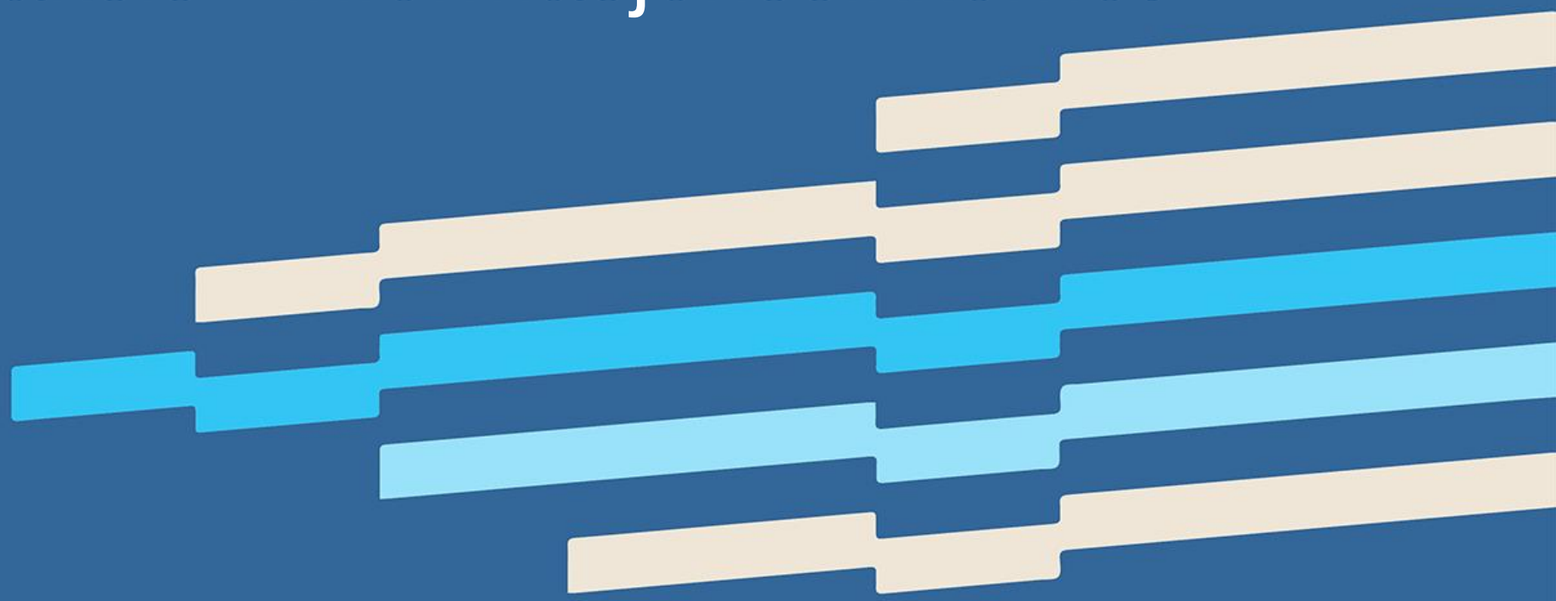
Difi
Direktoratet for
forvaltning og ikt

Innføringskurs
Internkontroll i praksis - informasjonssikkerhet

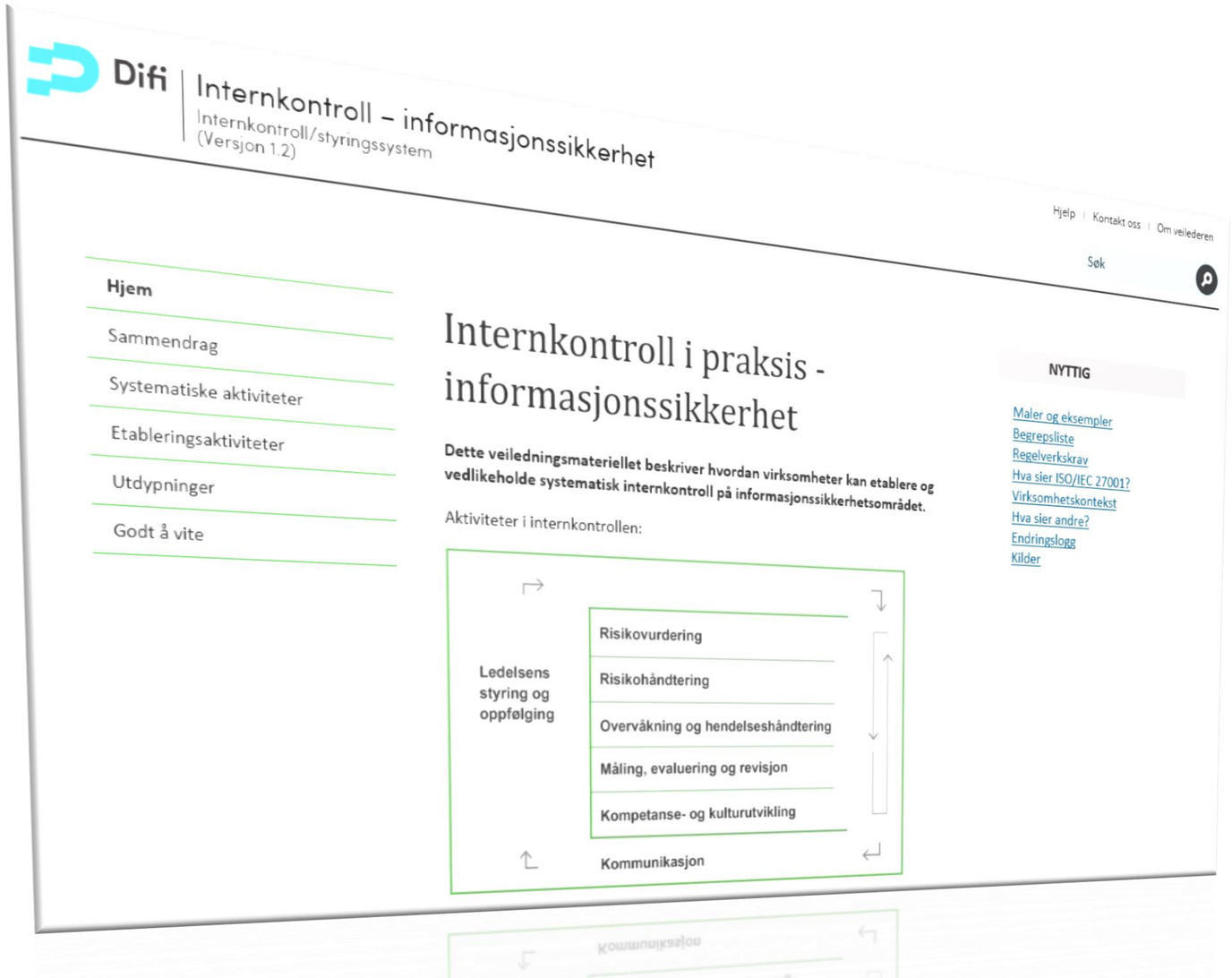
—

9. og 10. november 2017



Velkommen!

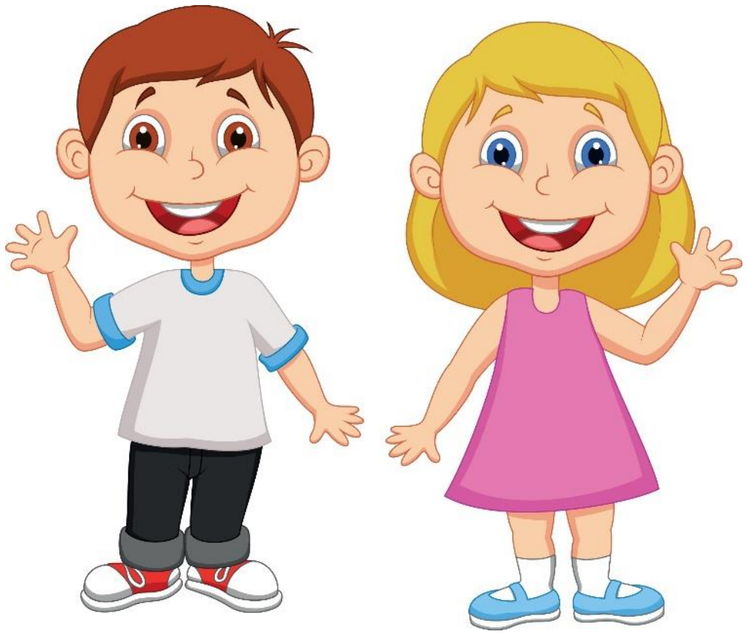
- «Internkontroll i praksis - informasjonssikkerhet»



Difi

Kort presentasjon av deltakerne

- Hvem er dere?
  - Navn
  - Virksomhet
  - Rolle/Stilling



Opplegg for kurset

- Kombinasjon av
  - Foredrag
  - Refleksjonsoppgaver
  - Gruppeoppgaver

- Spørsmål tar vi underveis

Kursdag 1

- Lunsj ca 11:20

Tema:

- Internkontroll og informasjonssikkerhet
- Begrep og roller
- Risikoforståelse
- Ledelsens styring og oppfølging
- Risikovurdering
- Risikohåndtering

Kursdag 2

- Oppstart 8:30
- Lunsj ca. 11:20

Tema:

- Oppsummering fra dag 1
- Overvåking og hendelseshåndtering
- Måling, evaluering og revisjon
- Kompetanse- og kulturutvikling
- Kommunikasjon
- Etableringsaktiviteter
- Overordnede styrende dokumenter
- Analysere status og planlegge etablering/forbedring
- Oppsummering og avslutning

http://internkontroll.infosikkerhet.difi.no

Difi | Internkontroll – informasjonssikkerhet
Internkontroll/styringssystem
(Versjon 1.2)

Hjelp | Kontakt oss | Om veilederen

Søk

Hjem

- Sammendrag
- Systematiske aktiviteter
- Etableringsaktiviteter
- Utdypninger
- Godt å vite

Internkontroll i praksis - informasjonssikkerhet

Dette veiledningsmateriellet beskriver hvordan virksomheter kan etablere og vedlikeholde systematisk internkontroll på informasjonssikkerhetsområdet.

