Direktoratet for forvaltning og IKT

Aggregering av risiko - behov og utfordringer i risikostyringen

SINTEF-seminar 4.4.2017

Jan Sørgård, Seniorrådgiver i Difi
Seksjon for informasjonssikkerhet og datadeling
Avdeling for digital forvaltning

Kort om Difi

- Samfunnsoppdrag
  - Være det sentrale fagorganet for modernisering og omstilling av offentlig sektor
- Strategiske satsningsområder
  - Effektivisering – Brukerorientering - Samordning
- Områder
  - Ledelse og organisering
  - Digital forvaltning (herunder informasjonssikkerhet)
  - Offentlige anskaffelser
  - Forvaltning og utvikling av (5) felleskomponenter
  - Tilsyn etter forskrift om universell utforming av IKT-løsninger
- Cirka 280 ansatte
- Oslo og Leikanger

Difis rolle og mandat innen informasjonssikkerhet

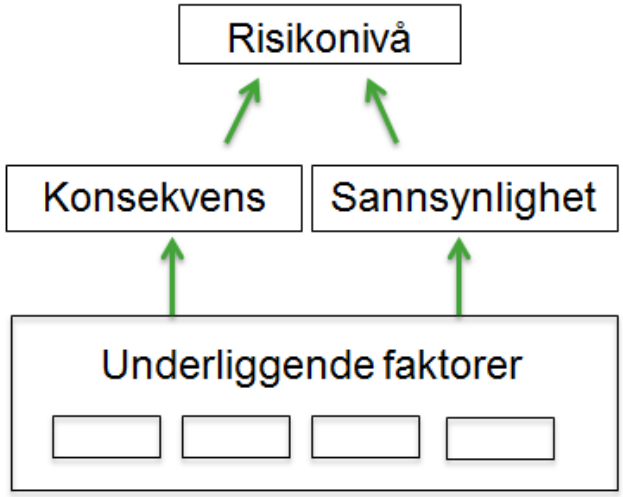
- *Statsforvaltningen*
  - *Arbeide for en styrket og mer helhetlig tilnærming*
  - *Være en pådriver for, og bidra til, bedre styring og kvalitetssikring*

- Stat og kommune
  - Gi anbefalinger og veiledning til forvaltningsorgan om internkontroll på informasjonssikkerhetsområdet
    - jf. eForvaltningsforskriften §15

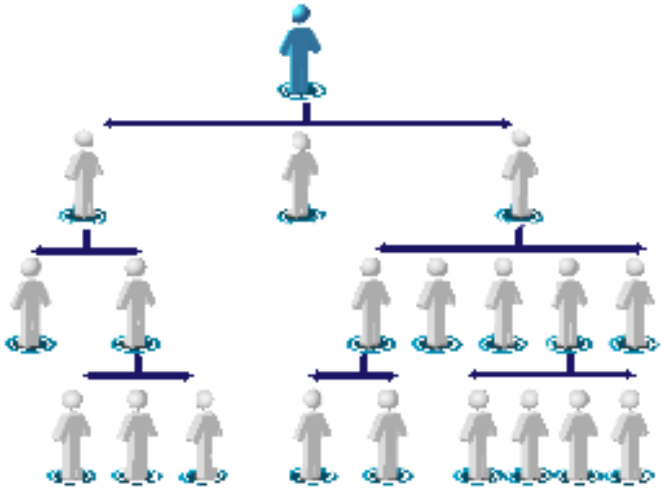
Aggregering av risiko

- Hva mener man?

