

Oppfølging og rapportering av etterlevelse av styrefastsatt risikoappetitt

- Representant fra andrelinjen

Stian Sviggum
24. november 2017



Andrelinjen...

- Er i mellom «barken og veden»
 - Er både kontrollør og hjelper
 - Eier «ingenting» men skal ha en mening om «alt»
- Består av flere funksjoner
 - Hver funksjon er ansvarlig for oppfølging og rapportering av styrets risikoappetitt innenfor hver sin silo
 - Skal rapporteringen være samlet, segregert men koordinert eller fullstendig segregert?
- Er ofte den som utarbeider forslag til risikoappetitt for ledelsen og styret...

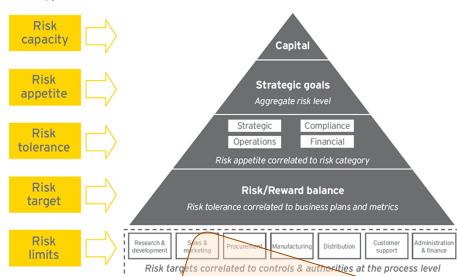


Risikoappetitt og terminologi

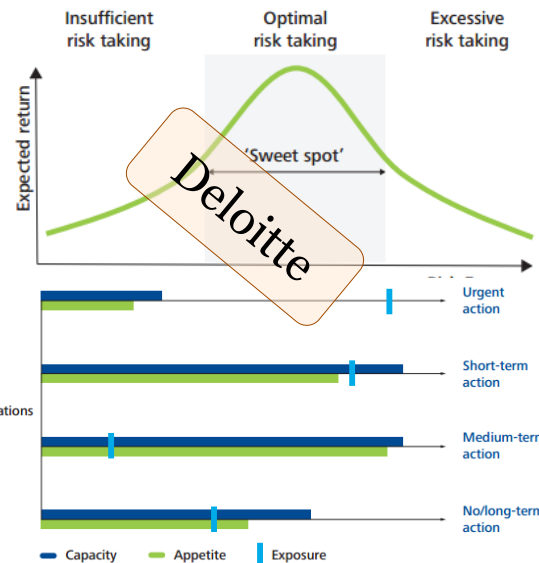
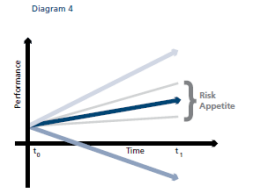
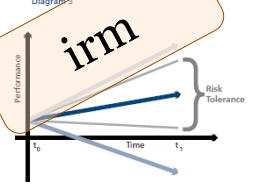
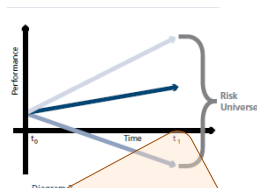
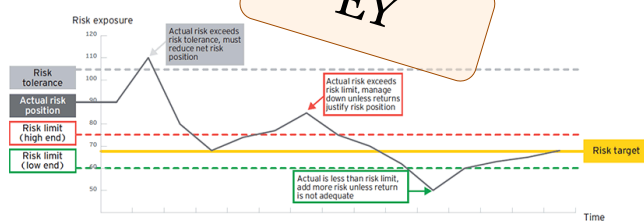
– et minefelt av begreper og definisjoner



The risk pyramid



Risk appetite/tolerance/target example



Existing Risk Profile	The current level and distribution of risks across the entity and across various categories	Determination of Risk Appetite
Risk Capacity	The amount of risk that the entity is able to support in pursuit of its objectives	
Risk Tolerance	The level of risk that the entity is willing to accept in pursuit of its objectives	
Attitudes Towards Risk	The attitudes towards growth, risk, and return	



Risk appetite
The amount of risk an organization is willing to accept in pursuit of strategic objectives.

Risk capacity
The actual amount of risk the company could bear based on its financial and operational capabilities.

