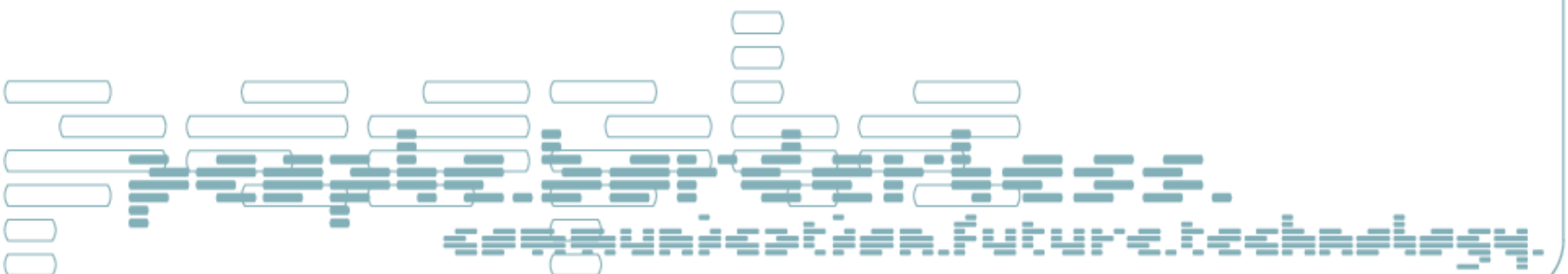
Telerisk
En metode som virker i praksis

Erik Wilmar

Business Consulting, Telenor

Det er sannsynlig at noe usannsynlig vil skje.

Aristoteles, 384-322 f.Kr.



Ingen verdier?

Ingen trusler?

Du trenger ikke sikkerhet!

Verdien av en risikoanalyse

- Risikoanalyser brukes bl a for å finne trusler og verdier for å si noe (meningsfylt) om behovet for sikkerhet
- En vellykket risikoanalyse
  1. Gir ny innsikt i og forståelse for analyseobjektet
  2. Gjør at man selv kan gjøre en risikoanalyse en annen gang
  3. Påvirker en reell beslutningssituasjon
- Risikoanalyser kan være unødvendige
- Risikoanalyser kan være for grundige
- Å ikke gjennomføre en risikoanalyse kan bli ubehagelig!

Begreper – informasjonssikkerhet

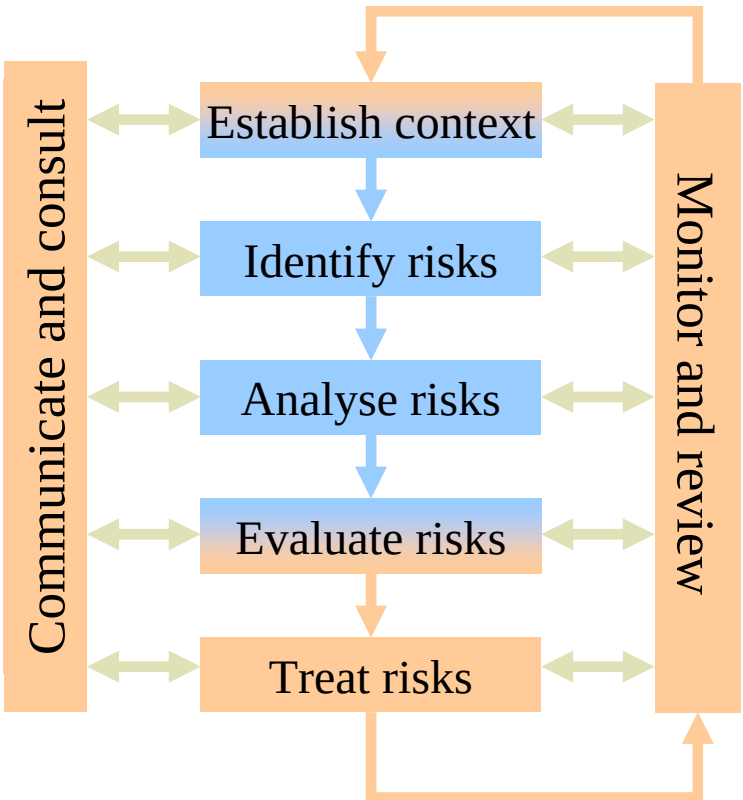
- Telenors definisjon:
  - Tiltak for at informasjon har den nødvendige beskyttelse for å oppnå konfidensialitet, integritet og tilgjengelighet ut fra informasjonens verdi.
  - Fagområde som omfatter sikker informasjonshåndtering, personellsikkerhet, IT-sikkerhet inkl kryptografi, og systemsikkerhet.
- Dette betyr
  - Sikkerhetsbrudd er negativt → skal unngås
  - Ikke sikkerhet for enhver pris → risikobasert og lønnsomt
  - Fysisk sikkerhet inkluderes → helhetlig tilnærming