Aktiviteter i internkontrollen:

NYTTIG

- Maler og eksempler
- Begrepsliste
- Regelverkskrav
- Hva sier ISO/IEC 27001?
- Virksomhetskontekst
- Hva sier andre?
- Endringslogg
- Kilder

Difi

Struktur på hovedaktiviteter

Ledelsens styring og oppfølging

Navn på hovedaktivitet

Dette er en beskrivelse av delaktivitetene under Ledelsens styring og oppfølging.

Målgruppe

- fagansvarlig informasjonssikkerhet
  - hele beskrivelsen
- personer som skal forberede eller lede enkeltaktiviteter
  - enkeltaktiviteter avhengig av ansvarsområde

Innhold

- Innledning
- Virksomhetsledelsens gjennomgang
- Delegere og følge opp gjennom linjen
- Sikre finansielle rammer for internkontroll- og sikkerhetsarbeidet
- Kommunisere viktighet
- Løfte og håndtere problemstillinger gjennom linjen
- Krise- og beredskapshåndtering

Oversikt over delaktiviteter

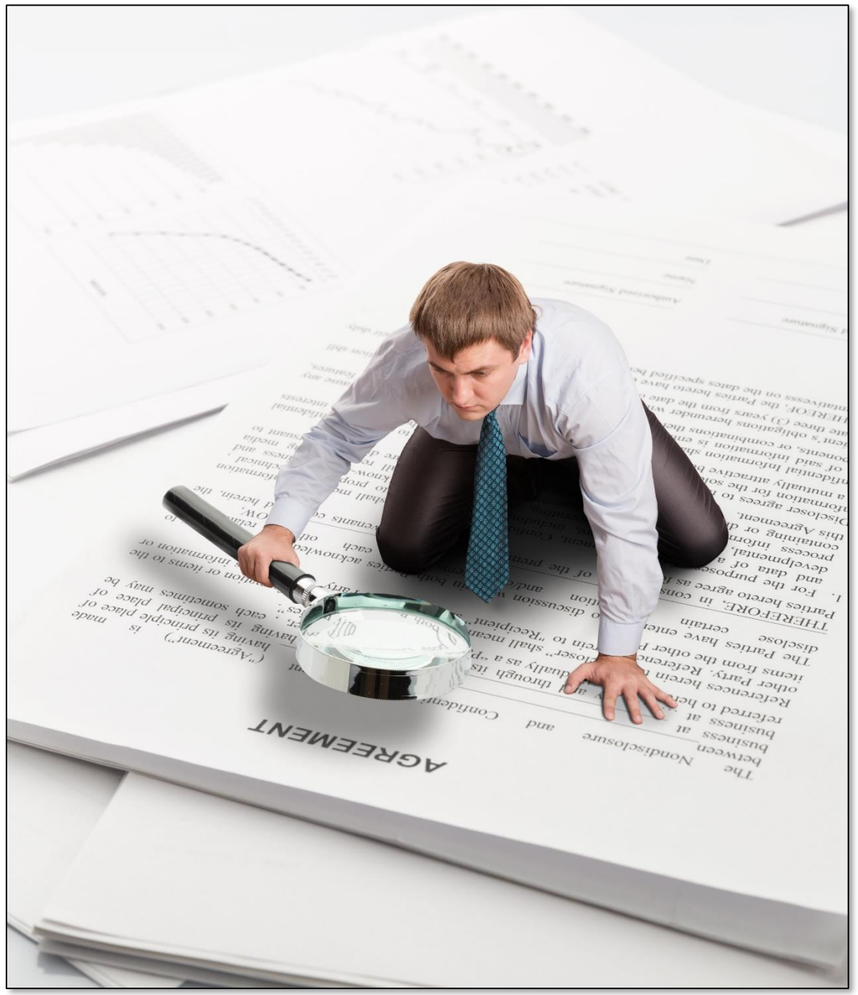
1 Innledning

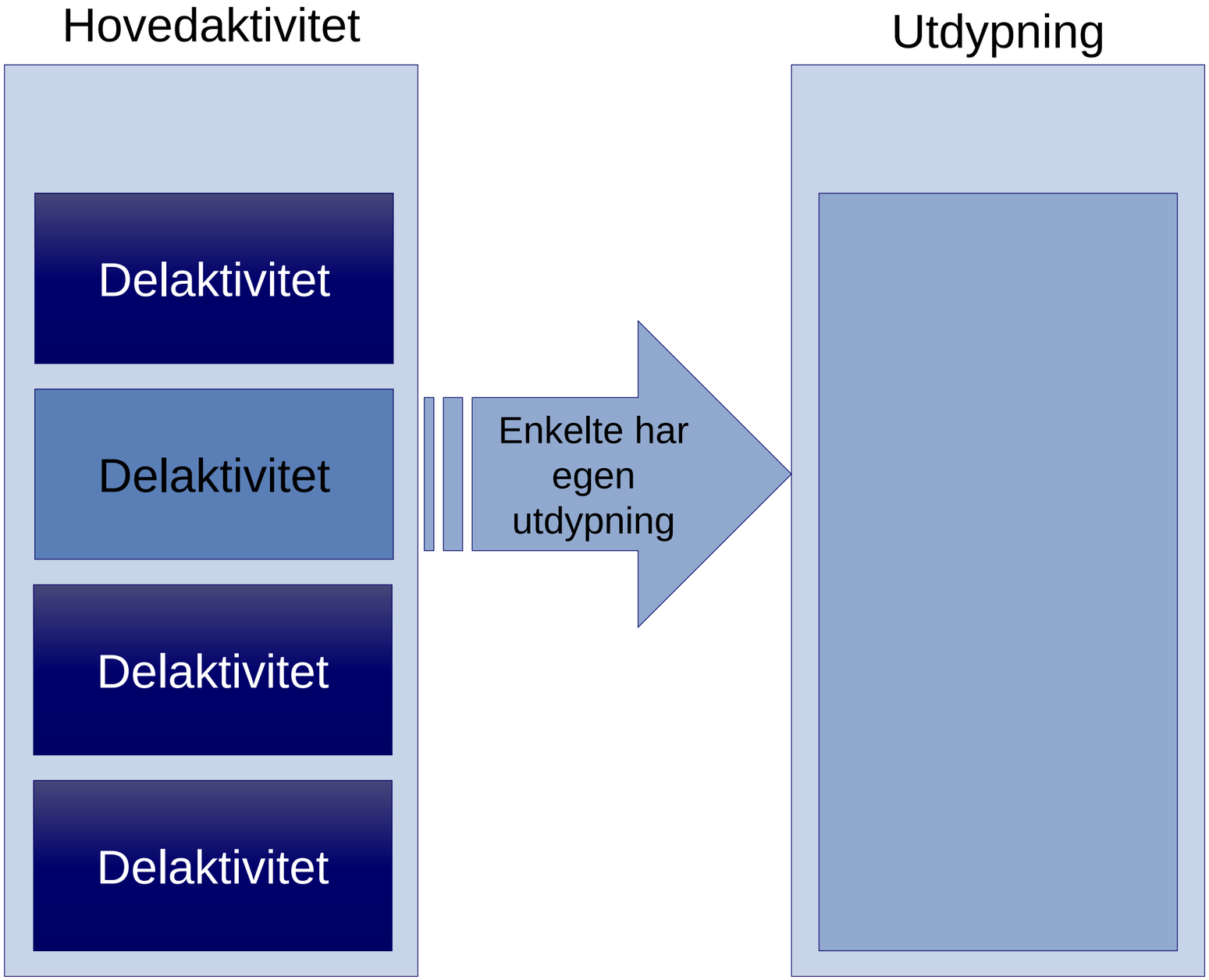
Det er virksomhetsledelsens ansvar å få etablert tilstrekkelig internkontroll i virksomheten. Det følger av lover og regler. Virksomhetsledelsen er i tillegg selv avhengig av tilstrekkelig styring og kontroll på informasjonssikkerhetsområdet for å lede virksomheten på en god måte. Det oppnår de gjennom etablering og oppfølging av et systematisk internkontrollarbeid i hele virksomheten.

Innholds-beskrivelse av delaktivitetene

Difi

Utdypningssider




Hovedaktivitet
Delaktivitet
Delaktivitet
Delaktivitet
Delaktivitet
Enkelte har egen utdypning
Utdypning

Lenke fra hovedaktivitet

(Utdrag fra hovedaktiviteten Risikohåndtering)

4 Iverksette godkjente tiltak

Ansvarlig for gjennomføring:

- Den person risikoeier eller systemeier fellessystem har pekt ut som håndteringsansvarlig, det vil si de som har fått i oppdrag å planlegge og følge opp den samlede gjennomføringen eller etableringen av et sett av godkjente tiltak. Ved enkle tiltak kan risikoeier selv være håndteringsansvarlig.

4.1 Om aktiviteten

Aktiviteten Iverksette godkjente tiltak utføres av en håndteringsansvarlig. Før oppstart skal tiltakene være godkjent av den risikoeieren som har ansvaret for risikovurderingene, og som har pekt ut håndteringsansvarlig.

