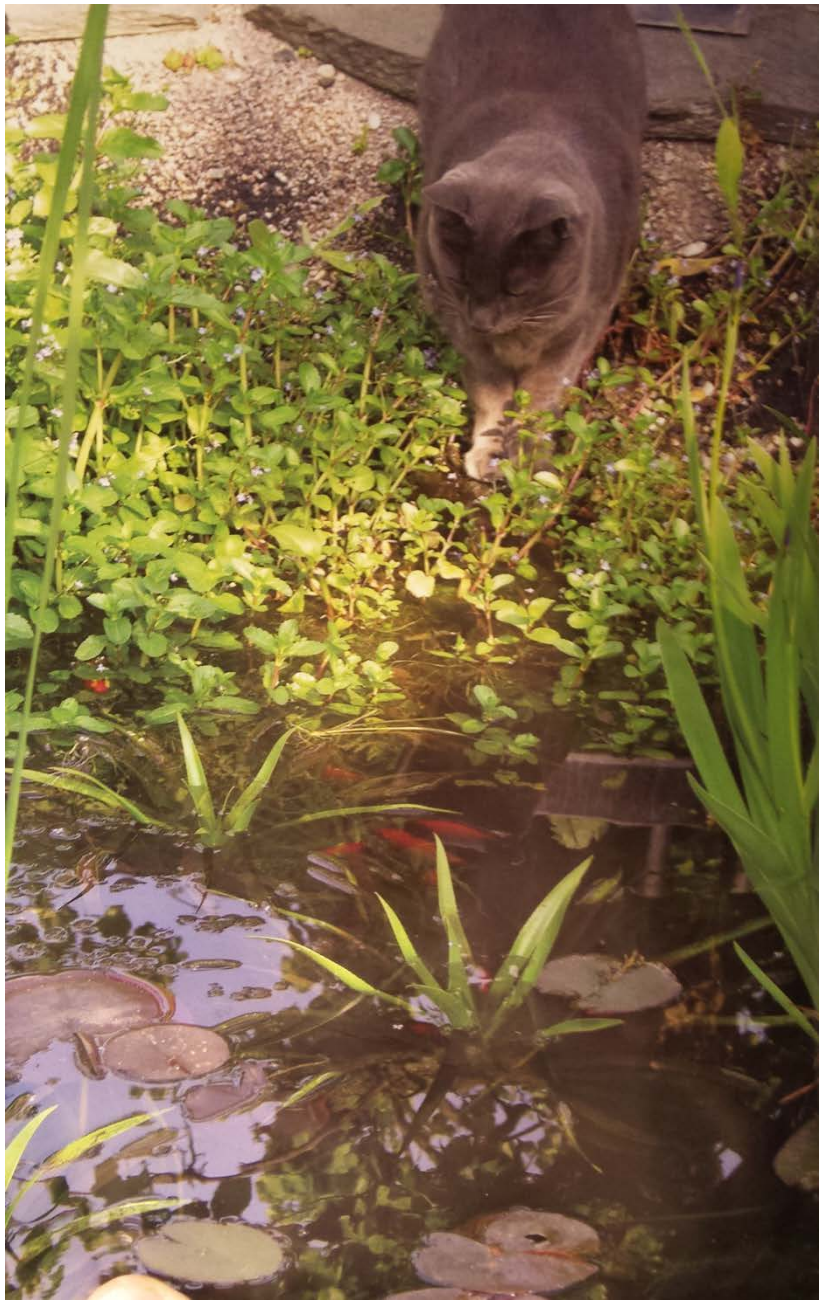
Innhold

- Hvorfor kost-nytte
- Hva er prisen?
- Hva er verdien?
- Hva er balansegangen?
- Hvordan velge blant tiltakene?


ProjectTi
HOME
ARTICLE
COMPUTERWORLD
Special Report
SOFTWARE THINKTANK
Helping You Make The Right Business Software Decisions.
[2014, SoftwareThinkTank]
Top 3 Reasons Business Owners Make Bad IT Decisions
When it comes to buying business management software, part of the battle is thinking about why business owners make bad decisions so you can avoid falling into the same traps.
Here are the Top 3 Reasons Business Owners Make Bad IT Decisions:
1. They fail to plan, they plan to fail.
Though this seems like a no-brainer, it's a crucial step that all too many business
accumulated by relatives of China's Prime Minister Wen Jiabao, the Times report said.
[2013, Constantin]
3,3

Kost-nytte innen sikkerhet er ikke bare penger inn og penger ut!