Begreper – risiko

- Risiko = f(hendelse, konsekvens, sannsynlighet, alfa)
- Risiko oppleves forskjellig
  - Et problem er ikke en risiko
  - Risiko skal ikke fjernes for en hver pris
  - Ståsted avgjør om risiko er negativt eller positivt
  - Opplevd risiko = frekvens * konsekvens * alfa
- Sikkerhetsrisiko er ”nedside”
- Sikkerhetsrisiko kan ikke diversifiseres bort

Begreper – styring og analyse av risiko

Figur tilpasset fra AS/NZS 4360



Risikostyring

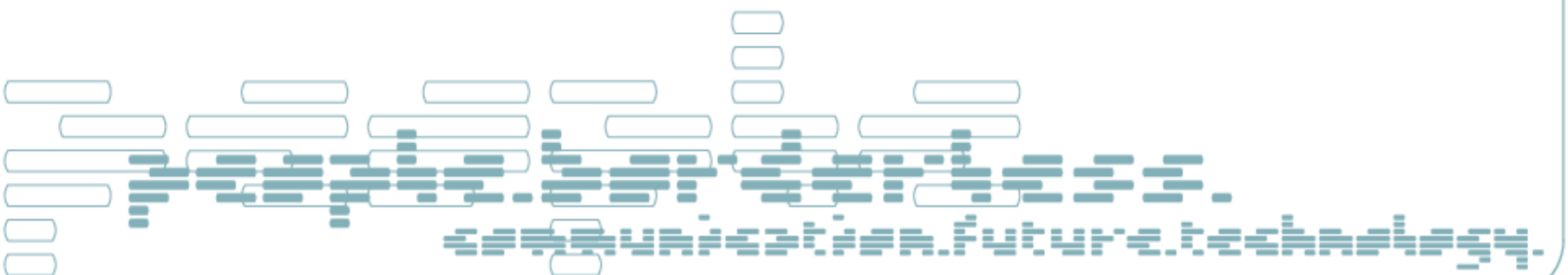
- Kontinuerlig forretningsprosess
- Hensikten er å bestemme hvilke risikoer man aksepterer, basert på forretningsmessige kriterier

Risikoanalyse

- Risikoanalyse (blå farge) er en del av risikostyringsprosessen
- Hensikten er å avdekke risikoer og de relevante opplysninger i forbindelse med disse

Beste praksis og standarder

telenor



Eksempler på kjente standarder

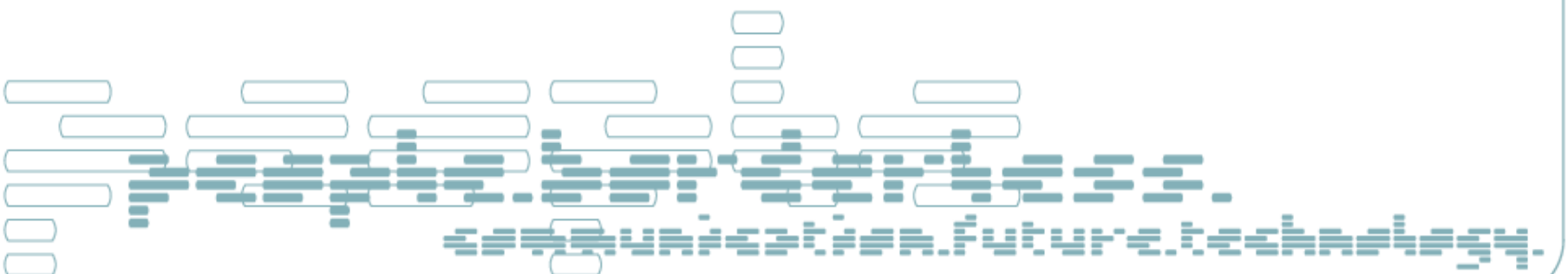
- Norske ”de jure” standarder
  - Personopplysningsloven
  - Sikkerhetsloven
- Internasjonale ”de facto” standarder
  - Windows 9x, C++, RS232, Ethernet …
- Formelle standarder
  - ISO 17799:2000 – Code of practice for information security management
  - JIS Q 2001:2001 – Retningslinjer og anbefalinger om risikostyringssystemer
  - NS 5814 – Krav til risikoanalyser
- Bedriftsinterne standarder
  - Obligatoriske krav
  - Anbefalte retningslinjer