Håndteringsansvarlig må først utforme en konkret handlingsplan for gjennomføring eller etablering av de godkjente tiltakene. Planen må oftest utformes i dialog med dem som skal gjennomføre aktivitetene. Planleggingen bør følge god praksis for prosjekt- og aktivitetsplanlegging generelt, og vektlegge tid, kost og forventet effekt av tiltakene.

Håndteringsansvarlig må avtale frister og hva som konkret skal gjøres, med dem som faktisk skal gjennomføre aktivitetene i handlingsplanen. Vi kaller dem tiltaksleverandører. Formalisering og detaljeringsnivå bør tilpasses

- tiltakenes viktighet
- omfang og kompleksitet på det som skal gjøres
- hvem som skal være ansvarlig
- hvordan virksomheten har organisert seg internt

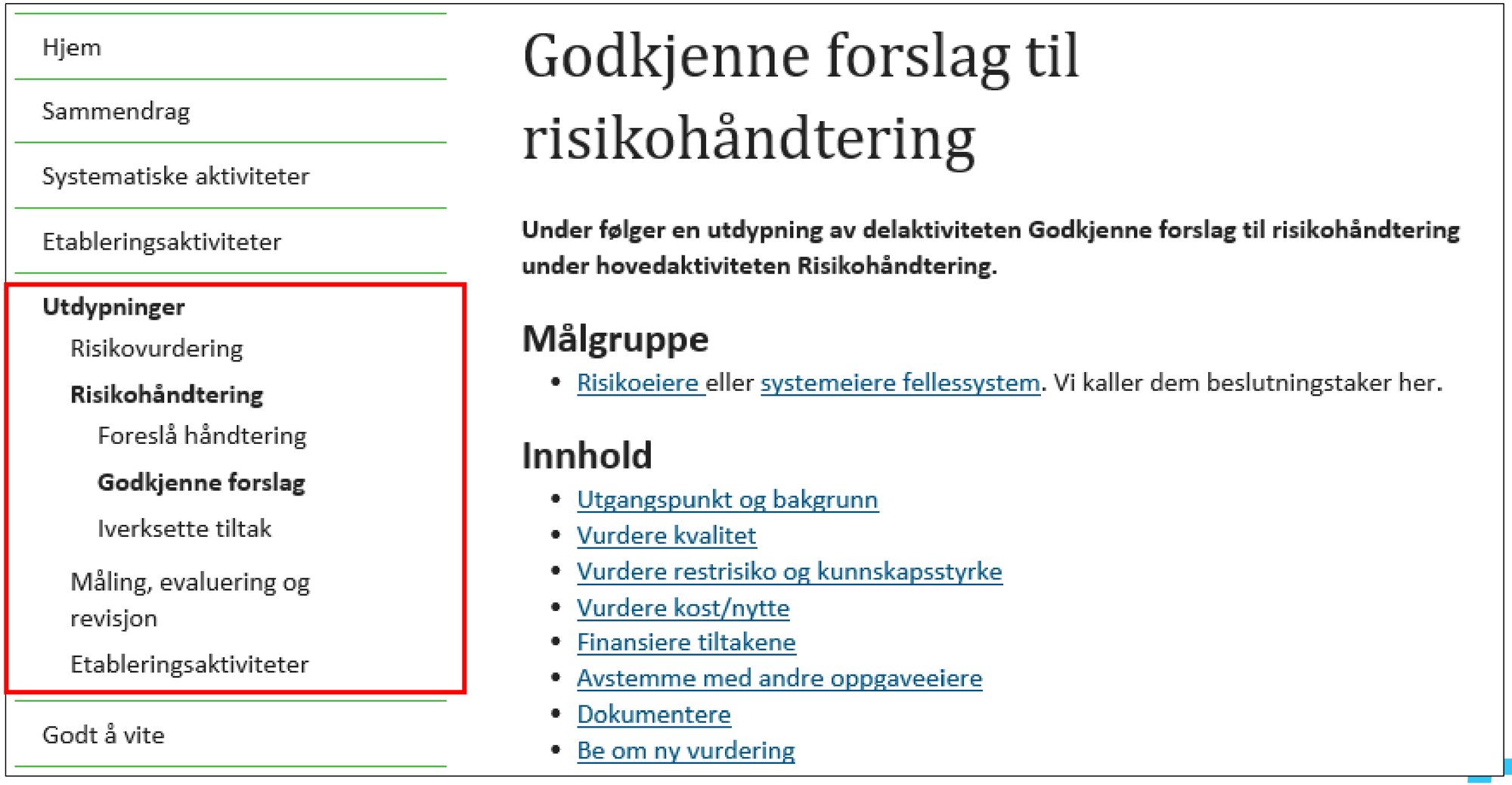
Håndteringsansvarliges handlingsplan bør godkjennes av risikoeier før den iverksettes. Håndteringsansvarlig bør systematisk følge opp fremdriften, og rapportere til risikoeier eller systemeier fellessystem som avtalt.

Utdypning:

- Delaktiviteten Iverksette godkjente tiltak er beskrevet mer detaljert i veiledningsmateriellets samling av utdypninger

*****

Utdypingssider ligger under eget menypunkt



Difi

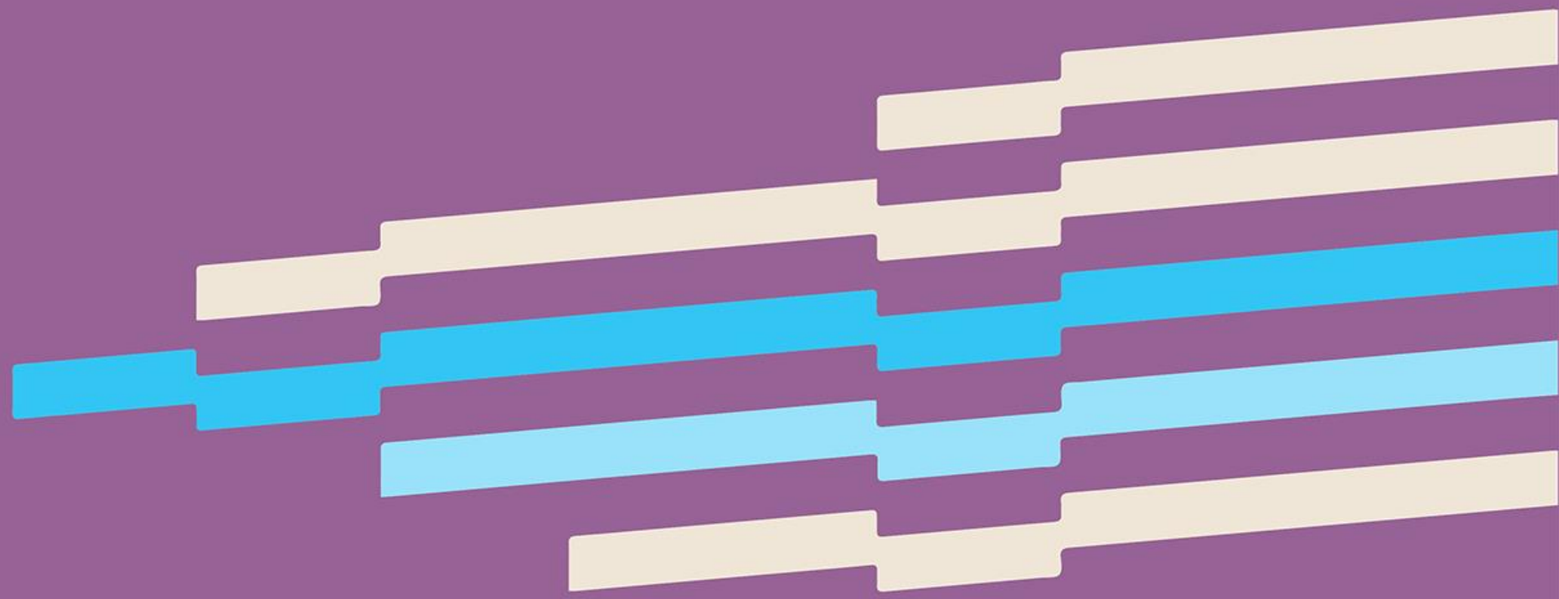
Difi
Direktoratet for
forvaltning og ikt