I risikovurderinger

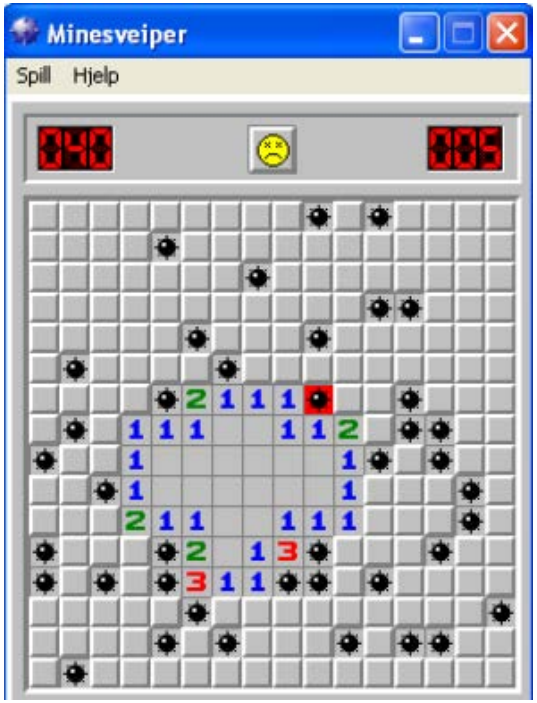


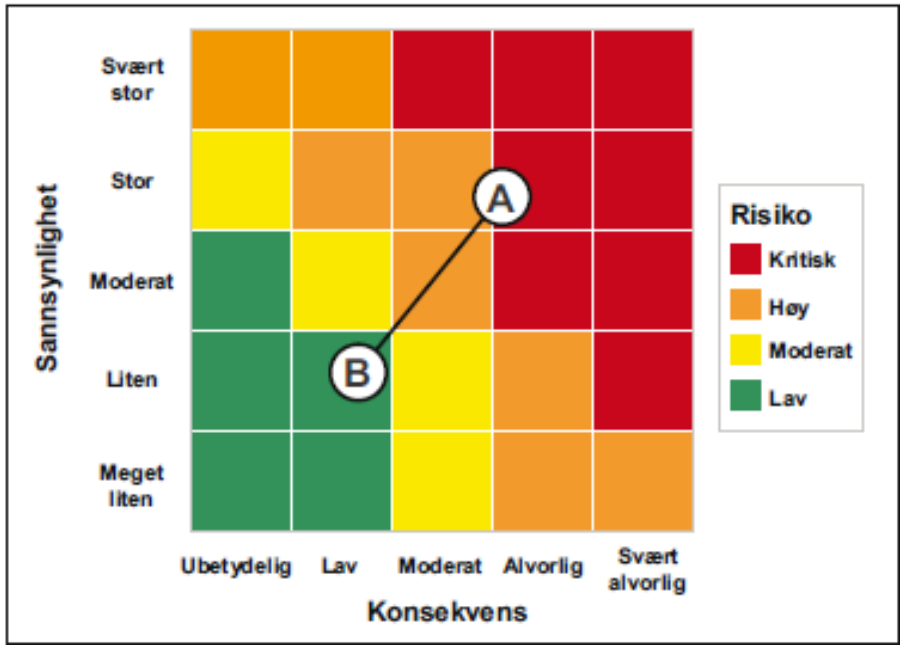
Opp gjennom organisasjonen



- Hva skal aggregeres?
- Hva skal man bruke det til?
- Gir aggregering pålitelig og nyttig informasjon?
- Er det samsvar mellom ressursbruk og nytte?

Hva er dette?

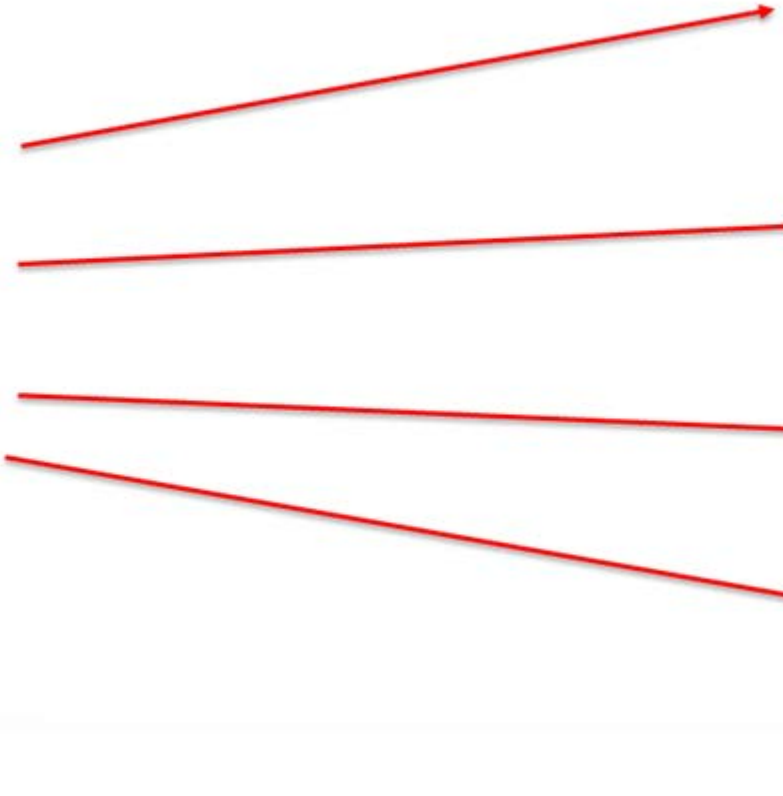




- Minesveipersyndromet
  - Mer opptatt av teknikker, verktøy og fine presentasjoner enn risikoforståelse, risikoanalyse og god risikokommunikasjon

FORSTÅ RISIKO

Sklir på isen



Liv og helse	Øko-nomi	Tjeneste-nivå
	?	?

Uønsket hendelse / Risikobeskrivelse / Scenario

utløsende hendelse, følgehendelse, følgehendelse, …. konsekvens ….. …….