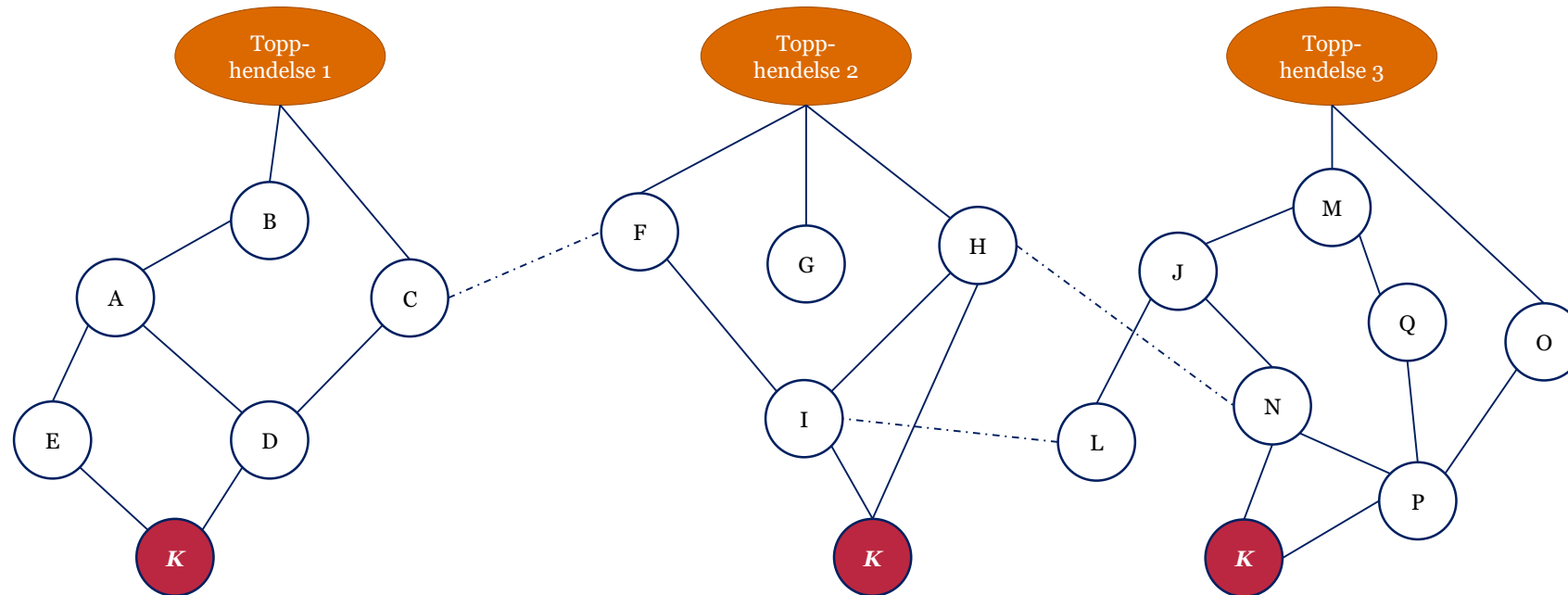
Risk tolerance
The acceptable levels of variability to achieving strategic objectives.

COSO ERM (2004)

Deloitte

PwC

Hva har kultur med risikoappetitt å gjøre?