Økt 2
Internkontroll

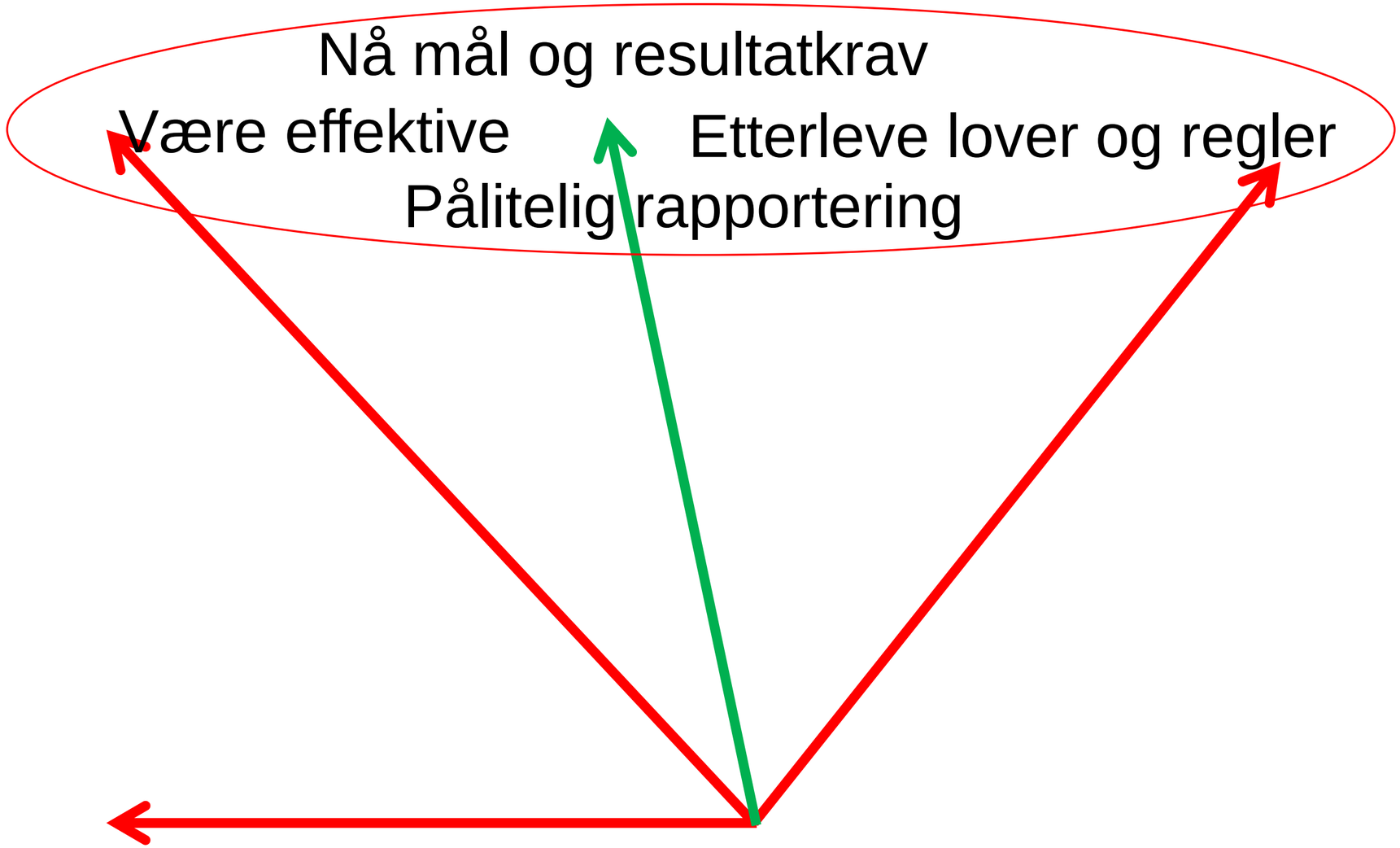
—

Innføringskurs

Internkontroll i praksis - informasjonssikkerhet

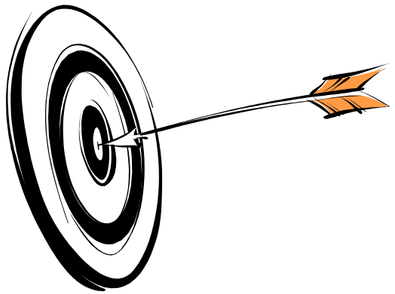


Hvorfor internkontroll?



Treffer eller bommer vi?

God internkontroll er



Målorientert

Risikobasert

Balansert

Internkontroll / Styringssystem / Ledelsessystem / ….

- Ulike begrep for det samme
- Det handler om

systematikk og formalisering

for å oppnå

tilstrekkelig

intern

styring og kontroll

slik at vi kan

nå målene våre

(nå mål og resultatkrav, være effektive
etterleve lover og regler, ha pålitelig
rapportering)

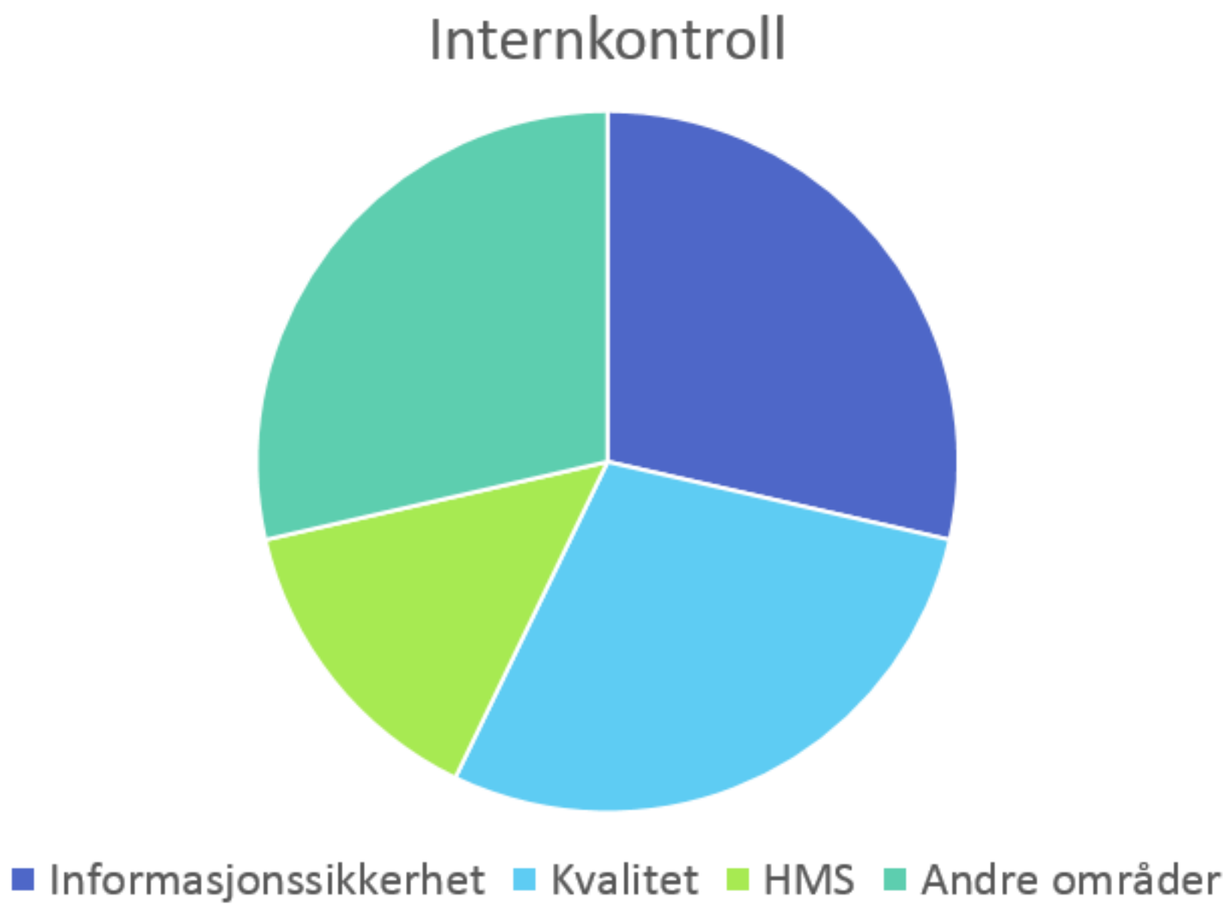
Difi

eForvaltningsforskriften § 15

- Forvaltningsorganet skal ha en *internkontroll (styring og kontroll)* på informasjonssikkerhetsområdet som *baserer seg på anerkjente standarder* for styringssystem for informasjonssikkerhet
- …internkontrollen skal *inkludere relevante krav* som er fastsatt i annen lov, forskrift eller instruks
- Internkontrollen bør være en *integrert del* av virksomhetens helhetlige styringssystem
- Omfang og innretning på internkontrollen skal være *tilpasset risiko*

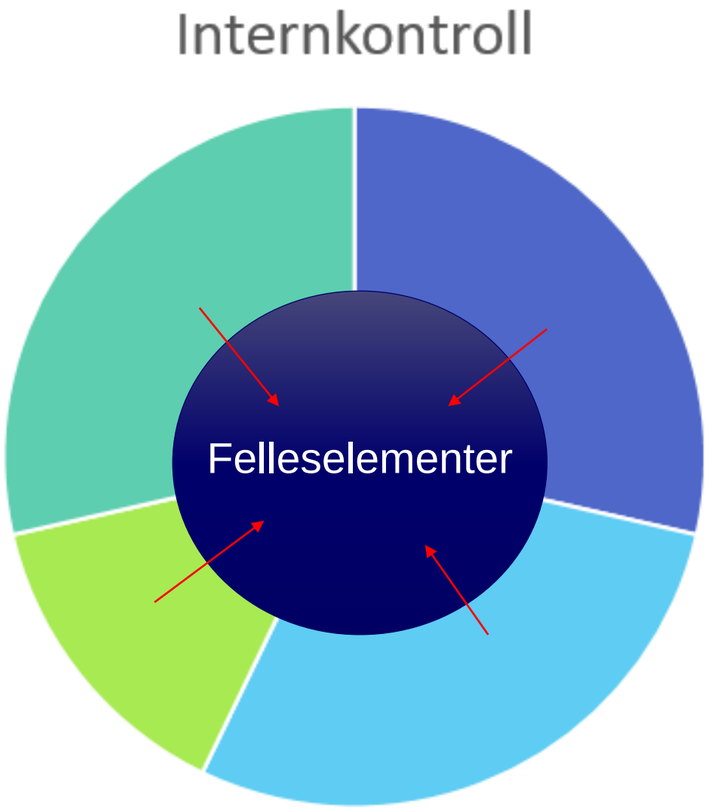
Difi

Internkontrollområder (eksempler)



Helhetlig internkontroll

Områdespesifikke deler



Omfang av integrering på tvers må tilpasses virksomheten

Difi

Flere har Identifisert «god praksis» for internkontroll (styring og kontroll) i ulike virksomheter

Rammeverk og standarder:

COSO

Internkontroll generelt

ISO

27001 9001 31000 m.m.