Sklir på isen

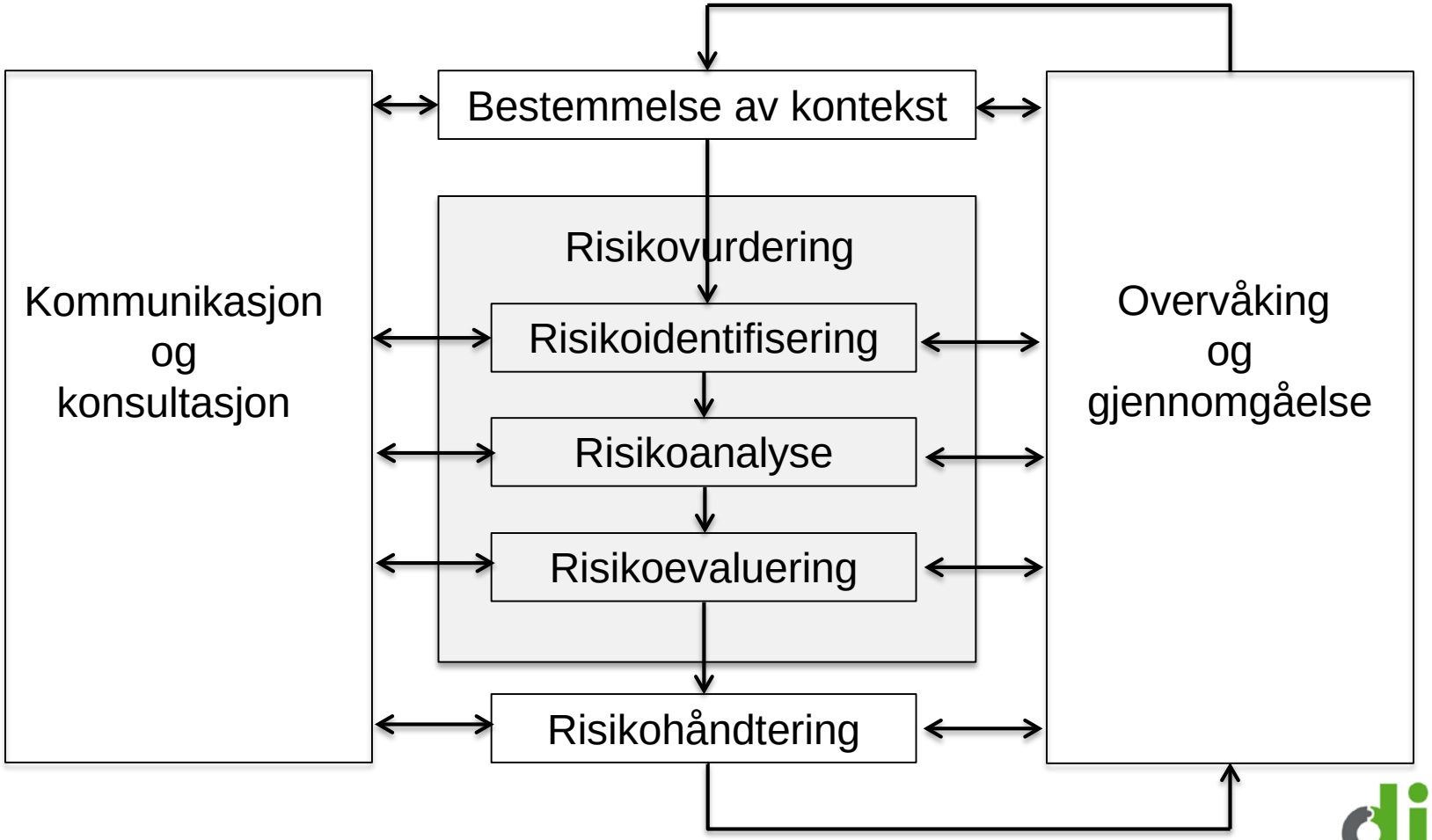
Liv og helse	Øko-nomi	Tjeneste-nivå
	?	?
		
		
		

Hva er risikoen?
Hvilken konsekvens?
Sannsynlighet for hva?
Hva er hendelsen?

ISO 31000 Risikostyring

Prinsipper og retningslinjer

Risikostyringsprosessen



ISO 31010

Metoder for risikovurdering

- 31 metoder/verktøy nevnt
  - Er likevel ikke en komplett liste
  - Kan kombineres til sammensatte og helhetlige metoder

- Gir ulik støtte under
  - identifisere
  - analysere
  - evaluere

- Mange er også relevant under
  - håndtere risiko
  - i kommunikasjon

Utfordringer ved aggregering

- Forskjellene mellom strategisk-, taktisk-, operativ/operasjonell-, finansiell- og prosjekt-risiko
- Ulike risikovurderinger kan ha behov for ulike metoder og støtteverktøy
- Ulik kunnskapsstyrke i analysene
- Man benytter ofte forenklinger – bevisst eller dessverre ubevist
  - En uønsket hendelse vil oftest ha flere mulige konsekvenser med ulik sannsynlighet
  - Man velger ofte bare å uttrykke en kombinasjon
  - Man bør ofte supplere med skriftlige kvalitative vurderinger
- Minesveipersyndromet
  - Mer opptatt av teknikker, verktøy og fine presentasjoner enn risikoforståelse, risikoanalyse og god risikokommunikasjon

Formål med risikovurderinger

- Både risikovurderinger og forslag til håndtering av risiko er beslutningsgrunnlag for ledere
  - om aksept av risiko
  - og annen risikohåndtering

- Beslutningene bør skje
  - i samsvar med virksomhetsledelsens krav og føringer
  - på tilstrekkelige beslutningsgrunnlag
  - på hensiktsmessig og riktig ledernivå