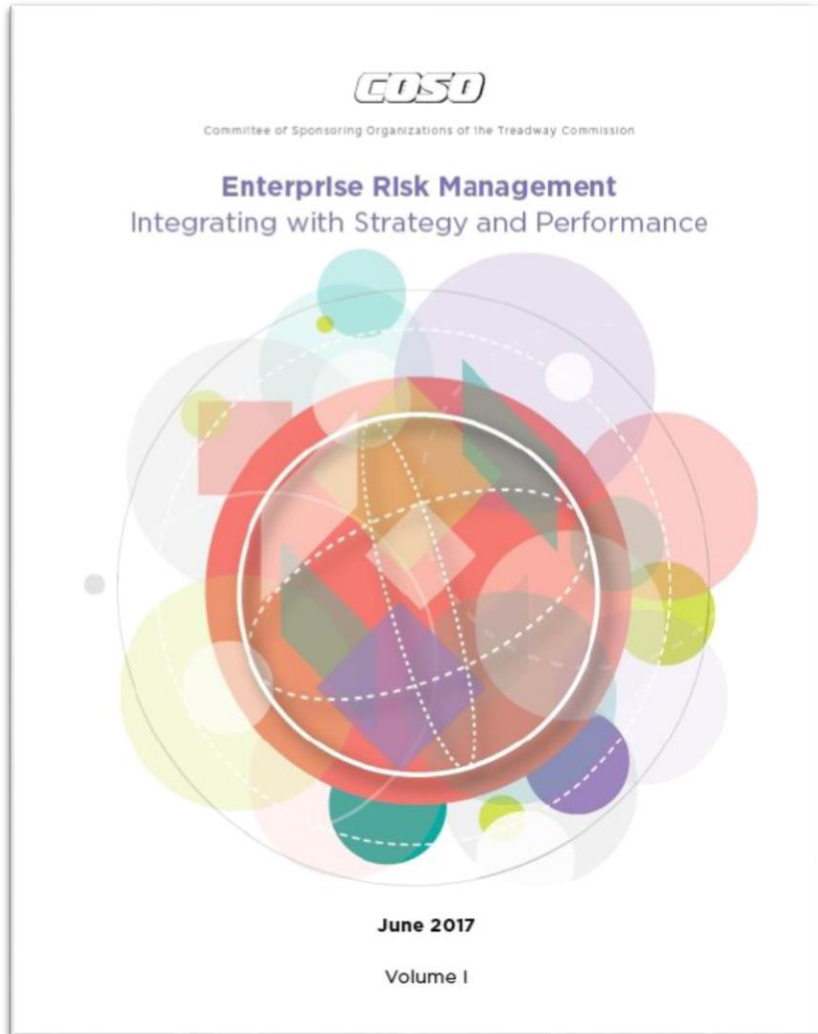


Kulturen (holdninger og atferd) er den faktoren man helt sikkert vet påvirker alle risikoscenarioer.

Positive kulturendringer er antagelig de tiltakene som har størst risikoreduserende effekt. Risikoappetitt er et verktøy for styret å sette rammer for akseptabel atferd.

COSO Enterprise Risk Management

- Helhetlig risikostyring er blitt mer helhetlig



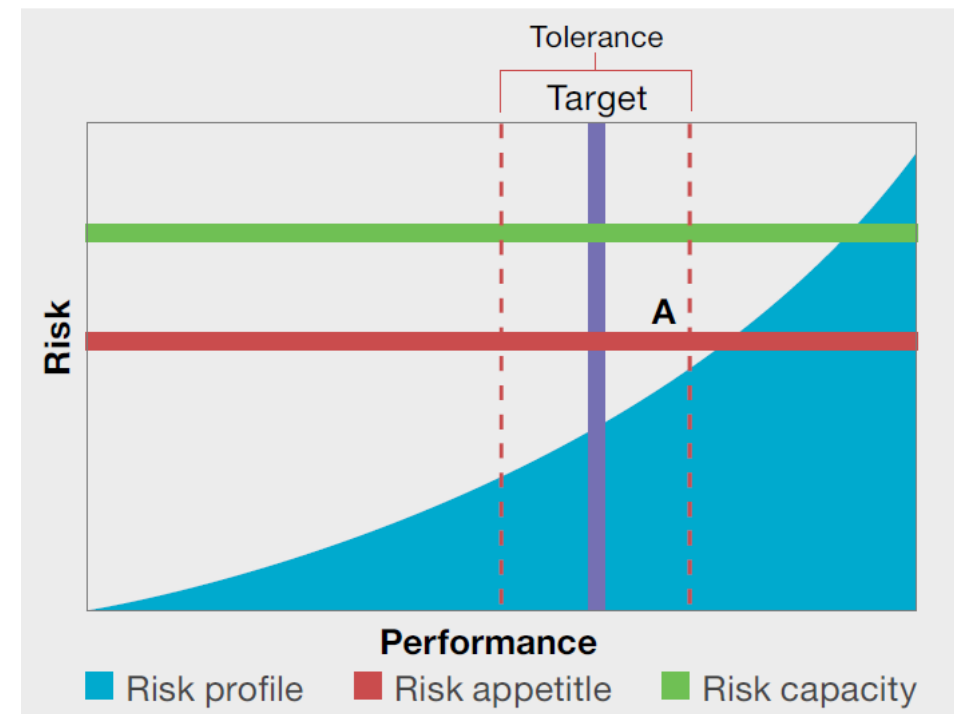
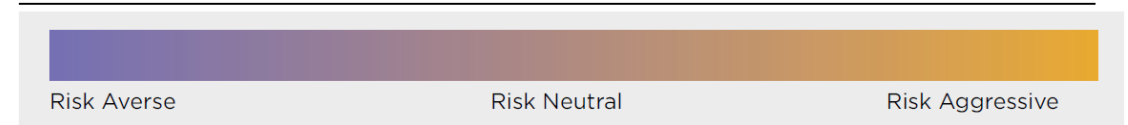
COSO ERM (2017) og risikoappetitt

- Kulturen reflekterer en virksomhets verdier, atferd og beslutninger
- Kulturen i en virksomhet påvirker
 - Hvordan den **identifiserer** risiko
 - Hvilken type risiko den **aksepterer**
 - Hvordan den **styrer** risiko

Some entities consider risk appetite in qualitative terms while others prefer to use quantitative terms, often focusing on balancing growth, return, and risk. Whatever the approach for describing risk appetite, it should reflect the entity's culture. Moreover, if the organization wants to change some aspect of the culture, defining a strong risk appetite can help create and reinforce that desired culture.