Eksempler på sikkerhetsfaglige (krav) standarder i Telenor

- Alle systemer og produkter i Telenor skal klassifiseres med tanke på sikkerhet
- Sikkerhet skal støtte forretningen og skal være lønnsomt
- Systemeier skal ha en aktiv og gjennomtenkt risikostyring
- Risikostyringen skal baseres på risikoanalyser
- Men Telenor stiller inntil videre IKKE krav om bruk av én bestemt metode for risikoanalyse eller risikostyring

Et eksempel på en konsernfelles standard for risikoanalyse

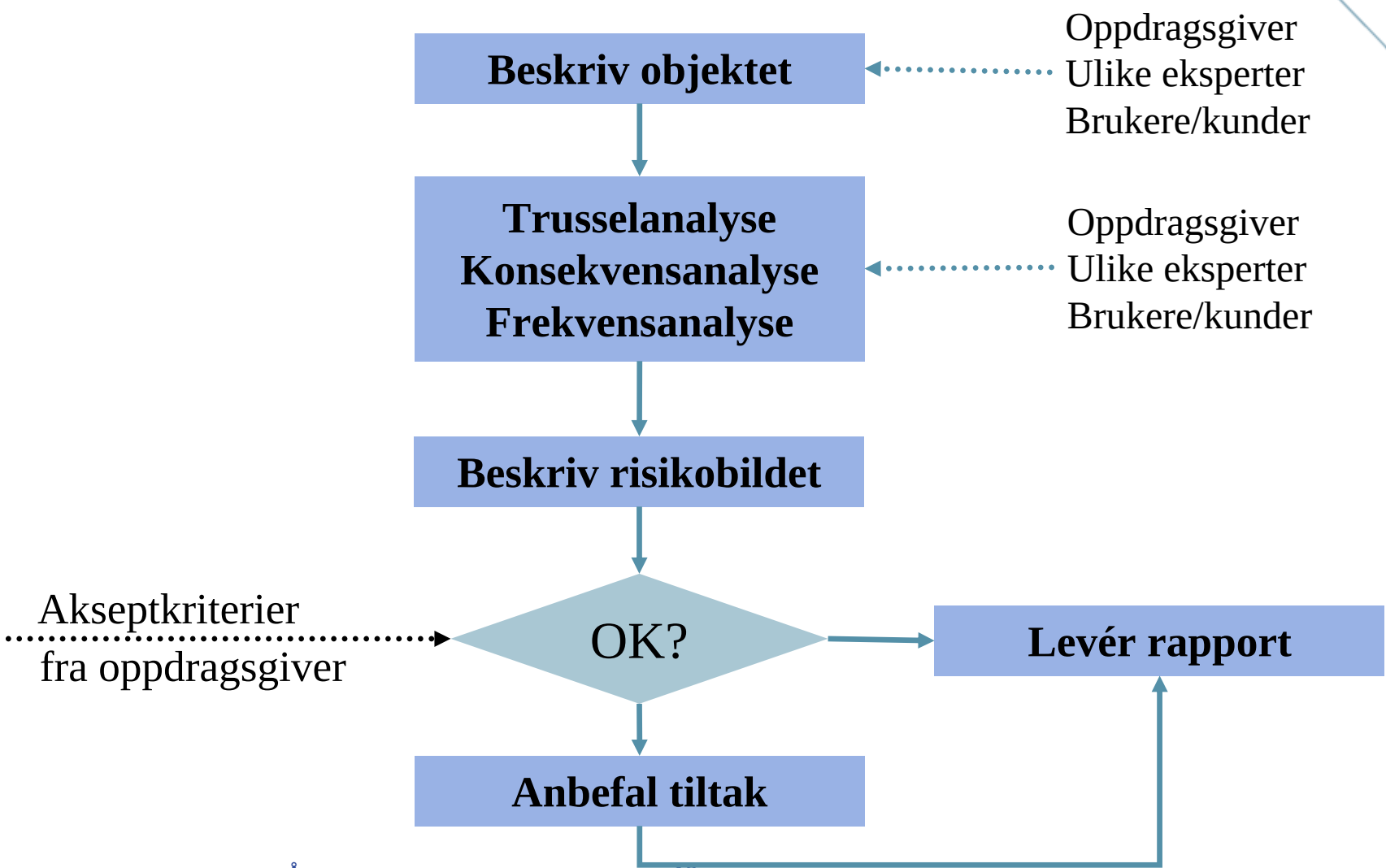
telenor



TeleRisk = Telenors Risikoanalysemetode

- Noen målsettinger med TeleRisk
  - Ansatte skal kunne gjøre enkle risikoanalyser selv