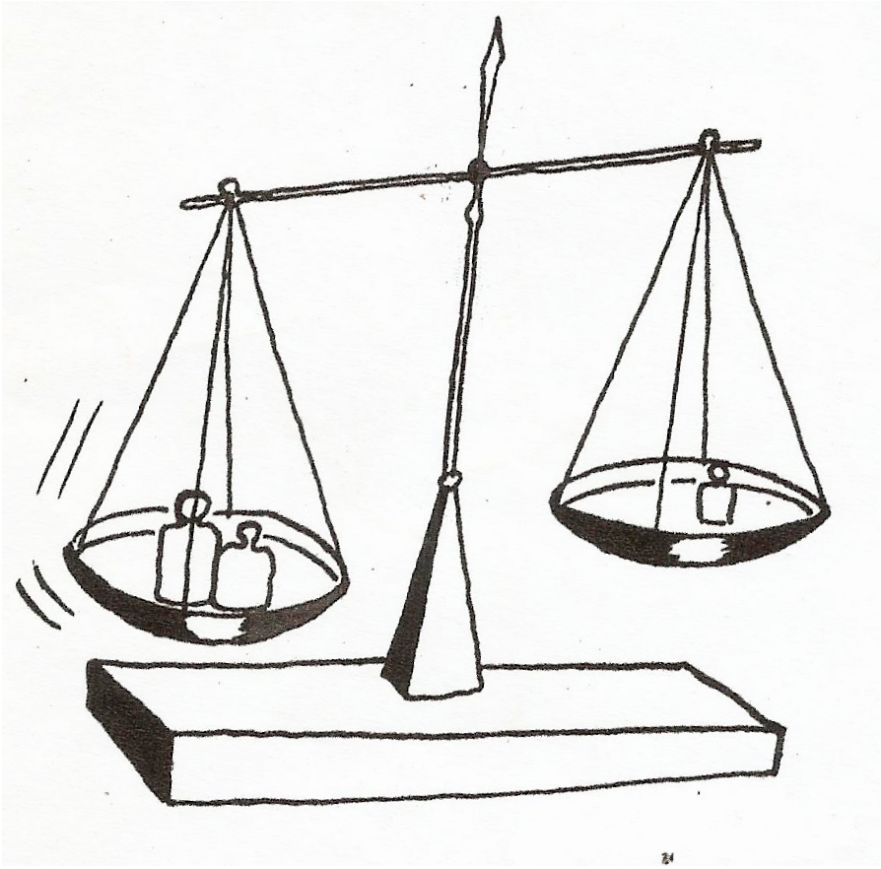
1. Sikkerhet oppnås gjennom en **kombinasjon** av tiltak som må settes sammen nøye. Det er ikke en komponent du kan sette inn eller ta ut.
2. Sikkerhet ivaretas overalt – i funksjonaliteten, i brukernes oppførsel, i arkitekturen, i policyen.
3. Sikkerhet balanseres med andre funksjonelle og ikke-funksjonelle hensyn, samt pris.
4. Sikkerhet er ikke binær – den oppnås i ulik grad og endres over tid.
5. Kost-nytte innen sikkerhet er ikke som en vanlig investeringsanalyse.



[2015, Pondteam]

Sikkerhet oppnås gjennom en **kombinasjon** av tiltak som må settes sammen nøye

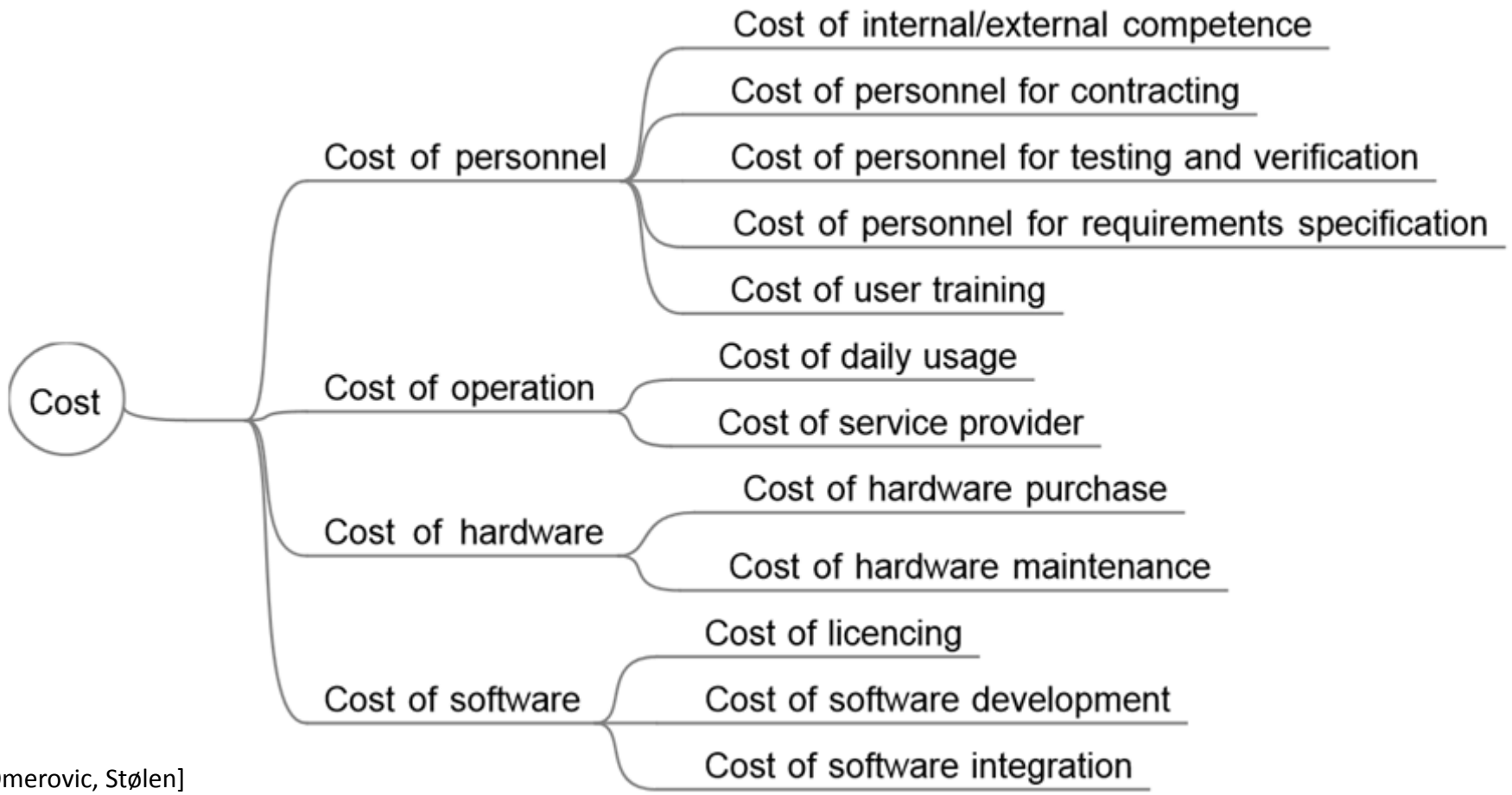
Sikkerhet balanseres med andre funksjonelle og ikke-funksjonelle hensyn