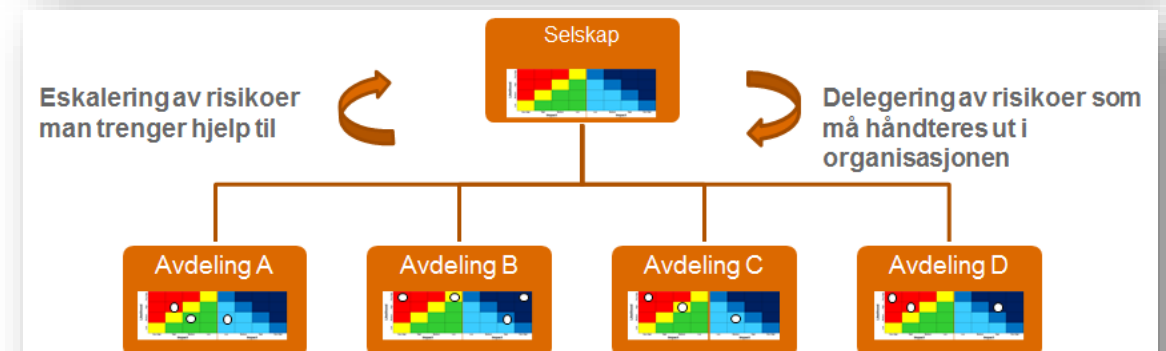
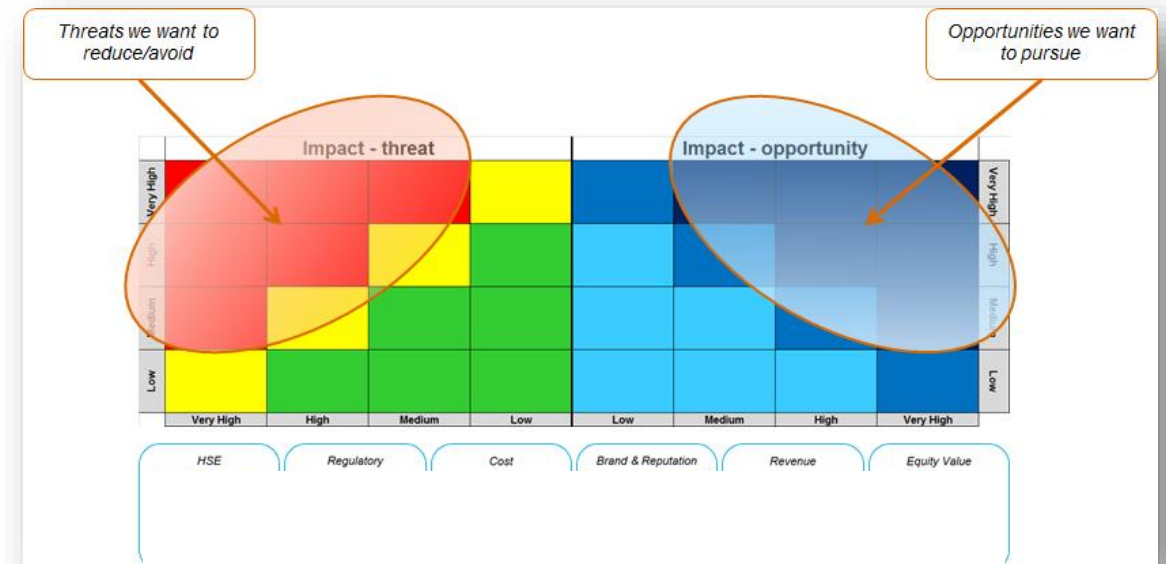
The best approach for an entity is one that aligns with the analysis used to assess risk in general, whether that is qualitative or quantitative. Developing the risk appetite statements is an exercise in seeking the optimal balance between risk and opportunity.