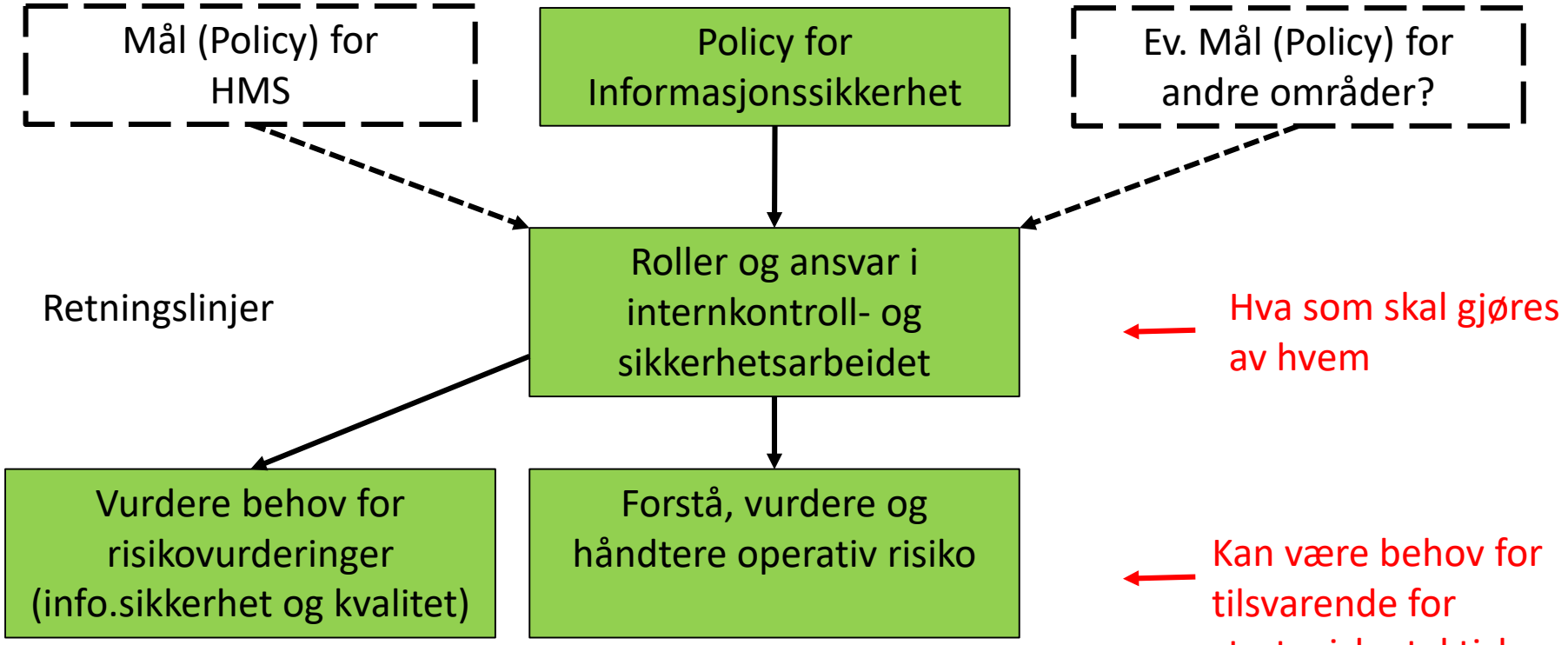
Virksomhetsledelsens behov 1

- Få etablert en systematikk
  - der risikoer rundt om i hele virksomheten blir identifisert, analysert, håndtert mv. i samsvar med virksomhetsledelsens føringer
  - herunder at virksomhetsledelsen og andre ledernivå blir involvert når det er nødvendig

- Systematikken kalles internkontroll (styring og kontroll)
  - eller styringssystem, ledelsessystem, sikkerhetsadministrasjon…

Difis forklaringsmodell for internkontroll/styringssystem

Overordnede styrende dokumenter



Del av retningslinje (eksempel)

Forstå, vurdere og håndtere operativ risiko

Vedlegg D: Normerende beskrivelser av konsekvensnivå

	Konsekvens-kategori	Indikatorer	Konsekvensnivå				
			Ubetydelig	Lav	Moderat	Høy	Svært høy
Virksomhetskritisk	Tjenestenivå	Virkning [3]	Ikke merkbart	Et lite merkbart økonomisk eller rettighetsmessig tap	Et godt merkbart økonomisk eller rettighetsmessig tap	Påvirker fungering i samfunnet	Vesentlig hindrer fungering i samfunnet (eller mer)
	Regelverk [4]	Virkning [3]					
	Personvern	Virkning [5]	Ikke merkbart	Noen kan føle seg krenket	De fleste ville følt seg krenket		
	HMS	Behandlingsbehov	Må ikke behandles	Må ikke til lege e.l.	Krever lege eller inntil 2 dg sykehus e.l.	2dg til 2 uker på sykehus e.l.	Mer enn 2 uker sykehus e.l.
		Sykemelding	Ingen	Maks 1 uke	Over 1, maks 5 uker	Over 5, maks 25 uker	Over 25 uker
	Vår økonomi	Økonomisk tap [6]	Tap <= 1.000	Tap <= 5.000	Tap <= 20.000	Tap <= 80.000	Tap > 80.000

Del av retningslinje (eksempel)

Forstå, vurdere og håndtere operativ risiko

Vedlegg E: Normerende beskrivelser av sannsynlighetsnivå

	Bruksområde:	**Vår økonomi** (+ evt. flere konsekvenskategorier)		Eventuelt andre konsekvenskategorier med andre intervallbehov
	Sannsynlighets-type:	**Hyppighet per år**	**Hyppighet per periode**	
Sannsynlighetsnivå				
	Svært høy	Over 50 ganger per år	Over 1 gang per uke	
	Høy	Inntil 50 ganger per år	Inntil 1 gang per uke	
	Moderat	Inntil 12 ganger per år	Inntil 1 gang per mnd.	
	Lav	Inntil 3 ganger per år	Inntil 1 gang hver 3. mnd.	
	Ubetydelig	Tilnærmet 0	Tilnærmet 0	