Mange områder

BS OHSAS 18001

HMS

++

Veiledninger (konkretiseringer):

Direktoratet for økonomistyring

KS

difi Direktoratet for forvaltning og IKT

Datatilsynet

NSM

dsb Direktoratet for samfunnssikkerhet og beredskap

Arbeidstilsynet Kontroll og veiledning om arbeidsmiljø

Helsedirektoratet

Normen

++

Nødvendig:

Lokal samordning og tilpasning til den enkelte virksomhet sin egenart og historie

Resultat:

God internkontroll i **vår** virksomhet med kontinuerlig forbedring

Difi

Standarden ISO/IEC 27001 og Difis veiledningsmateriell

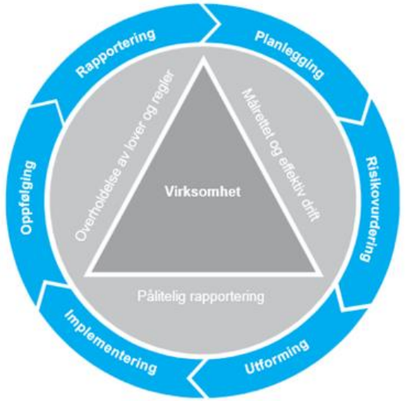
- ISO/IEC 27001
  - er anbefalt standard å basere seg på
    - stiller overordnede krav til
      - hva man skal ha og hva man skal gjøre
        i et sertifisert «system» for styring og kontroll innen informasjonssikkerhet

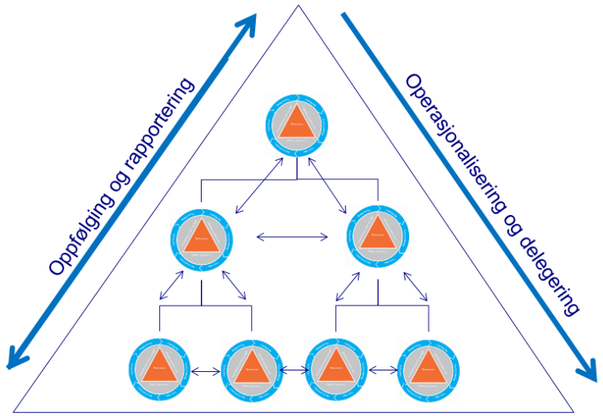
- Difis veiledningsmateriell
  - har en pragmatisk og behovsorientert tilnærming til standarden
    - fokus på tilstrekkelig styring og kontroll (ikke sertifisering)
    - baserer seg på standarden
    - dekker det Difi anser som de viktigste kravene
  - konkretiserer hvordan disse kravene kan implementeres og etterleves

Difi

Ulike forklaringsmodeller

DFØ – Staten
Internkontroll generelt





Difi – Stat og kommune
Informasjonssikkerhet

KS – Kommunene
Internkontroll generelt

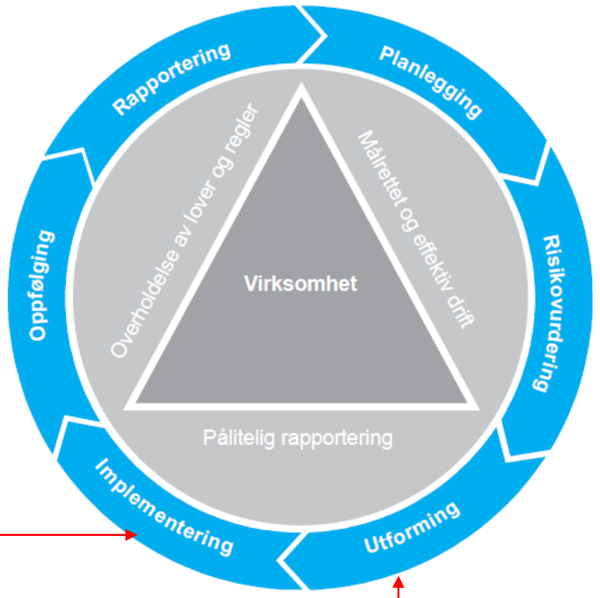
Difi

Difis forklaringsmodell

Difi vs DFØ veiledningsmateriell

Difis «forklaringsmodell» – internkontroll informasjonssikkerhet

DFØs «metode» – internkontroll generelt



Difi

Samordning og tilpasning…

- … i den enkelte virksomhet
- Må gjøres ut fra egen status og utgangspunkt på ulike internkontrollområder.
- Gjenbruk på tvers der det er hensiktsmessig
- Tilpass til etablert praksis i virksomheten – dersom det gir tilstrekkelig styring og kontroll

Difi
Direktoratet for
forvaltning og ikt

Økt 3
Internkontroll Informasjonssikkerhet

—

Innføringskurs

Internkontroll i praksis -
informasjonssikkerhet

Hva er informasjonssikkerhet?

Sikre:

- konfidensialitet
- integritet
- tilgjengelighet

på informasjon som behandles

i tilknytning til våre arbeidsoppgaver

Difi

Hva er informasjonssikkerhet?

- Konfidensialitet
  - Informasjon blir ikke kjent for uvedkommende
- Integritet
  - Informasjon blir ikke endret utilsiktet eller av uvedkommende
- Tilgjengelighet
  - Informasjon er tilgjengelig ved behov

Difi

AKTIVITETER I INTERNKONTROLLARBEIDET

Difis forklaringsmodell

Viktige aktører

- Virksomhetsledelsen
- Ledere som delegerer og skal følge opp

- Risikoeiere
- Systemeiere fellessystem
- Tiltaksleverandører

- Utpekt person som lederstøtte og pådriver
  - innen internkontroll informasjonssikkerhet
  - Fagansvarlig informasjonssikkerhet
- Støttepersoner
  - prosessledere for risikovurderinger m.fl.

Etablering | Systematisk

Etableringsaktiviteter

- Analysere status
- Planlegge etablering | forbedring

- Hjelpeaktiviteter for å lette de systematiske aktivitetene

Systematiske aktiviteter

Ledelsens styring og oppfølging

- Virksomhetsledelsens gjennomgang
  - Minimum en gang årlig

- Ledere på alle nivå
  - Delegere og følge opp gjennom linjen
  - Sikre finansielle rammer
  - Kommunisere viktighet
  - Løfte og håndtere problemstillinger gjennom linjen
  - Beredskap og krisehåndtering

Risikovurdering

- Få oversikt og prioritere
- Analysere eksterne krav
- Planlegge og gjennomføre risikovurderinger

Risikohåndtering

- Risikoeiere og systemeiere fellessystem:
  - Foreslå håndtering av risikoer
  - Godkjenne forslag til håndtering
  - Iverksette godkjente tiltak

- Tiltaksleverandører:
  - Utforme og implementere tiltakene
  - Oppdatere fellessikring og tilleggssikring

Difi

Overvåking og hendelseshåndtering

- Tiltaksleverandører:
  - Overvåke i henhold til avtale
- Alle ansatte:
  - Rapportere hendelser, avvik og informasjonssikkerhetsbrudd
- Ulike aktører ur fra ansvar:
  - Følge opp hendelser, avvik og informasjonssikkerhetsbrudd

Måling, evaluering og revisjon

- Ledere på alle nivå:
  - Vurdere status på eget ansvarsområde
- Ut fra ledelsens behov:
  - Måle definerte indikatorer
  - Evalueringer
  - Internrevisjon

Kompetanse- og kulturutvikling

- Ledere på alle nivå:
  - Identifisere og følge opp behov for kompetanse- og kulturutvikling
- Fagansvarlig informasjonssikkerhet:
  - Følge opp lokale sikkerhetskoordinatorer

Kommunikasjon

- Formidle nye føringer
- Dokumentere
  - gjennomførte aktiviteter
  - etterlevelse av tiltak
- Årlige rapporter og notat
  - Statusrapporter som grunnlag for risikovurderinger
  - Saksnotat til virksomhetsledelsens gjennomgang
- Kommunikasjon mellom delaktiviteter og aktører
- Ekstern kommunikasjon