Sikkerhet oppnås i ulik grad og endres over tid

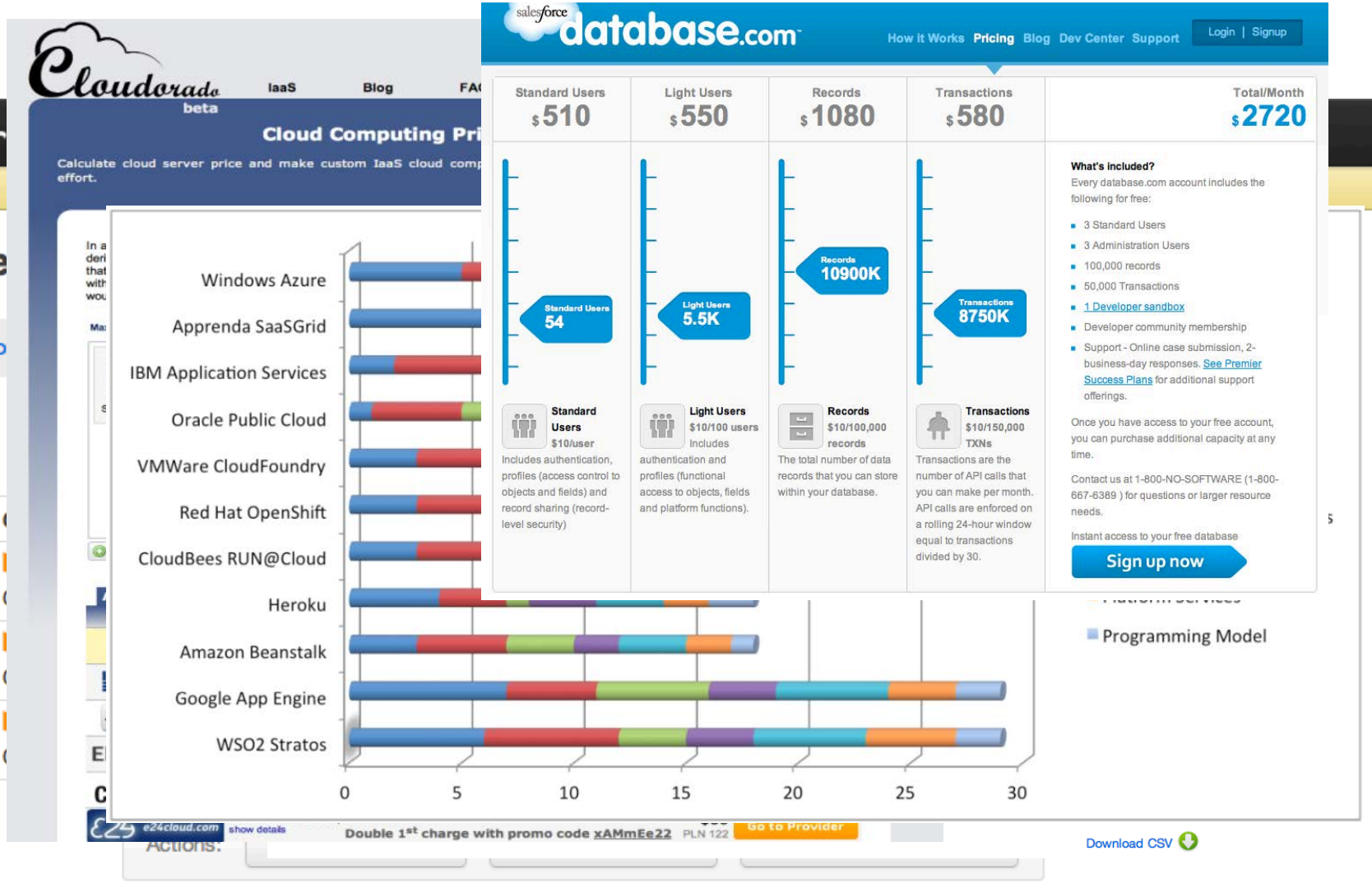
Kost-nytte for sikkerhet er ikke som en vanlig investeringsanalyse

Pris, prismodeller og usikkerhet



[2013, Omerovic, Stølen]

Pris, prismodeller og usikkerhet



Men du kan bruke modeller fra mikroøkonomi

- Net present value
- Annual loss expectancy
- Real option analysis
- Return on security investment

$$ROSI = \frac{(\text{Risk Exposure} \bullet \% \text{ Risk Mitigated}) - \text{Solution Cost}}{\text{Solution Cost}}$$