Bruk (jf. vedlegg G i eksempelet):

- Estimer nivå først ut fra trolig hyppighet (jf. vedlegg E)
- Vurder justering ut intensjon og kapasitet dersom det gjelder trusselaktører
- Vurder justering ut fra sårbarhet (tiltaksetablering/letthetsvurdering)

Del av retningslinje (eksempel)

Forstå, vurdere og håndtere operativ risiko

Risikonivå

Sannsynlighets-nivå	< --- Risikonivå --- >				
Svært høy	Ubetydelig	Moderat	Høy	Høy	Svært høy
Høy	Ubetydelig	Moderat	Moderat	Høy	Høy
Moderat	Ubetydelig	Lav	Moderat	Moderat	Høy
Lav	Ubetydelig	Lav	Lav	Moderat	Moderat
Ubetydelig	Ubetydelig	Ubetydelig	Ubetydelig	Ubetydelig	Ubetydelig
	Ubetydelig	**Lav**	**Moderat**	**Høy**	**Svært høy**
	Konsekvensnivå				

Normerende beskrivelser - konsekvensnivå

Vedlegg D: Normerende beskrivelser av konsekvensnivå

	Konsekvens-kategori	Indikatorer	Konsekvensnivå				
			Ubetydelig	**Lav**	**Moderat**	**Høy**	**Svært høy**
Virksomhetskritisk	Tjenestenivå	Virkning [3]	Ikke merkbart	Et lite merkbart økonomisk eller rettighetsmessig tap	Et godt merkbart økonomisk eller rettighetsmessig tap	Påvirker fungering i samfunnet	Vesentlig hindrer fungering i samfunnet (eller mer)
	Regelverk [4]	Virkning [3]					
	Personvern	Virkning [5]	Ikke merkbart	Noen kan føle seg krenket	De fleste ville følt seg krenket		
	HMS	Behandlingsbehov	Må ikke behandles	Må ikke til lege e.l.	Krever lege eller inntil 2 dg sykehus e.l.	2dg til 2 uker på sykehus e.l.	Mer enn 2 uker sykehus e.l.
		Sykemelding	Ingen	Maks 1 uke	Over 1, maks 5 uker	Over 5, maks 25 uker	Over 25 uker
	Vår økonomi	Økonomisk tap [6]	Tap <= 1.000	Tap <= 5.000	Tap <= 20.000	Tap <= 80.000	Tap > 80.000

Normerende beskrivelser - sannsynlighetsnivå

Vedlegg E: Normerende beskrivelser av sannsynlighetsnivå

	Bruksområde:	**Vår økonomi** (+ evt. flere konsekvenskategorier)		Eventuelt andre konsekvenskategorier med andre intervallbehov
	Sannsynlighets-type:	**Hyppighet per år**	**Hyppighet per periode**	
Sannsynlighetsnivå	**Svært høy**	Over 50 ganger per år	Over 1 gang per uke	
	Høy	Inntil 50 ganger per år	Inntil 1 gang per uke	
	Moderat	Inntil 12 ganger per år	Inntil 1 gang per mnd.	
	Lav	Inntil 3 ganger per år	Inntil 1 gang hver 3. mnd.	
	Ubetydelig	Tilnærmet 0	Tilnærmet 0	

Kriterier for å akseptere risiko inklusiv føringer for risikohåndtering og hvem som kan akseptere risikoer på ulikt nivå