Figure 6.1: Culture Spectrum



Risikoappetitt som et verktøy for å fremme god risikokultur

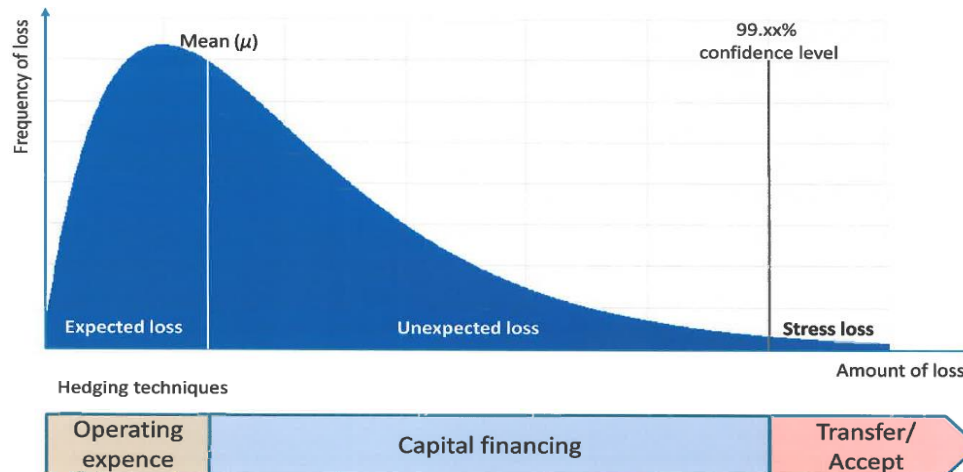
- Risikomatriser og tilhørende behandlingsregler (appetitt/toleranse)
 - Setter krav til eskalering av kritiske risikoer
 - Definerer hvem som har myndighet til å akseptere risikoer
 - Opp- og nedside, eller??
- Risikostyringsprosesser på flere nivå i en virksomhet
 - Mulighet for mellomledere å definere sitt eget risikobilde - transparens
 - Kunne eskalere risiko (overføre ansvaret) oppover i organisasjonen, og delegere (overføre ansvaret) av risiko nedover
 - Kan få til en dynamikk der det er «positivt» å si ifra om «røde» risikoer...



Finanstilsynets og Basel

- Finanstilsynets tematisyn om operasjonell risiko:
 - Påpeker at holdninger fra styret og toppledelsen er avgjørende for risikostyringen (“**tonen fra toppen**”), og at en forutsetning for en sterk kultur er at **mellomledelsen viderefører** og tydeliggjør holdningene fra toppledelsen.
 - Bankene bør tydeliggjøre **ambisjonsnivå** og **risikotoleranse** i sine styrende dokumenter, og dette bør inkludere **kvantifiserte måltall/rammer** og ulike risikoindikatorer.

- Basel:

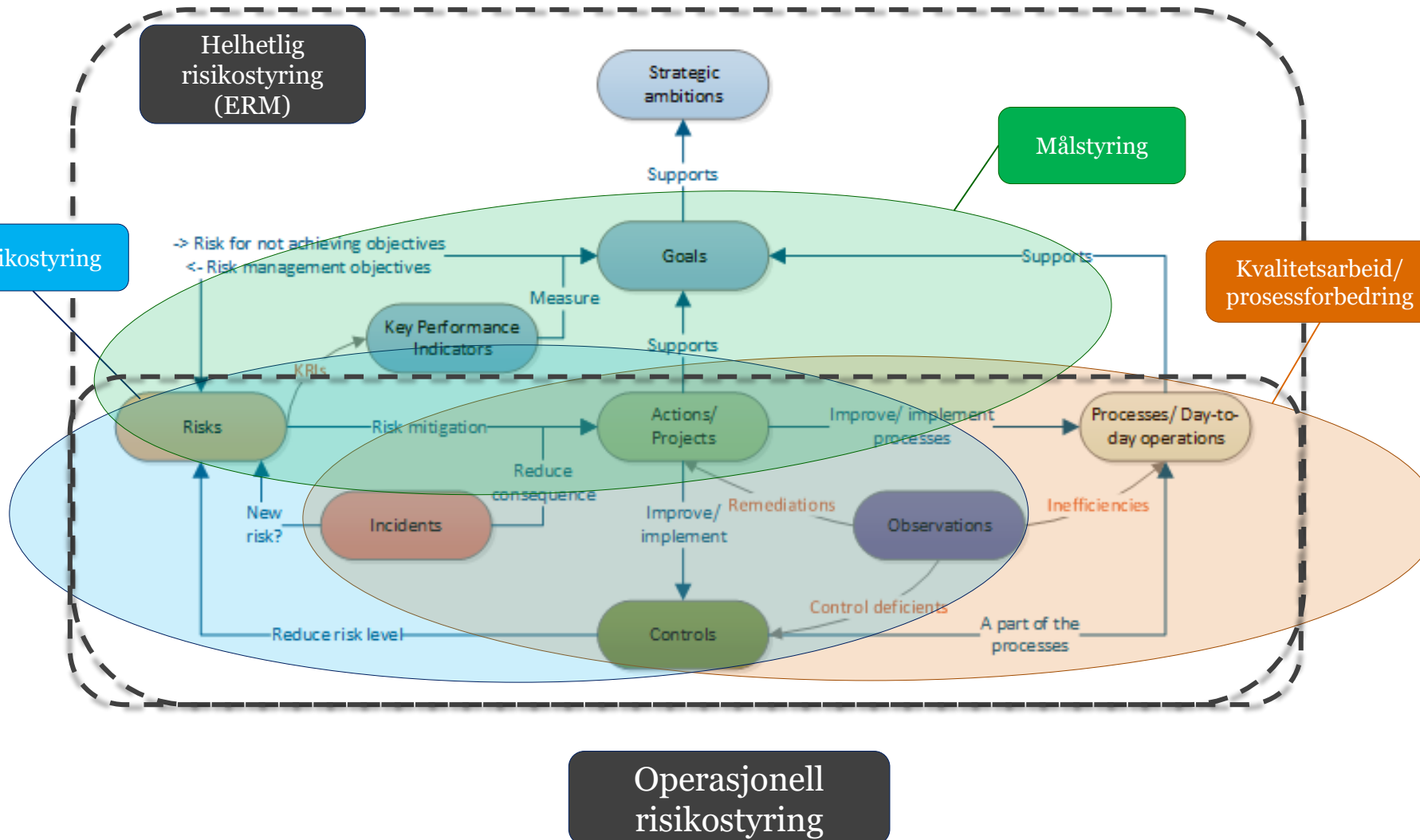


Tematisyn
Operasjonell risiko
– hendelser

Rapport

	DATE: 11.07.2017

Risikostyring – oppfølging og styring av risikoappetitt

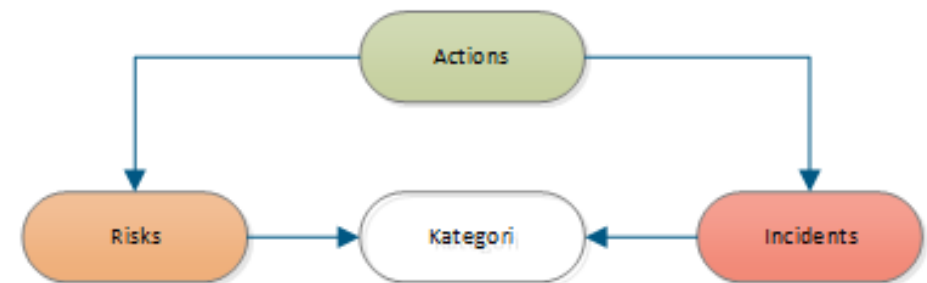
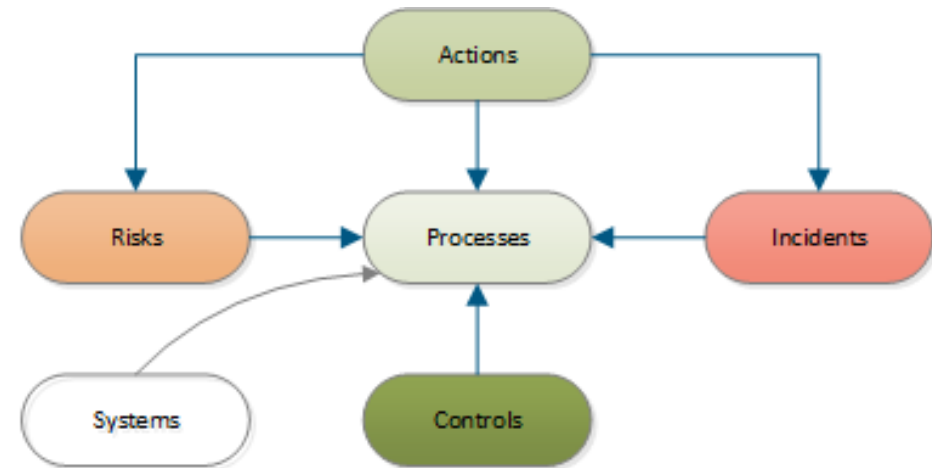


*Study the art of science;
study the science of art.
Learn how to see.
Realize that everything
connects to everything else.*