I kombinasjon med risikoanalyse og trade-off analyse

Underbygget av empiriske data og simuleringer

What if…

Analyse og prioritering blant tiltakene

SensApp Case

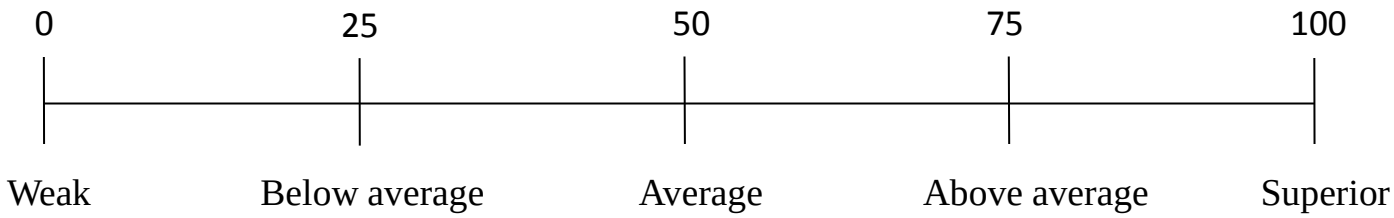
[2015, A. Singh et al.]
[2014, A. Singh et al.]

Systemet har en kostnad

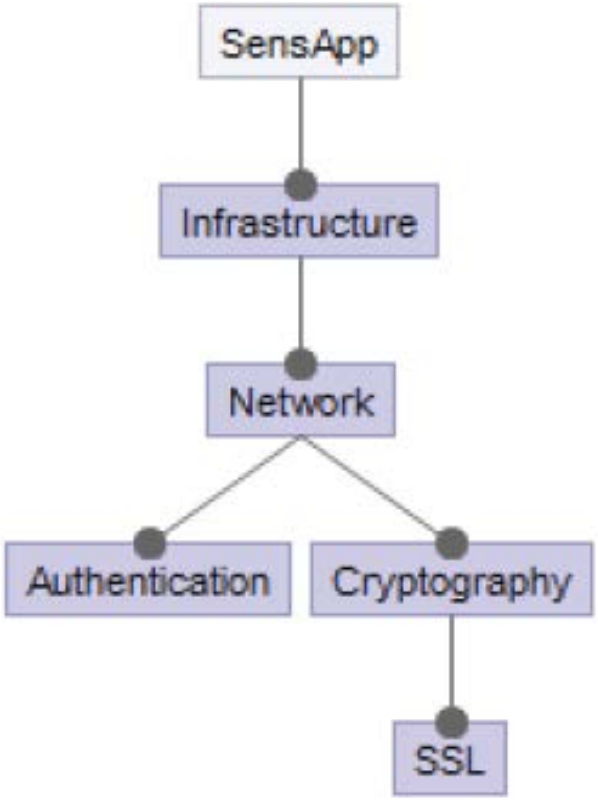
#	Cost type	Description	Acceptance value (NOK)	Present cost (NOK)
1	Migration	Costs related to service movement	< 30 000	10 000
2	Education	Costs related to personnel education	< 15 000	15 000
3	Licenses	Costs related to new or updated licenses	< 10 000	0
4	Infrastructure	Costs related to infrastructure	< 100 000	70 000
5	Support	Costs related to assistance and support	< 150 000	100 000
6	Software evolution	Costs related to software development and maintenance of SensApp	< 700 000	500 000
7	Other	Unforeseen costs	< 100 000	20 000
	Total =		< 1105 000	715 000

Og kvalitet

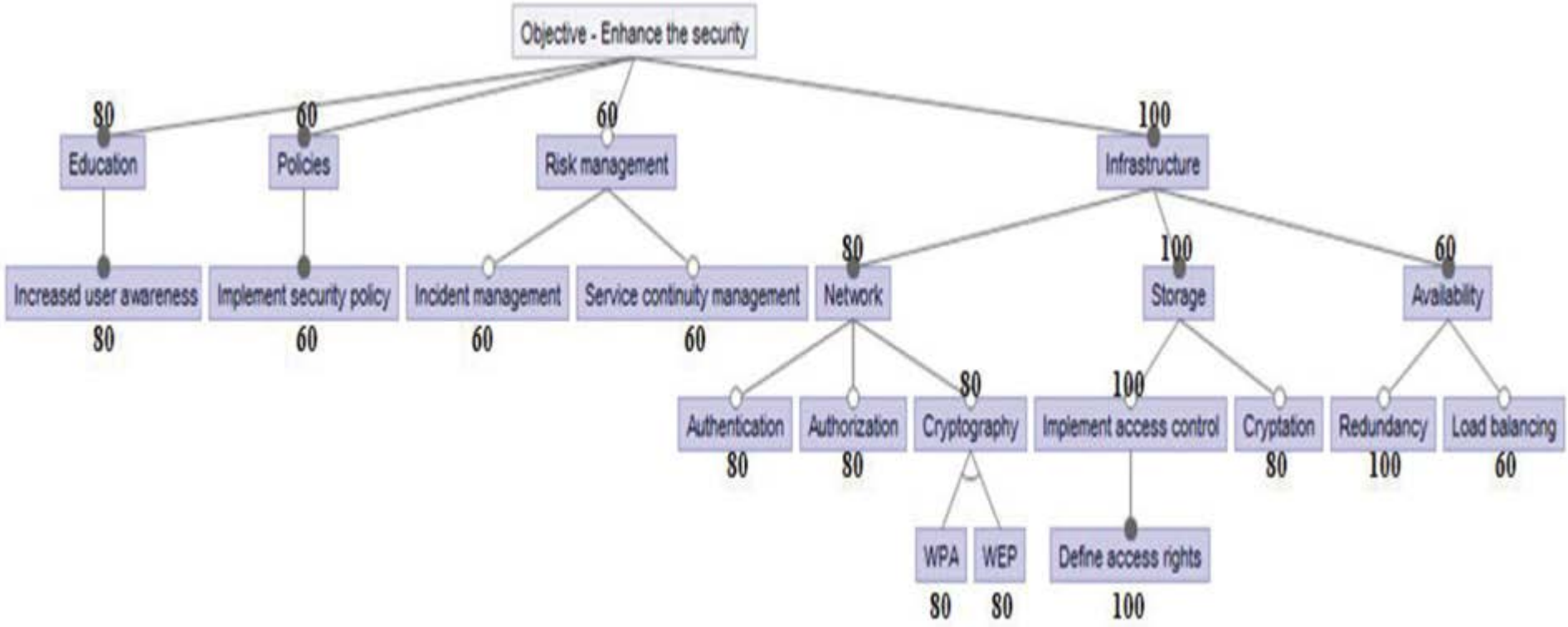
#	Quality characteristic	Description	Present value	Minimal acceptance value
1	Reliability	SensApp should constantly be able to perform its intended and required function on demand.	65	80
2	Response time	The elapsed time between the initiation of an action and the required response should be satisfactory.	75	60
3	Security	Users should be able to have secure access to personal data. Only authorized users should be able to access the data in question.	10	80
4	Accuracy of data	The accuracy of sensor data provided by SensApp should be close to the true value.	50	50/80