Ofte «the missing link» ved internkontroll / styringssystem

Vedlegg B: Kriterier for å akseptere risiko

Risikonivå	Kriterier for å akseptere risiko
Lav	Kan aksepteres **uten å lete etter eller vurdere nytten av** alternative arbeidsmåter eller flere risikoreduserende tiltak. Merk at dette gjelder når hele utfallsrommet for en risiko har risikoestimerelse på nivå lav innen alle berørte konsekvenskategorier.
	Kan aksepteres av ledere på alle beslutningsnivå.
Moderat	Oppgaven/tjenesten som utføres har **vesentlig betydning** for å nå **virksomhetens mål**.
	Det er gjennomført et **systematisk arbeid** for å identifisere alternative arbeidsmåter og risikoreduserende tiltak for denne eller direkte sammenlignbare risikoer.
	Alternative arbeidsmåter som gjør at man kan unngå risikoen **er uhensiktsmessige, gir høyere risiko på dette eller andre områder, eller er vesentlig mer kostbare.**
	Tiltak er valgt i samsvar med **prinsippene** for **ALARP** på liv og helse og **nytte/kost** på øvrige områder (jf. kapittel *4 Førende prinsipper for risikohåndteringen*)
	Nytten ved at oppgaven/tjenesten utføres anses større enn risikoen.
	Kan aksepteres av ledere på alle beslutningsnivå.
Høy	Oppgaven/tjenesten som utføres er **nødvendig** for å nå **virksomhetens mål**.
	Det er gjennomført et **systematisk og grundig** arbeid for å identifisere alternative arbeidsmåter og risikoreduserende tiltak for denne eller direkte sammenlignbare risikoer.
	Alternative arbeidsmåter som gjør at man kan unngå risikoen **er svært uhensiktsmessige, gir høyere risiko på dette eller andre områder, eller er svært kostbare.**
	Tiltak er valgt i samsvar med **prinsippene** for **ALARP** på liv og helse og **nytte/kost** på øvrige områder (jf. kapittel *4 Førende prinsipper for risikohåndteringen*)
	Nytten ved at oppgaven/tjenesten utføres er større enn risikoen.
	Kan kun aksepteres av ledere på minimum avdelingssjefsnivå.
Svært høy	Oppgaven/tjenesten som utføres er **strengt nødvendig** for å nå **virksomhetens mål**.
	Det er gjennomført et **systematisk og svært grundig** arbeid for å identifisere alternative arbeidsmåter og risikoreduserende tiltak for denne eller direkte sammenlignbare risikoer.
	Alternative arbeidsmåter som gjør at man kan unngå risikoen **er totalt uhensiktsmessige, gir høyere risiko på dette eller andre områder, eller er utenfor virksomhetens økonomiske handlingsrom.**
	Tiltak er valgt i samsvar med **prinsippene** for **ALARP** på liv og helse og **nytte/kost** på øvrige områder (jf. kapittel *4 Førende prinsipper for risikohåndteringen*)
	Nytten ved at oppgaven/tjenesten utføres er større enn risikoen.
	Kan kun aksepteres av direktør eller assisterende direktør.

Risikonivå

Sannsynlighets-nivå	< --- Risikonivå --- >				
Svært høy	Ubetydelig	Moderat	Høy	Høy	Svært høy
Høy	Ubetydelig	Moderat	Moderat	Høy	Høy
Moderat	Ubetydelig	Lav	Moderat	Moderat	Høy
Lav	Ubetydelig	Lav	Lav	Moderat	Moderat
Ubetydelig	Ubetydelig	Ubetydelig	Ubetydelig	Ubetydelig	Ubetydelig
	Ubetydelig	**Lav**	**Moderat**	**Høy**	**Svært høy**
	Konsekvensnivå				

Normerende beskrivelser - konsekvensnivå

Vedlegg D: Normerende beskrivelser av konsekvensnivå

	Konsekvens-kategori	Indikatorer	Konsekvensnivå				
			Ubetydelig	**Lav**	**Moderat**	**Høy**	**Svært høy**
Virksomhetskritisk	Tjenestenivå	Virkning [3]	Ikke merkbart	Et lite merkbart økonomisk eller rettighetsmessig tap	Et godt merkbart økonomisk eller rettighetsmessig tap	Påvirker fungering i samfunnet	Vesentlig hindrer fungering i samfunnet (eller mer)
	Regelverk [4]	Virkning [3]					
	Personvern	Virkning [5]	Ikke merkbart	Noen kan føle seg krenket	De fleste ville følt seg krenket		
	HMS	Behandlingsbehov	Må ikke behandles	Må ikke til lege e.l.	Krever lege eller inntil 2 dg sykehus e.l.	2dg til 2 uker på sykehus e.l.	Mer enn 2 uker sykehus e.l.
		Sykemelding	Ingen	Maks 1 uke	Over 1, maks 5 uker	Over 5, maks 25 uker	Over 25 uker
	Vår økonomi	Økonomisk tap [6]	Tap <= 1.000	Tap <= 5.000	Tap <= 20.000	Tap <= 80.000	Tap > 80.000

Normerende beskrivelser - sannsynlighetsnivå

Vedlegg E: Normerende beskrivelser av sannsynlighetsnivå

	Bruksområde:	**Vår økonomi** (+ evt. flere konsekvenskategorier)		Eventuelt andre konsekvenskategorier med andre intervallbehov
	Sannsynlighets-type:	**Hyppighet per år**	**Hyppighet per periode**	
Sannsynlighetsnivå	**Svært høy**	Over 50 ganger per år	Over 1 gang per uke	
	Høy	Inntil 50 ganger per år	Inntil 1 gang per uke	
	Moderat	Inntil 12 ganger per år	Inntil 1 gang per mnd.	
	Lav	Inntil 3 ganger per år	Inntil 1 gang hver 3. mnd.	
	Ubetydelig	Tilnærmet 0	Tilnærmet 0	

Del av retningslinje (eksempel)

Forstå, vurdere og håndtere operativ risiko

Vedlegg B: Kriterier for å akseptere risiko

Risikonivå	Kriterier for å akseptere risiko
Lav	Kan aksepteres **uten å lete etter eller vurdere nytten av** alternative arbeidsmåter eller flere risikoreduserende tiltak. Merk at dette gjelder når hele utfallsrommet for en risiko har risikostørrelse på nivå lav innen alle berørte konsekvenskategorier.
	Kan aksepteres av ledere på alle beslutningsnivå.
Moderat	Oppgaven/tjenesten som utføres har **vesentlig betydning** for å nå **virksomhetens mål**.
	Det er gjennomført et **systematisk arbeid** for å identifisere alternative arbeidsmåter og risikoreduserende tiltak for denne eller direkte sammenlignbare risikoer.
	Alternative arbeidsmåter som gjør at man kan unngå risikoen **er uhensiktsmessige, gir høyere risiko på dette eller andre områder, eller er vesentlig mer kostbare.**
	Tiltak er valgt i samsvar med **prinsippene** for **ALARP** på liv og helse og **nytte/kost** på øvrige områder (jf. kapittel *4 Førende prinsipper for risikohåndteringen*)
	Nytten ved at oppgaven/tjenesten utføres ansees større enn risikoen.
	Kan aksepteres av ledere på alle beslutningsnivå.