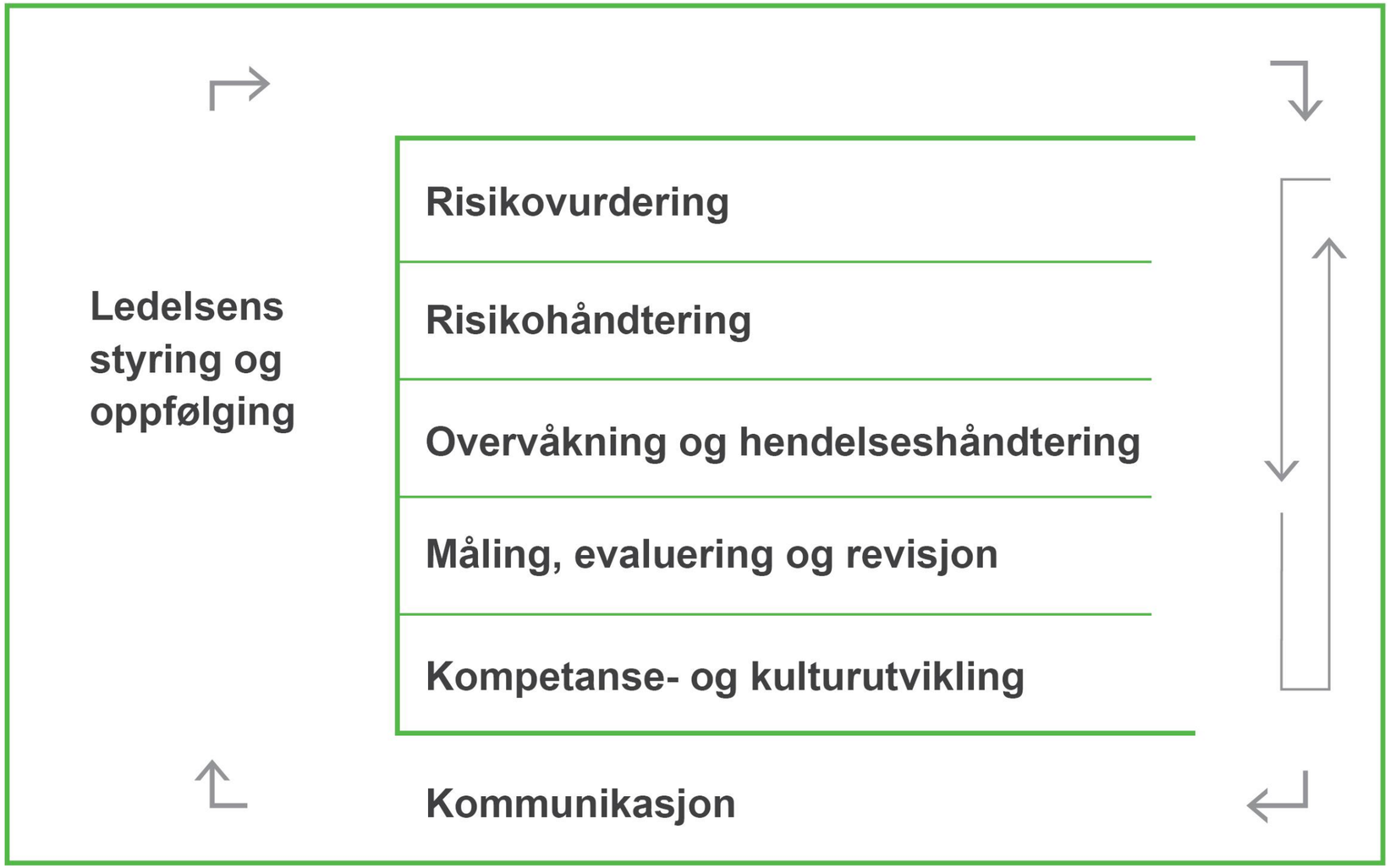
Internkontroll i praksis - informasjonssikkerhet

Ledelsens styring og oppfølging

- Risikovurdering
- Risikohåndtering
- Overvåking og hendelseshåndtering
- Måling, evaluering og revisjon
- Kompetanse- og kulturutvikling

Kommunikasjon

Difi


Ledelsens styring og oppfølging
Risikovurdering
Risikohåndtering
Overvåkning og hendelseshåndtering
Måling, evaluering og revisjon
Kompetanse- og kulturutvikling
Kommunikasjon

Difi

- Instrukser og rutiner
- Avtaler
- Retningslinje for fysisk sikkerhet
- Tilgangsstyring IT-systemer
- Sikkerhetskopiering og gjenoppretting
- Osv osv osv

Tilleggssikring

Fellessikring

Difi

«Styringstiltak»

«Sikkerhetsstiltak»

Tilleggssikring

Fellessikring

Difi

«Styringstiltak»

- ISO 27001

«Sikkerhetsstiltak»

Tiltaksbanker

- ISO 27002 | Annex A (i ISO 27001)
- «Normen» kap. 5 + faktaark
- NIST SP 800-53
- SoGP
- NSM anbefalinger
- Osv osv osv

«Styringstiltak»

«Sikkerhetsstiltak»

Tiltaksbanker

- ISO 27002 | Annex A (i ISO 27001)
- «Normen» kap. 5 + faktaark
- NIST SP 800-53
- SoGP
- NSM anbefalinger
- Osv osv osv

Difi

1

- **Analysere** status
- **Planlegge** etablering/forbedring
- Gjennomføre andre **etableringsaktiviteter**

Gjennomføre aktivitetene systematisk

2

Internkontroll-aktiviteter

1

- **Analysere** status
- **Planlegge** etablering/forbedring
- Gjennomføre andre **etableringsaktiviteter**

Internkontroll-aktiviteter

Gjennomføre aktivitetene systematisk

2

Sikkerhetstiltak

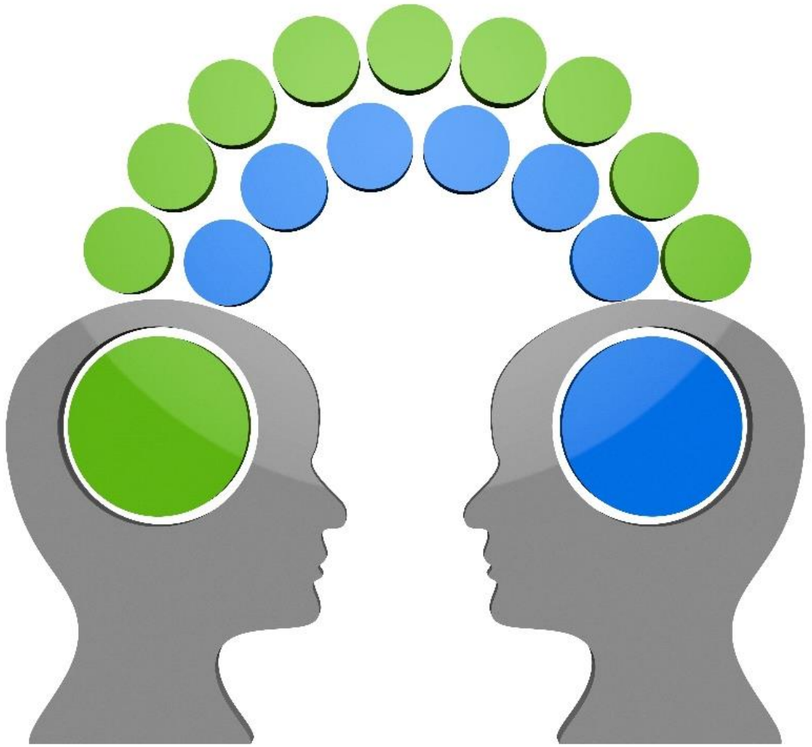
3

Tilleggssikring

Fellessikring

- Instrukser og rutiner
- Avtaler
- Retningslinje for fysisk sikkerhet
- Tilgangsstyring IT-systemer
- Sikkerhetskopiering og gjenoppretting
- Osv.

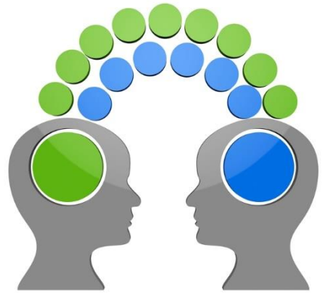
Difi



REFLEKSJONSOPPGAVE

Difi

Refleksjonsoppgave 1



Diskuter noen av punktene under:

- Hvor er deres virksomhet med hensyn til **informasjonssikkerhet** og
  - forståelse av sentrale begreper
  - forankring av informasjonssikkerhetsarbeidet i internkontrollmålene:
    - nå mål og resultatkrav
    - være effektive
    - etterleve lover og regler
    - pålitelig rapportering
  - fokus på informasjonsbehandling og arbeidsoppgaver (arbeidsprosesser)
  - reell topplederstyring
  - systematisk arbeid i hele virksomheten

- Hva er vanskelig å få til hos dere?

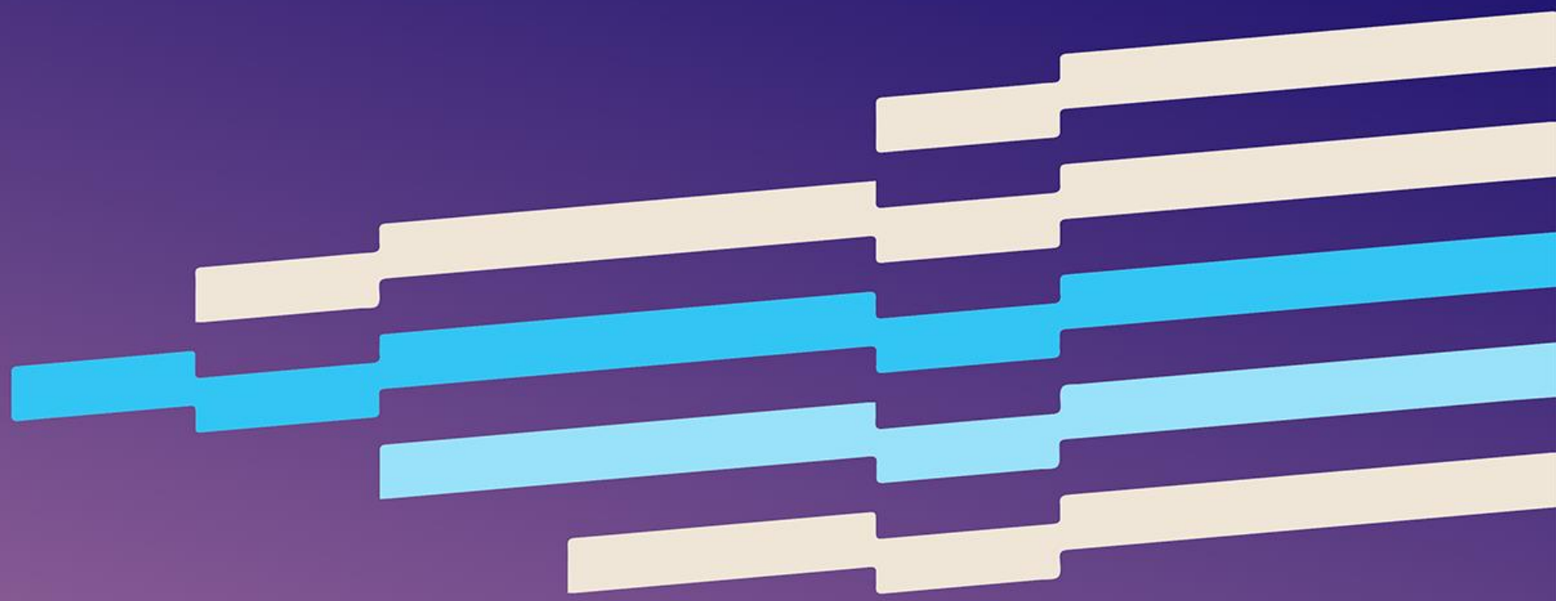
Difi

Difi
Direktoratet for forvaltning og ikt

Økt 4
Begrep og roller

Innføringskurs

Internkontroll i praksis - informasjonssikkerhet



Hva er informasjonssikkerhet?