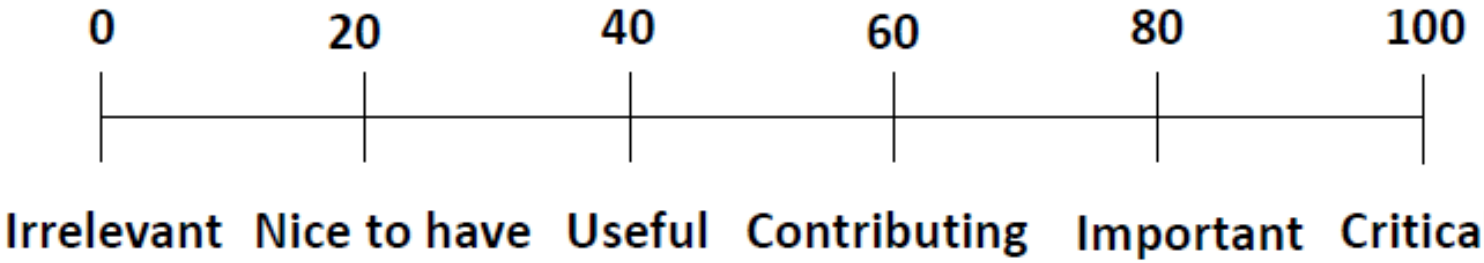


Og visse sikkerhetsfunksjoner



Men ideelt sett skulle sikkerheten…

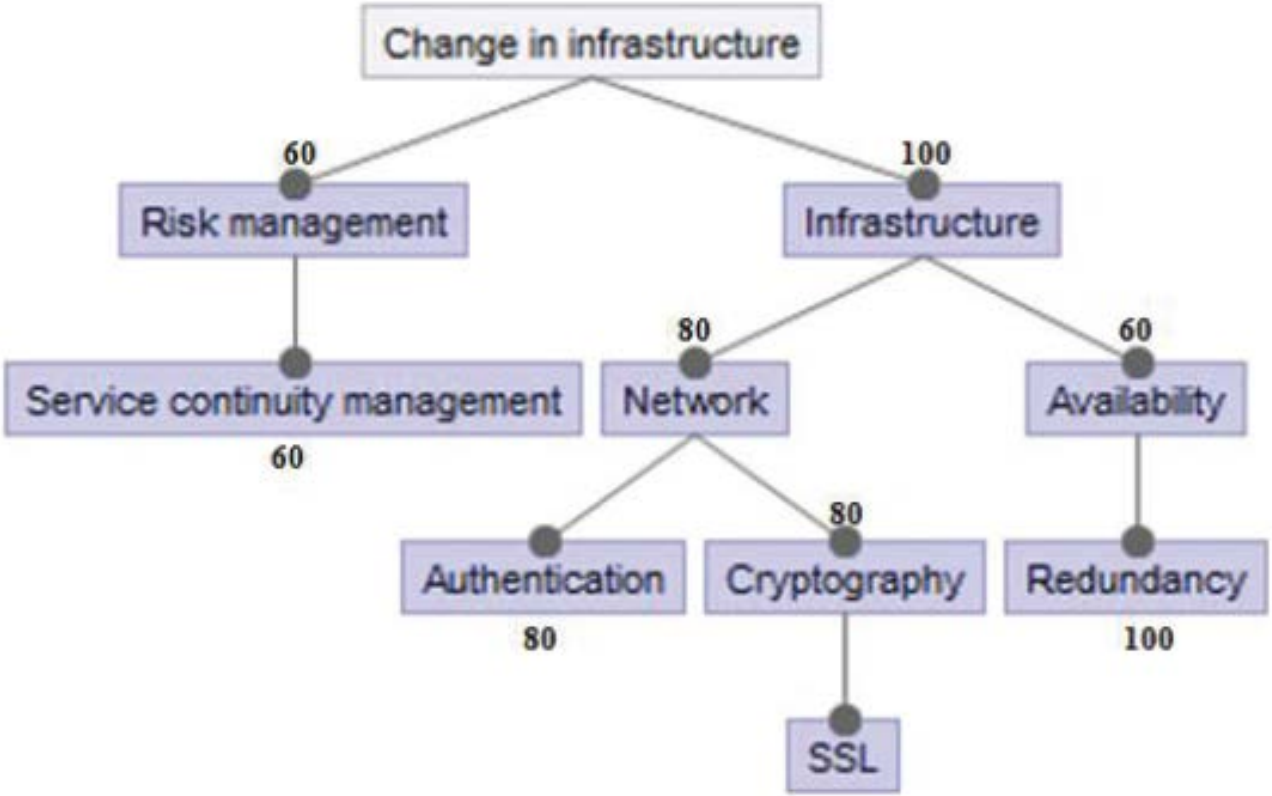




Mulige tiltak

#		Description
A	Change in infrastructure	Infrastructure is defined as the technical base or fundament needed for the functioning of the service provided by SensApp.
B	Change of topology	Topology is defined as the configuration of the technical base or fundament needed for the functioning of the service provided by SensApp.
C	Change of licenses	Upgrading or purchasing enterprise and commercial software licenses for information security purposes.