Høy	Oppgaven/tjenesten som utføres er **nødvendig** for å nå **virksomhetens mål**.
	Det er gjennomført et **systematisk og grundig** arbeid for å identifisere alternative arbeidsmåter og risikoreduserende tiltak for denne eller direkte sammenlignbare risikoer.
	Alternative arbeidsmåter som gjør at man kan unngå risikoen **er svært uhensiktsmessige, gir høyere risiko på dette eller andre områder, eller er svært kostbare.**
	Tiltak er valgt i samsvar med **prinsippene** for **ALARP** på liv og helse og **nytte/kost** på øvrige områder (jf. kapittel *4 Førende prinsipper for risikohåndteringen*)
	Nytten ved at oppgaven/tjenesten utføres er større enn risikoen.
	Kan kun aksepteres av ledere på minimum avdelingssjefsnivå.
Svært høy	Oppgaven/tjenesten som utføres er **strengt nødvendig** for å nå **virksomhetens mål**.
	Det er gjennomført et **systematisk og svært grundig** arbeid for å identifisere alternative arbeidsmåter og risikoreduserende tiltak for denne eller direkte sammenlignbare risikoer.
	Alternative arbeidsmåter som gjør at man kan unngå risikoen **er totalt uhensiktsmessige, gir høyere risiko på dette eller andre områder, eller er utenfor virksomhetens økonomiske handlingsrom.**
	Tiltak er valgt i samsvar med **prinsippene** for **ALARP** på liv og helse og **nytte/kost** på øvrige områder (jf. kapittel *4 Førende prinsipper for risikohåndteringen*)
	Nytten ved at oppgaven/tjenesten utføres er større enn risikoen.
	Kan kun aksepteres av direktør eller assisterende direktør.

Kriterier for å akseptere risiko inklusiv føringer for risikohåndtering og hvem som kan akseptere risikoer på ulikt nivå

Ofte «the missing link» ved internkontroll / styringssystem

Vedlegg B: Kriterier for å akseptere risiko

Risikonivå	Kriterier for å akseptere risiko
Lav	Kan aksepteres **uten å lete etter eller vurdere nytten av** alternative arbeidsmåter eller flere risikoreduserende tiltak. Merk at dette gjelder når hele utfallsrommet for en risiko har risikoestimerelse på nivå lav innen alle berørte konsekvenskategorier.
	Kan aksepteres av ledere på alle beslutningsnivå.
Moderat	Oppgaven/tjenesten som utføres har **vesentlig betydning** for å nå **virksomhetens mål**.
	Det er gjennomført et **systematisk arbeid** for å identifisere alternative arbeidsmåter og risikoreduserende tiltak for denne eller direkte sammenlignbare risikoer.
	Alternative arbeidsmåter som gjør at man kan unngå risikoen **er uhensiktsmessige, gir høyere risiko på dette eller andre områder, eller er vesentlig mer kostbare.**
	Tiltak er valgt i samsvar med **prinsippene** for **ALARP** på liv og helse og **nytte/kost** på øvrige områder (jf. kapittel *4 Førende prinsipper for risikohåndteringen*)
	Nytten ved at oppgaven/tjenesten utføres anses større enn risikoen.
	Kan aksepteres av ledere på alle beslutningsnivå.
Høy	Oppgaven/tjenesten som utføres er **nødvendig** for å nå **virksomhetens mål**.
	Det er gjennomført et **systematisk og grundig** arbeid for å identifisere alternative arbeidsmåter og risikoreduserende tiltak for denne eller direkte sammenlignbare risikoer.
	Alternative arbeidsmåter som gjør at man kan unngå risikoen **er svært uhensiktsmessige, gir høyere risiko på dette eller andre områder, eller er svært kostbare.**
	Tiltak er valgt i samsvar med **prinsippene** for **ALARP** på liv og helse og **nytte/kost** på øvrige områder (jf. kapittel *4 Førende prinsipper for risikohåndteringen*)
	Nytten ved at oppgaven/tjenesten utføres er større enn risikoen.
	Kan kun aksepteres av ledere på minimum avdelingssjefsnivå.
Svært høy	Oppgaven/tjenesten som utføres er **strengt nødvendig** for å nå **virksomhetens mål**.
	Det er gjennomført et **systematisk og svært grundig** arbeid for å identifisere alternative arbeidsmåter og risikoreduserende tiltak for denne eller direkte sammenlignbare risikoer.
	Alternative arbeidsmåter som gjør at man kan unngå risikoen **er totalt uhensiktsmessige, gir høyere risiko på dette eller andre områder, eller er utenfor virksomhetens økonomiske handlingsrom.**
	Tiltak er valgt i samsvar med **prinsippene** for **ALARP** på liv og helse og **nytte/kost** på øvrige områder (jf. kapittel *4 Førende prinsipper for risikohåndteringen*)
	Nytten ved at oppgaven/tjenesten utføres er større enn risikoen.
	Kan kun aksepteres av direktør eller assisterende direktør.