Sikre:

- konfidensialitet
- integritet
- tilgjengelighet

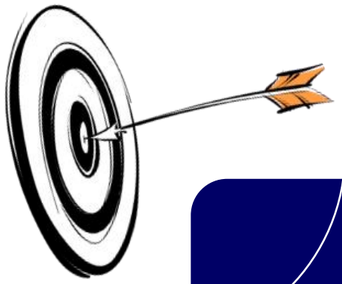
på informasjon som behandles

i tilknytning til våre arbeidsoppgaver

Difi

Arbeidsoppgaver

Informasjonsbehandling



Mål og resultater
Være effektive
Etterleve lover og regler

Informasjonsbehandling

INFORMASJONSSIKKERHET
KONFIDENSIALITET
INTEGRITET
TILGJENGELIGHET
INFOSIKKERHET.DIFI.NO

Informasjonssikkerhet

Difi

Systematiske aktiviteter

SENTRALE ROLLER

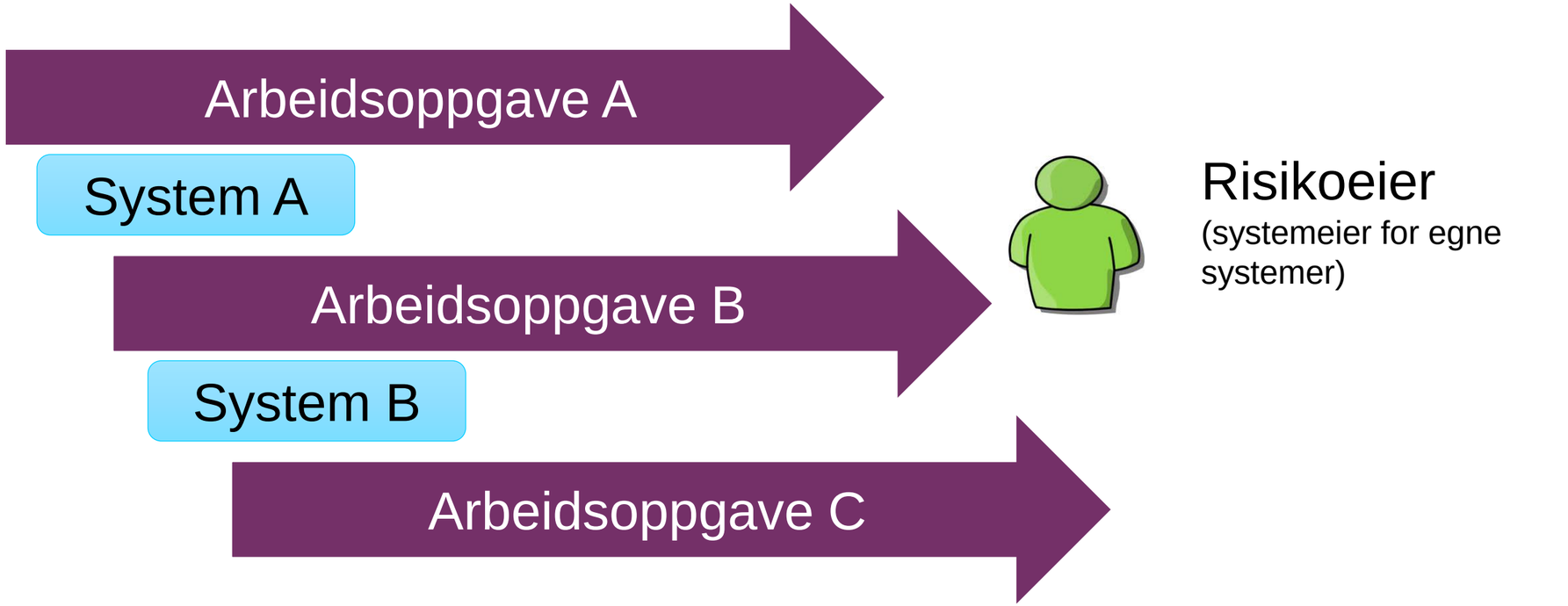
Difi

Virksomhetsledelsen – viktige oppgaver

- Få gjennomført etableringsaktiviteter
  - Gi føringer for organisering, systematiske aktiviteter mv.
- Tilføre nødvendige ressurser
- Følge opp at de systematiske aktivitetene blir gjennomført
- Følge opp at ting fungerer som forutsatt
- Gjøre endringer ved behov

Risikoeier

- Ansvarlig for mål og resultater
- Oppgaveeier eller prosesseier
- Typisk: operativ linjeleder



Risikoeier
(systemeier for egne systemer)

Fellessystem 1

Fellessystem 2

Systemeier fellessystem

Difi

Tiltaksleverandør

- Ansvarlig for sikkerhetstiltak

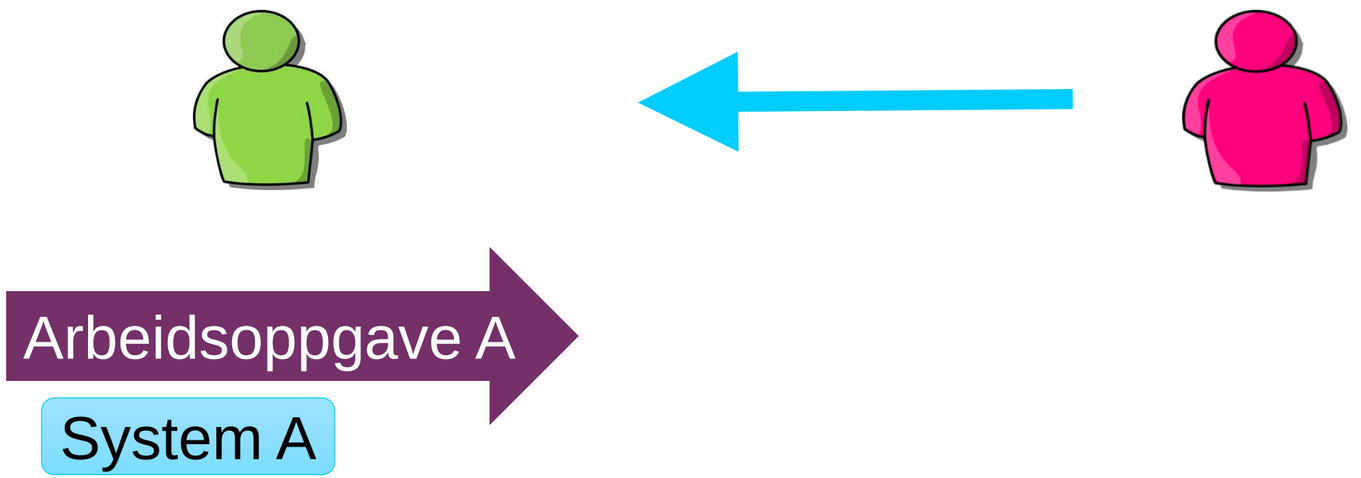
- Utformer, implementerer og vedlikeholder
- Rapporterer status på sikkerhetstiltak
- Informerer risikoeiere om endringer som påvirker risiko