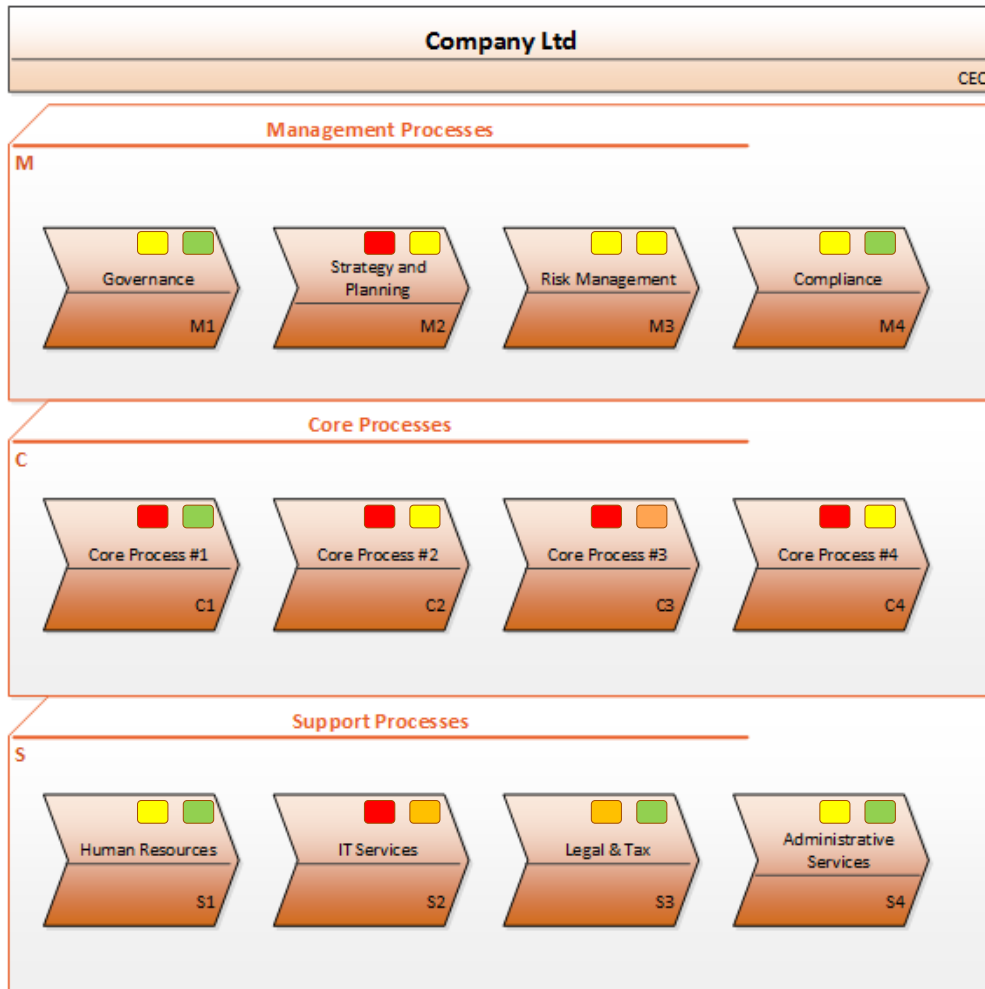
- Leonardo da Vinci

Hvordan knytte de forskjellige elementene sammen i praksis?

- Bruke prosesser som «nav»
 - Kontroller er ofte egne prosessteg
 - Uønskede hendelser skjer oftest i utførelsen av arbeidsaktiviteter i en prosess eller i systemer som brukes i prosessen
 - Muliggjør risikovurdering av selve prosessen, og rapportering per prosess
- Bruke samme kategorisering av uønskede hendelser og risikoer
 - Kan se risikoer og hendelser i sammenheng innenfor hver delkategori
 - Muliggjør aggregering av risiko innenfor delkategorier
 - Muliggjør rapportering per kategori



Eksempel – prosessbasert risikorapportering og risikoregister



Controls			Future (Residual)			Inherent (Gross) Risk		Lines of defence - Controls		Current (Net) Risk		Future (Residual) Risk			
Hide	Hide	Hide	Threat	Opportunity	Threat	Opportunity	Threat	Opportunity	Threat	Opportunity	Threat	Opportunity	Threat	Opportunity	
Unhide	Unhide	Unhide	Level	Level	Level	Level	Level	Level	Level	Level	Level	Level	Level	Level	
Risk ID	Risk name	Risk description	Risk Owner	Organization	Main Risk Category	Risk Sub-Category	Threat, opportunity or both	Level	Level	Level	Level	Level	Level	Level	
R-1	Riska		PwC Norway	Strategic	Market Dynamics	Both	Significant	Yes	4 (0)	Low	Significant	Yes	2	Moderate	Significant
								Yes	0 (0)			Yes	0		
								Yes	0 (0)			Yes	0		