D	Change of location	Geographical relocation of the infrastructure, the platform, and the environment that SensApp is based upon.
E	Update software	Update the current software version of SensApp involves implementation of various security mechanisms in the already existing solution of SensApp.

Tiltak A: vektet og aggregert

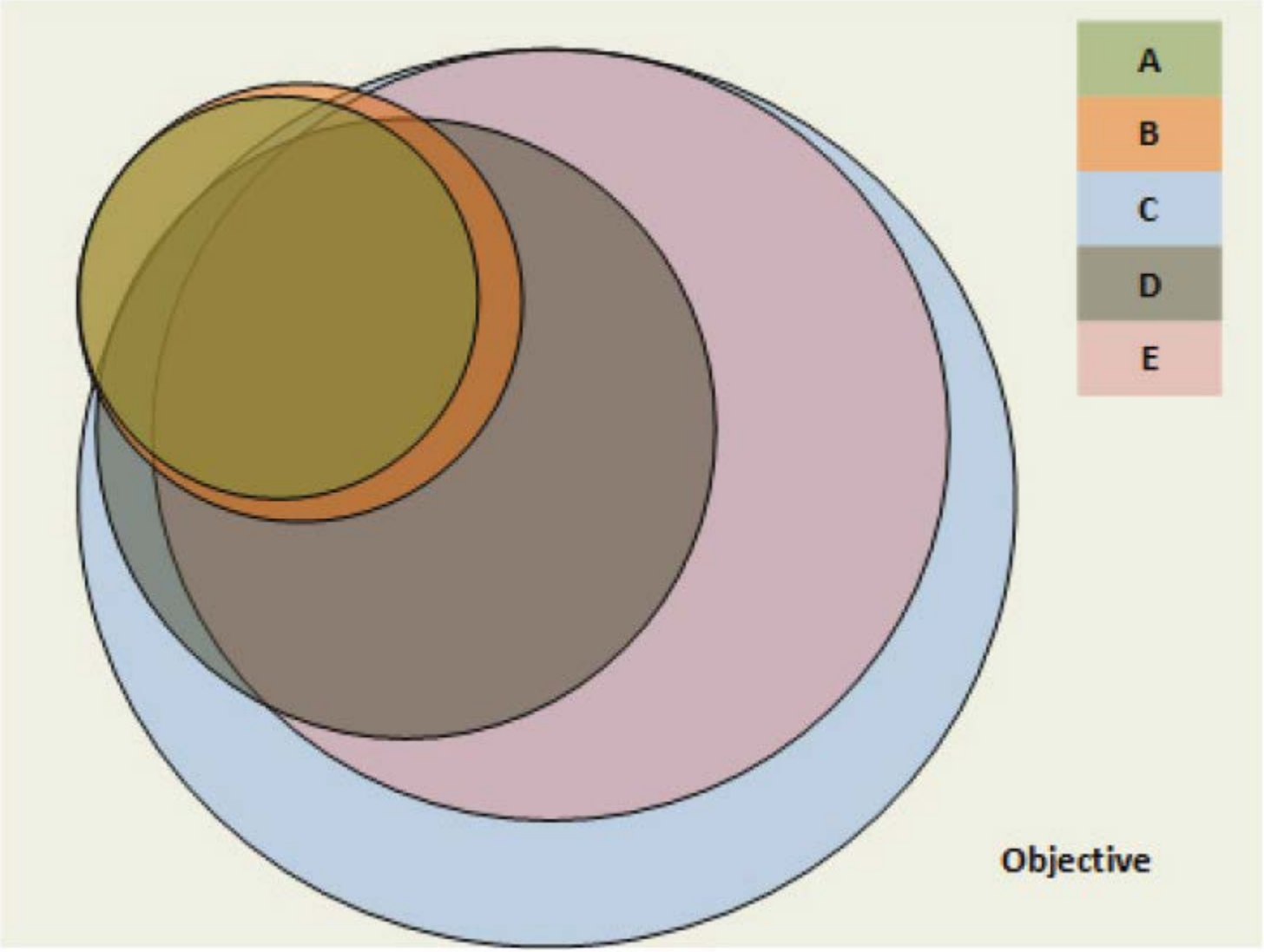


$$\frac{0}{300}+\frac{0}{300}+\frac{60}{300}\left(\frac{60}{120}\right)+\frac{100}{300}\left(\frac{80}{240}\left(\frac{80}{240}+\frac{0}{240}+\frac{80}{240}\left(\frac{80}{80}\right)\right)+\frac{0}{240}+\frac{60}{240}\left(\frac{100}{160}+\frac{0}{160}\right)\right)\approx 0.226$$