  - Snakke samme risikospråk
  - Gi ny innsikt og forståelse → involvering
  - Fremme handling … og oppfølging
  - He en fleksibel og felles grunnmetodikk i bunn
- Første versjon av TeleRisk ble tatt i bruk i 1996
- TeleRisk videreutvikles kontinuerlig
  - Basert på forskning og/eller empiri

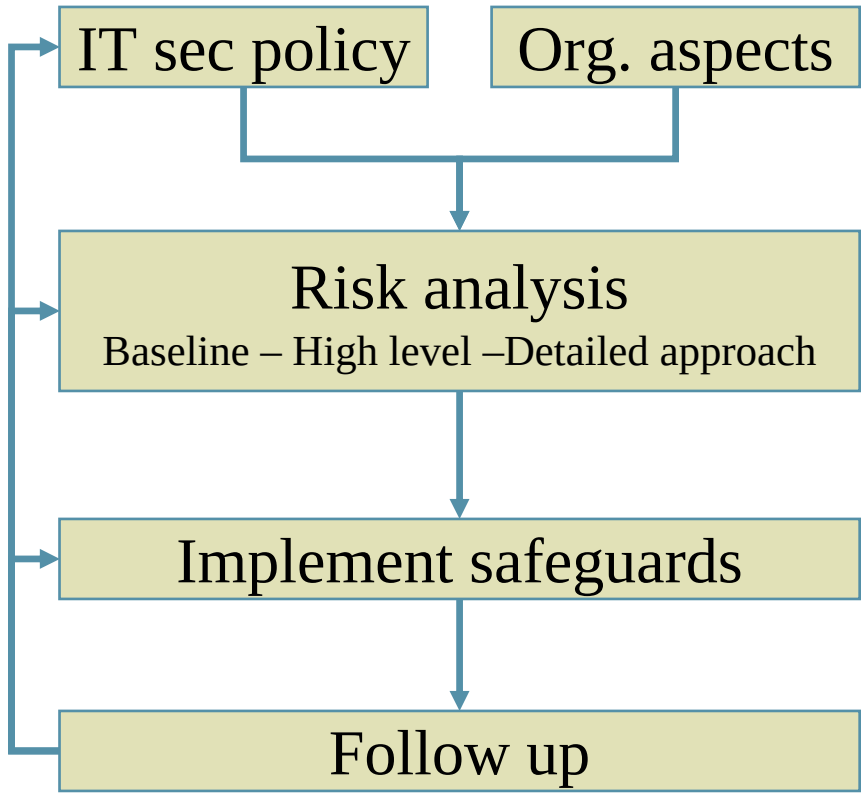
TeleRisk = Telenors Risikoanalysemetode



TeleRisk og ISO/IEC TR 13335-3

"Techniques for the Management of IT Security "

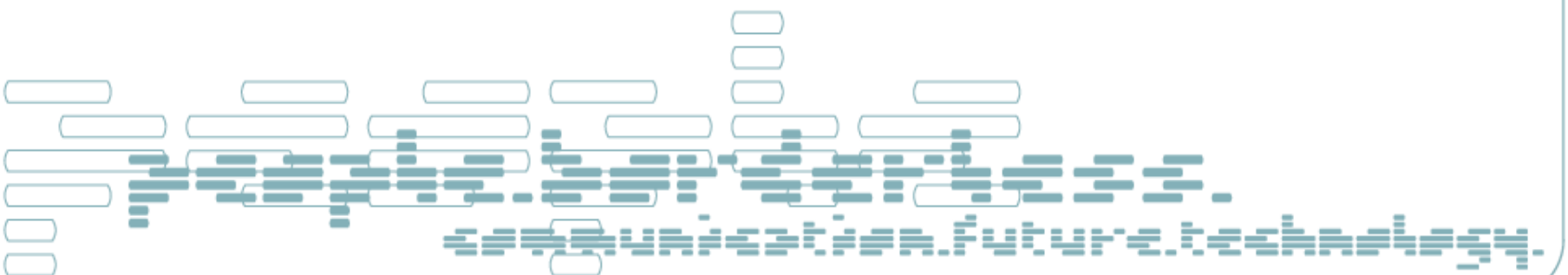
- Baseline
  - Forhåndsdefinerte sikkerhetsmekanismer, gitt av sikkerhetsklassen.
- High level risk analysis
  - Forenklet risikoanalyse
- Detailed approach
  - Utvidet risikoanalyse