Risikonivå

Sannsynlighets-nivå	< --- Risikonivå --- >				
Svært høy	Ubetydelig	Moderat	Høy	Høy	Svært høy
Høy	Ubetydelig	Moderat	Moderat	Høy	Høy
Moderat	Ubetydelig	Lav	Moderat	Moderat	Høy
Lav	Ubetydelig	Lav	Lav	Moderat	Moderat
Ubetydelig	Ubetydelig	Ubetydelig	Ubetydelig	Ubetydelig	Ubetydelig
	Ubetydelig	**Lav**	**Moderat**	**Høy**	**Svært høy**
	Konsekvensnivå				

Normerende beskrivelser - konsekvensnivå

Vedlegg D: Normerende beskrivelser av konsekvensnivå

	Konsekvens-kategori	Indikatorer	Konsekvensnivå				
			Ubetydelig	**Lav**	**Moderat**	**Høy**	**Svært høy**
Virksomhetskritisk	Tjenestenivå	Virkning [3]	Ikke merkbart	Et lite merkbart økonomisk eller rettighetsmessig tap	Et godt merkbart økonomisk eller rettighetsmessig tap	Påvirker fungering i samfunnet	Vesentlig hindrer fungering i samfunnet (eller mer)
	Regelverk [4]	Virkning [3]					
	Personvern	Virkning [5]	Ikke merkbart	Noen kan føle seg krenket	De fleste ville følt seg krenket		
	HMS	Behandlingsbehov	Må ikke behandles	Må ikke til lege e.l.	Krever lege eller inntil 2 dg sykehus e.l.	2dg til 2 uker på sykehus e.l.	Mer enn 2 uker sykehus e.l.
		Sykemelding	Ingen	Maks 1 uke	Over 1, maks 5 uker	Over 5, maks 25 uker	Over 25 uker
	Vår økonomi	Økonomisk tap [6]	Tap <= 1.000	Tap <= 5.000	Tap <= 20.000	Tap <= 80.000	Tap > 80.000

Normerende beskrivelser - sannsynlighetsnivå

Vedlegg E: Normerende beskrivelser av sannsynlighetsnivå

	Bruksområde:	**Vår økonomi** (+ evt. flere konsekvenskategorier)		Eventuelt andre konsekvenskategorier med andre intervallbehov
	Sannsynlighets-type:	**Hyppighet per år**	**Hyppighet per periode**	
Sannsynlighetsnivå	**Svært høy**	Over 50 ganger per år	Over 1 gang per uke	
	Høy	Inntil 50 ganger per år	Inntil 1 gang per uke	
	Moderat	Inntil 12 ganger per år	Inntil 1 gang per mnd.	
	Lav	Inntil 3 ganger per år	Inntil 1 gang hver 3. mnd.	
	Ubetydelig	Tilnærmet 0	Tilnærmet 0	

Virksomhetsledelsens behov 2

- Virksomhetsledelsens gjennomgang
  - Etterleves og fungerer internkontrollen/styringssystemet?
    - Blir pålagte aktiviteter gjennomført rundt om i virksomheten? (aggregering)
    - Avviks- og hendelseshåndtering (aggregering)
    - Evalueringer og revisjoner
  - Oversikt over spesielle forhold og risikoer
    - ut fra virksomhetens egenart og ledelsens fokus
    - Er (automatisk) aggregering av risikonivå e.l. svaret?
    - Eller er tilpassede rapporteringskrav mer hensiktsmessig?
    - Eller er det status på strategiske og taktiske risikoer man egentlig er ute etter?

Spørsmål som bør stilles når aggregering av risiko vurderes

- Hva er formålet ?
- Er det på aggregering av risiko eller på god internkontroll/styringssystem skoen trykker?
- Hvor nyttig er aggregering om man mangler god internkontroll/styringssystem?
- Forsvinner viktig forståelse av risikoene når man aggregerer?
- Bør man ha større fokus på nytte og risikostyring enn hva som teknisk kan aggregeres og automatiseres?

Oppsummert

- Minesveipersyndromet
  - Mer opptatt av teknikker, verktøy og fine presentasjoner enn risikoforståelse, risikoanalyse og god risikokommunikasjon
- Risikoforståelse og risikokommunikasjon
  - Risikoen ved å skli på isen som eksempel
  - Vit og kommuniser at man benytter forenklinger og hva som kan skjule seg bak disse
- «The missing link» i risikostyringen
  - Kriterier for å akseptere risiko, med føringer
    - for risikohåndtering
    - hvilket ledernivå som kan akseptere risikoer på ulikt risikonivå
- Virksomhetsledelsens gjennomgang
  - Bl.a. aggregering av om pålagte aktiviteter blir gjennomført og viktige ting fra avviks- og hendelseshåndteringen
- Vær kritisk rundt formål og nytte når man vurderer aggregering av risiko

Difis veiledningsmateriell

- Internkontroll.infosikkerhet.difi.no

- med maler og eksempler bl.a. for overordnede styrende dokumenter


difi
Direktoratet for
forvaltning og IKT