Grad av oppfyllelse og overlapp

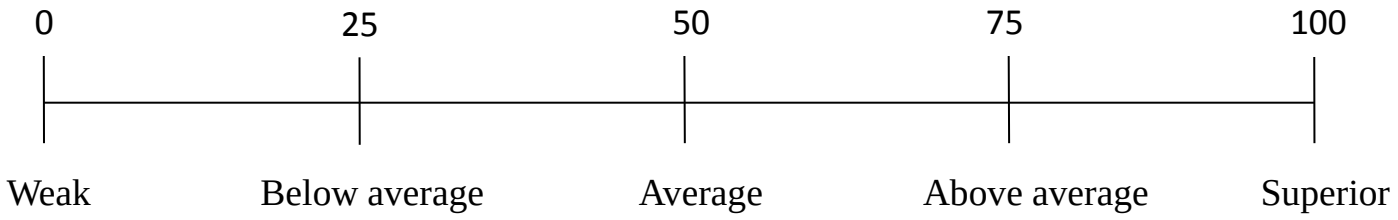
- Tiltak A: 0,226
- Tiltak B: 0,257
- Tiltak C: 0,917
- Tiltak D: 0,541
- Tiltak E: 0,717

	A	B	C	D	E
A		0.9	0.099	0.417	0.123
B	1		0.099	0.417	0.123
C	0.357	0.357		1	1
D	0.357	0.357	0.565		0.707
E	0.357	0.357	0.80	1	


A
B
C
D
E
Objective

Men så har de OGSÅ ulikt utslag på kvalitet

Decision alternative	**Reliability** (minimal: 80, present: 65)	**Response time** (60, 75)	**Security** (80, 10)	**Accuracy of data** (50/80, 50)
A	75	75	50	50
B	70	80	40	50
C	60	65	70	50
D	65	75	60	50
E	67	70	85	50
Weight [1...100]	***80***	***75***	***85***	***70***
Normalized weight	*0,3*	*0,2*	*0,3*	*0,2*



Og risiko (Tiltak A)

#	Risk	Likelihood	Consequence
1	Corruption of data during the replication process. Impact on security of data and storage.	Possible	Catastrophic
2	The data remains in the initial public cloud provider (not erased). Impact on security of the data.	Unlikely	Moderate
3	Someone may intercept data during the replication process due to low security (security breach). Impact on security of the data.	Possible	Major

		Consequence				
		Insignificant	*Minor*	*Moderate*	*Major*	*Catastrophic*
Likelihood	*Rare*					
	Unlikely			2		
	Possible				3	1
	Likely					
	Certain					

Og kostnad (Tiltak A)

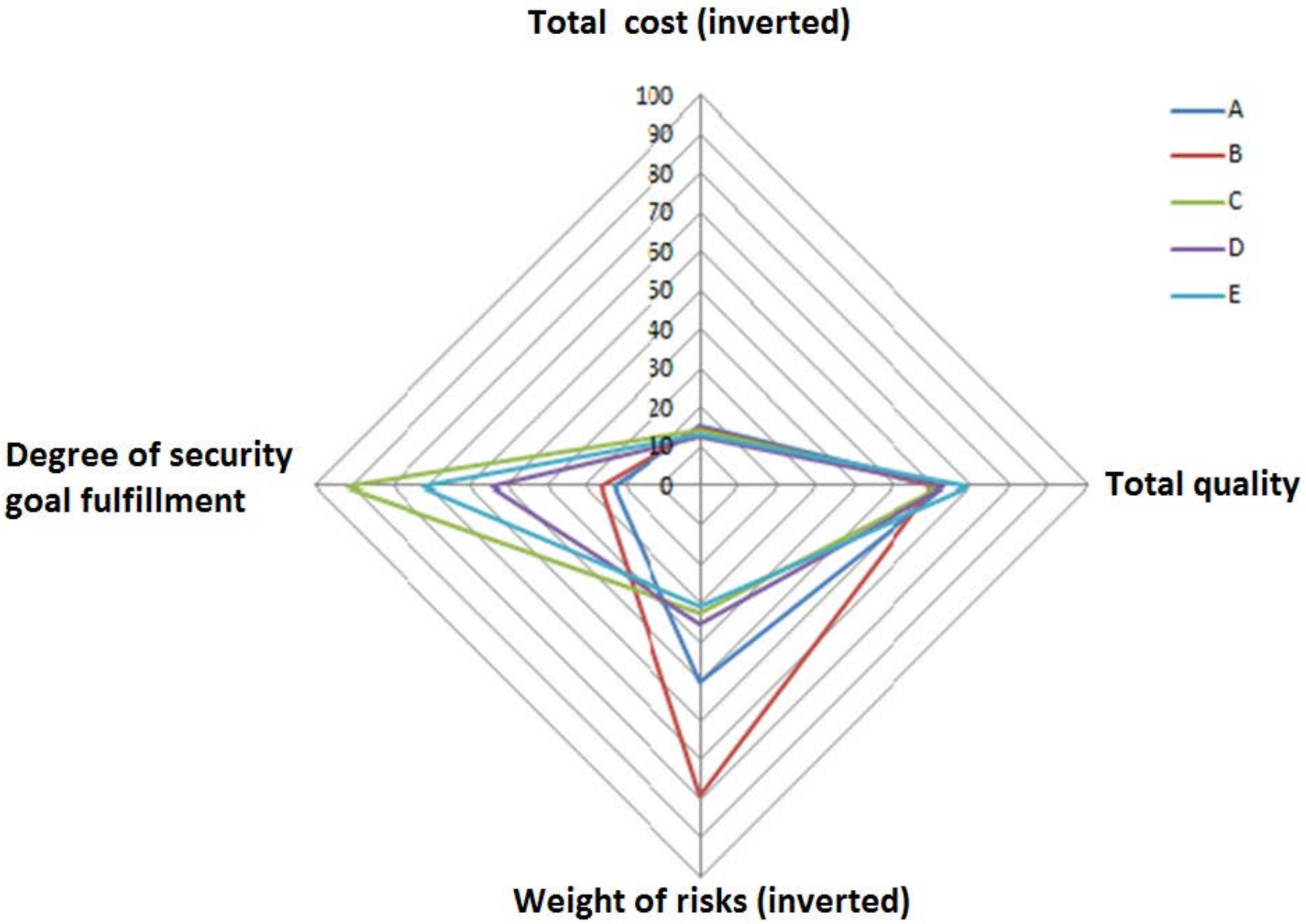
#	**Cost type**	**Description**	**Monetary value** (NOK)
1	Migration	Costs related to service movement	10 000
2	Education	Costs related to personnel education	15 000
3	Licenses	Costs related to new or updated licenses	0
4	Infrastructure	Costs related to infrastructure	75 000
5	Support	Costs related to assistance and support	100 000
6	Software evolution	Costs related to software development and maintenance of SensApp	500 000
7	Other	Unforeseen costs	20 000
	Total =		720 000