Risikoanalyse i Telenor

telenor

Fem enkle trinn



Praktisk risikoanalyse, trinn 1, klassifisering

	Poeng	Begrunnelse
Økonomi	1-2-3-4-5	
Marked	1-2-3-4-5	
Avhengighet	1-2-3-4-5	
Rammekrav	1-2-3-4-5	
Sikkerhetsprofil	1-2-3-4-5	
Sikkerhetsklasse	A – B – C – D	

- Tre perspektiv: Telenor, kunden og samfunnet
- Klassifiseringen gjøres med tanke på ”viktighet”, ikke med tanke på sikkerhet, og tar utgangspunkt i forretningsmessig verdi og dens betydning for Telenor og selskapets kunder
- Hensikten med klassifiseringen er å avgjøre
  1. Omfanget/dybden av risikoanalysen
  2. Basisnivå sikkerhetsmekanismer

Praktisk risikoanalyse, trinn 2, Planlegg analysen

1. Aktivitet	1. Aktivitet	1. Aktivitet	1. Aktivitet
2. Aktivitet	2. Aktivitet	2. Aktivitet	2. Aktivitet
3. Aktivitet	3. Aktivitet	3. Aktivitet	3. Aktivitet
….	….	….	….
n. Aktivitet	n. Aktivitet	n. Aktivitet	n. Aktivitet

Planlegging innebærer tilpasning av standardisert prosess, valg av rapportmal og verktøy/hjelpemidler

Praktisk risikoanalyse, trinn 3, trusselidentifikasjon

- Trusselidentifikasjonen er en styrt idédugnad
  - Gjerne HazOp
- Hva er en trussel?
  - Ikke brann/hærverk → men at et system går ned
- How to
  - Plugg-inn modul gir faglig fokus på risikoanalysen, f eks
    - Sikkerhets- og pålitelighetsrisiko
    - Prosjektrisiko
    - Forretningsprosesser
    - Osv…

Praktisk risikoanalyse, trinn 4, etablere risikobilde

- Analyse av konsekvens & frekvens er manuell (eller datamaskinstøttet i tyngre analyser)
- Sekkeposter brukes i Forenklet risikoanalyse
  - Standard er 4x4 matrise
- Oppdragsgiver bestemmer akseptabel risiko
  - ALARP brukes ikke
- Poenget er ikke å unngå risiko, men å *velge* risikoen
  - Og når valget er tatt, å undersøke årsakene til at trusselen utløses slik at tiltak blir effektive

Praktisk risikoanalyse, trinn 5, anbefale tiltak

- Tiltak skal bare identifiseres for uakseptabel risiko
- Krav til tiltak:
  - Helhetlige
  - Effektive
  - Lønnsomme
- Tiltak skal grupperes etter effekt
  - Unngå skade eller trusler
  - Forebygge skade
  - Redusere frekvens/sluttkonsekvens
  - Overføre risiko
  - Trenger grundigere vurderinger

Bruk av risikobildet

telenor

Risikoanalyser skal støtte ledere …

- Ved ”sjefsvennlig” dokumentasjon
  - Enkel kommunikasjon uten IT-språk
  - Ikke tusen detaljer i alle prosjekter → porteføljetenking
  - Pedagogisk presentasjon → gir beslutninger
- Som tilleggsinformasjon ved beslutninger
  - Kan risikoanalysen gi tilleggsinformasjonen med positiv nåverdi?
  - Svaret på spørsmålet avgjør om analysen er verd å gjennomføre
- Til å fokusere sikkerhetsarbeid
  - Setter fokus på kritiske prosesser → sparer penger
  - Overholde krav og oppfylle alminnelige forventninger
- Ved å øke intellektuell kapital
  - Humankapital, relasjonskapital, strukturkapital