Use this form to complete an Action Plan for each item in the Risk Assessment Template with a "Yes" in Column AG

Action ID	Risk Reference #	Action Name	Action Description	Action Owner	Organization	Target date for Completion	Action Status	Completion Date
A-1	R-1	Action 1				03/04/2017	Proposed	
A-2	R-1	Action 2				04/04/2017	In progress	
A-3	R-1	Action 3				23/04/2017	In progress	
A-4	R-2	Action 4					In progress	
A-5	R-2	Action 5					In progress	
A-6	R-3	Action 6					In progress	

Control ID	Risk Reference #	Control Name	Control Description	Related Network Standard	Control Owner	Organization	Date for next testing	Comments test/monitoring	Control Status/Assessment	Assessment Date
C-1	R-1	Control a							Active - OK	
C-2	R-1	Control a							Active - OK	
C-3	R-1	Control a							Active - OK	
C-4	R-2	Control a							Active - OK	
C-5	R-1	Blank							Active - Not working	

Hendelsesregister

ID	Navn	Beskrivelse	Dato da hendelsen skjedde	Registrerings-dato	Rapportert av	Hendelseskategori	Involverte leverandører	@konomisk konsekvens (NOK)	Omdømmetap	Vesentlighet/ Alvorlighetsgrad

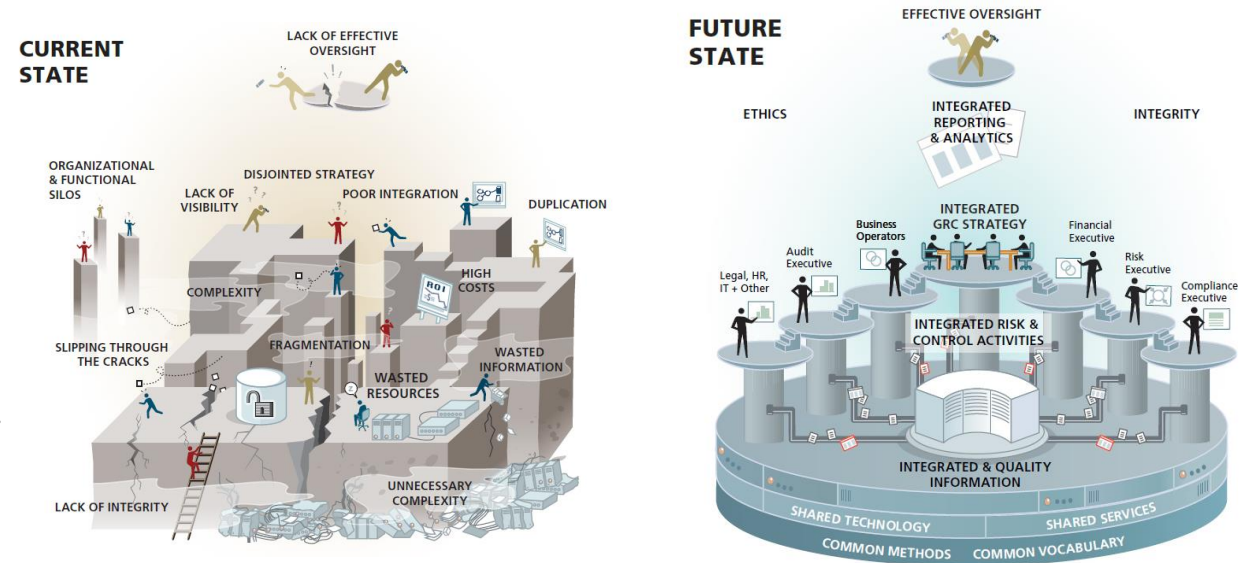
Verktøystøtte?

- GRC plattformer

The Open Ethics and Compliance Group (OECG®) definerer GRC på følgende måte:

Governance, Risk and Compliance (GRC) is the integrated collection of capabilities that

- *enable an organization to reliably achieve objectives (governance)*
- *while addressing uncertainty (risk)*
- *and acting with integrity (compliance)*



Kontaktinformasjon

Stian Sviggum



Direktør

TLF: 952 60 215

stian.sviggum@pwc.com