Samlet sett…

Decision alternative	Total cost	Total quality	Weight of risks	Degree of fulfillment
A	65,2	62,5	20,0	22,6
B	67,0	59,7	12,6	25,7
C	70,0	61,7	30,5	91,7
D	80,5	62,7	28,2	54,1
E	77,4	68,8	32,4	71,7

Decision alternative	Total cost’	Total quality	Weight of risks’	Degree of fulfillment
A	15,3	62,5	50,1	22,6
B	14,9	59,7	79,2	25,7
C	14,4	61,7	32,8	91,7
D	12,4	62,7	35,4	54,1
E	12,9	68,8	30,9	71,7

Samlet sett…


Total cost (inverted)
100
90
80
70
60
50
40
30
20
10
0
A
B
C
D
E
Degree of security goal fulfillment
Total quality
Weight of risks (inverted)

Oppsummering

Kost-nytte innen sikkerhet er ikke bare penger inn og penger ut!

1. Sikkerhet ivaretas overalt – i funksjonaliteten, i brukernes oppførsel, i arkitekturen, i policyen. Det er ikke en komponent du kan sette inn eller ta ut.
2. Sikkerhet oppnås gjennom en **kombinasjon** av tiltak som må settes sammen nøye.
3. Sikkerhet balanseres med andre funksjonelle og ikke-funksjonelle hensyn, samt pris.
4. Sikkerhet er ikke binær – den oppnås i ulik grad og endres over tid.
5. Kost-nytte innen sikkerhet er ikke som en vanlig investeringsanalyse

Vi har vist en praktisk beslutningsstøtte-metode for analyse og prioritering av tiltakene, der sikkerhet, kvalitet, kost, og risiko er hensyntatt.

- [2013, Pitagorsky] George Pitagorsky. Decision Making – A Critical Success Factor. Available: http://www.projecttimes.com/george-pitagorsky/decision-making-a-critical-success-factor.html. Accessed: May 12th 2014.
- [2012, 24/7 Wall St.] 24/7 Wall St. The Worst Business Decisions of All Time. Available: http://247wallst.com/special-report/2012/10/17/the-worst-business-decisions-of-all-time. Accessed: May 12th 2014.
- [2011, Ottervig] Vegard Ottervig. IT-prosjekt til flere milliarder i vasken. Available: http://www.hardware.no/artikler/it-prosjekt_til_flere_milliarder_i_vasken/102281. Accessed: May 12th 2014.
- [2013, Zachariassen] Espen Zachariassen. Nav stanser IT-prosjekt til 3,3 milliarder. Available: http://www.tu.no/it/2013/10/25/nav-stanser-it-prosjekt-til-33-milliarder. Accessed: May 12th 2014.
- [2013, Constantin] Lucian Constantin. New York Times computer network breached by Chinese hackers, paper says. Available: http://www.computerworld.com/s/article/9236400/New_York_Times_computer_network_breached_by_Chinese_hackers_paper_says. Accessed: May 20th 2014.
- [2014, SoftwareThinkTank] SoftwareThinkTank. Top 3 Reasons Business Owners Make Bad IT Decisions. Available: http://www.softwarethinktank.com/articles/top-3-reasons-business-owners-make-bad-it-decisions. Accessed: May 12th 2014.
- [2015, Pondteam] Pondteam "Trädgårdsdammar" 2015
- [2015, A. Singh et al.] Avjot Garcha Singh, Aida Omerovic, Franck Chauvel and Nicolas Ferry "Towards Feature-driven Goal Fulfillment Analysis – A Feasibility Study" In Proc. of the Third Int. Conference on Model-Driven Engineering and Software Development, (MODELSWARD'15) Angers France
- [2014, A. Singh et al.] Avjot Garcha Singh, Aida Omerovic, Franck Chauvel and Nicolas Ferry "Analyzing Impacts of Adaptations on Cost, Risk, and Quality – An Experience Report" In Proc. of 13th Workshop on Adaptive and Reflective Middleware (ARM2014), Bordeaux, France.
- [2013, Omerovic, Stølen] Aida Omerovic, Ketil Stølen Paper "Characterizing and Fulfilling Traceability Needs in the PREDIQT Method for Model-based Prediction of System Quality" Published in International Journal on Advances in Systems and Measurements, Volume 6 n 1&2 2013