Risikobildet– og oppdragsgivers akseptkriterier

Konsekvens	*Sannsynlighet*			
	Lite trolig	**Kan skje**	**Vanlig**	**Svært vanlig**
Liten	T1 T15	T2 T7	T14	T13
Middels	T3	T8 T4	T10	
Alvorlig	T16	T6 T12		**T9**
Katastrofal			**T11**	

Risikobildet som prioriteringsverktøy

Sannsynlighet

Konsekvens

	Liten	**Middels**	**Stor**
Ubetydelig	Aksepter risikoene **Fjerne tiltak?**		
Merkbar		Overvåk risiko **Velg tiltak**	
Alvorlig			Ledelsesfokus **Må gjøre noe!**

Arbeidsmetodikk – gangen i arbeidet

- Avgrensning av objektet – hva er det som skal kartlegges
- Kartlegging objektet / objektene
  - Beskrives på to nivåer
    - Logisk nivå
    - Fysisk nivå, hvordan systemet er realisert rent fysisk
- Styrt Idémyldring – HazOp
  - hvert objekt for seg
  - brukerdeltakelse fra kunden, objekt for objekt
- Presentasjon av resultatene
  - Risikobildet (sannsynlighet og konsekvens)
- Oppdragsgiver beslutter akseptnivå
- Forslag til tiltak / anbefalinger
- Spesifikasjon
  - Kommer som følge av anbefalingen / forslag til tiltak

Praktiske erfaringer med metodikken (1)

- Beskrivelse av objektet - det som skal analyseres
  - Kundens (IT-avdelingen/oppdragsgiver) oppfatning av hvordan egne systemer virkelig er stemmer sjelden helt med virkeligheten
  - Oppgaven med å beskrive objektet (objektene) som skal analyseres blir alltid undervurdert
  - Virker oppdragende på kunden, han er nødt til å beskrive egne systemer, ofte mangler beskrivelsene helt eller delvis
- Hvilke kriterier som skal legges til grunn for må analysen avklares på forhånd (tilgjengelighet, integritet, konfidensialitet etc)

Praktiske erfaringer med metodikken (2)

- Vi formidler resultatene av analysen for toppledelsen i et ”ikke teknisk” språk som blir forstått
  - Vi er en støtte for IT-avdelingen, ikke en trussel
  - IT-avdelinger har tradisjon for å hindre tilgang - ”forby” det som er risikabelt
- Kunden – brukerne – må tas med i risikoanalysen
  - Når du vurderer et system, ta med de som virkelig bruker det i vurderingene
- Det er ofte vanskelig å få kunden med å stille med bruker-ressurser - ”IT-avdelingen kan ta seg av dette”
  - Erfaringen er at når brukerne kommer med så øker engasjementet og ”sannheten” legges på bordet
  - Brukerne oppfatter metodikken som logisk og lett å forstå
- To leveranser
  - Rapporten
  - Opplæring ved at de som deltar i analysen ”lærer seg” metodikken

Hvilken risiko kan aksepteres - akseptnivå

- Det vi som konsulent gjør er å definere risikobildet og få aksept fra kunden for at bildet er riktig og troverdig
  - Forankringen skjer i stor grad under selve prosessen
- Vi utarbeider forslag til tiltak mot de ulike risikoelementene som ikke kan aksepteres – tiltaksplan/handlingsplan
- Kunden må selv beslutte hvilket risikonivå som kan aksepteres

Erfaringer med TeleRisk

Fordeler

- Skalerbar analysedybde
- Enkle, raske og gode analyser
- Kommuniserbar risikomatrise
- Leder til ny innsikt for overordnet nivå
- Beslutningsorientert
- Kvalitativ / kvantitativ
- Takler nye situasjoner

Ulemper

- Kvalitet avhengig av brukeren/deltakerne
- Entusiasme i prosessen kan lede til at man finner (for) mange trusler – prioritering

Konklusjon

- Et foretak eller en organisasjonen som ikke har verdier eller trusler trenger ikke sikkerhet.
- Risikoanalysen gir tilleggsinformasjon for beslutninger og den gir øker kompetansen hos de som deltar i den
- Å kreve 100% sikkerhet er som regel feil. Poenget er å ha tenkt gjennom hva som godtas/ikke godtas.
- Risikoanalysen er en måte å finne et fornuftig sikkerhetsnivå for din bedrift/organisasjon.