Risikoeier

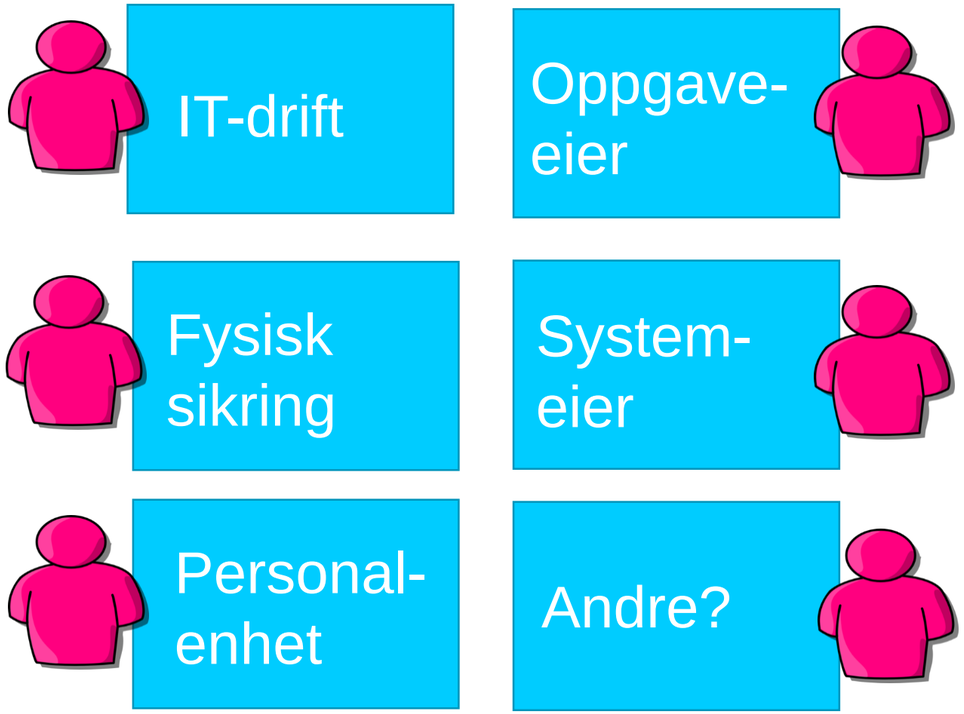
- Vurderer risiko
- Har behov

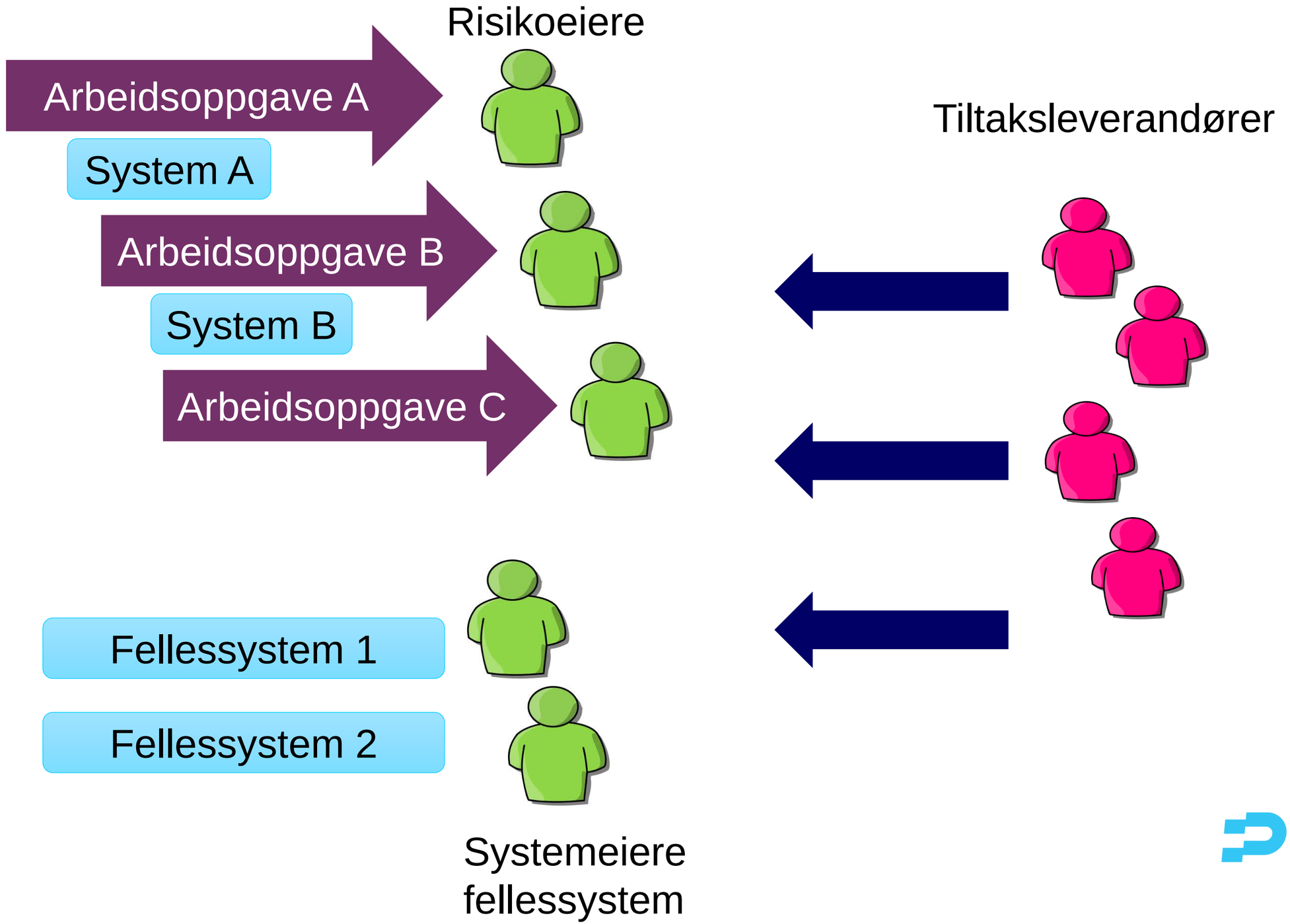
Tiltaksleverandør

- Har fagekspertise
- Tilbyr sikkerhetstiltak

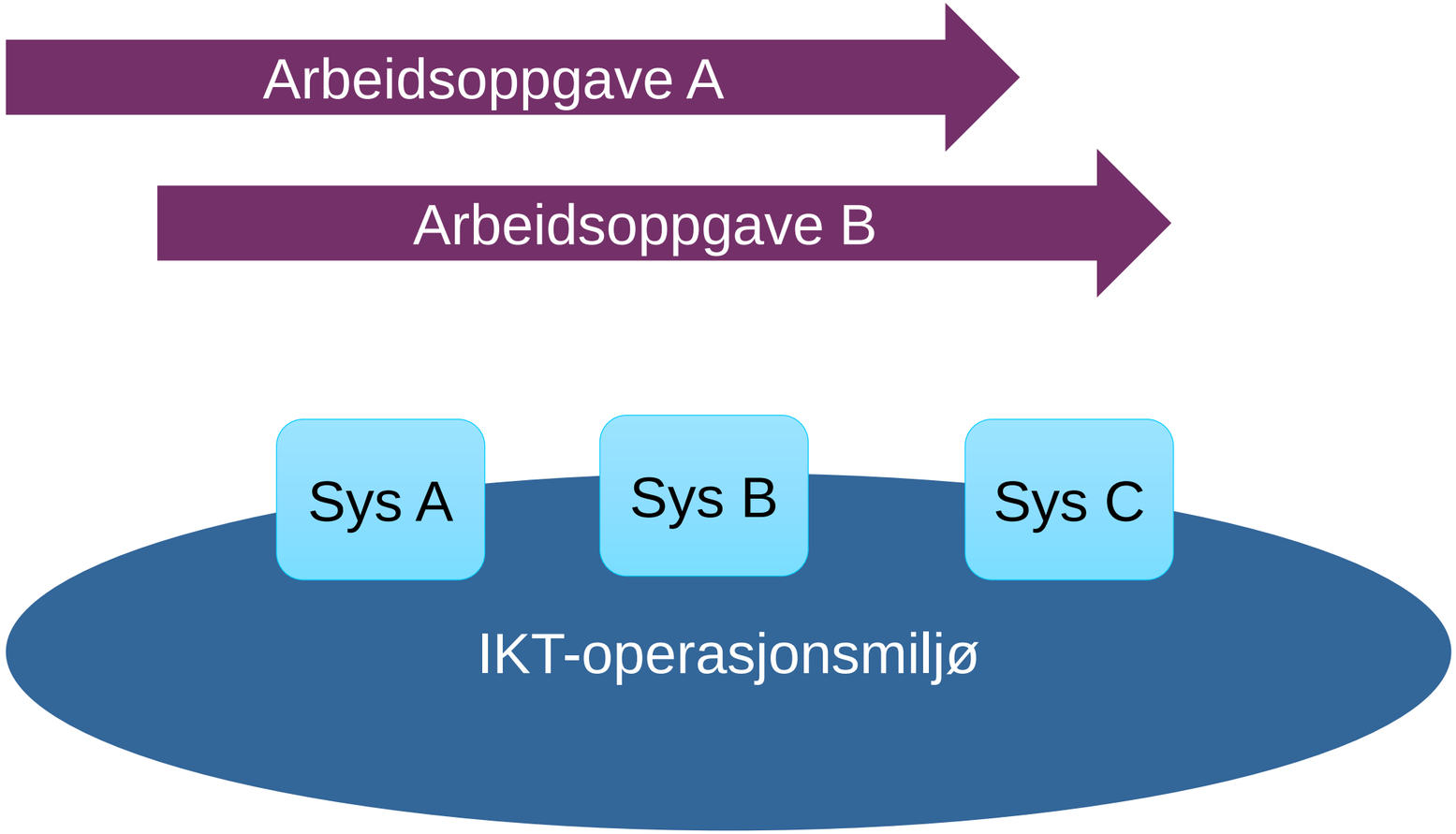


Tiltaksleverandører




Risikoeiere
Arbeidsoppgave A
System A
Arbeidsoppgave B
System B
Arbeidsoppgave C
Tiltaksleverandører
Fellessystem 1
Fellessystem 2
Systemeiere fellessystem

IKT-drift – en sentral tiltaksleverandør



STØTTE TIL LEDELSEN

Fagansvarlig informasjonssikkerhet

- Spesialfunksjon
- Den som har hovedansvaret for å støtte ledelsen i arbeidet med informasjonssikkerhet
- Tilrettelegge for god gjennomføring av internkontrollarbeidet
- Andre ofte brukte titler:
  - Informasjonssikkerhetsansvarlig
  - Informasjonssikkerhetsleder
  - CISO

Lokale Sikkerhetskoordinatorer

- Anbefaler lokale «pådrivere» for informasjonssikkerhet
  - Pr. avdeling eller tilsvarende org-enhet
- Støtte ledelsen og ansatte lokalt

- Funksjon som kan legges til en ordinær fagstilling
  - Motivasjon
  - Personlig egnethet

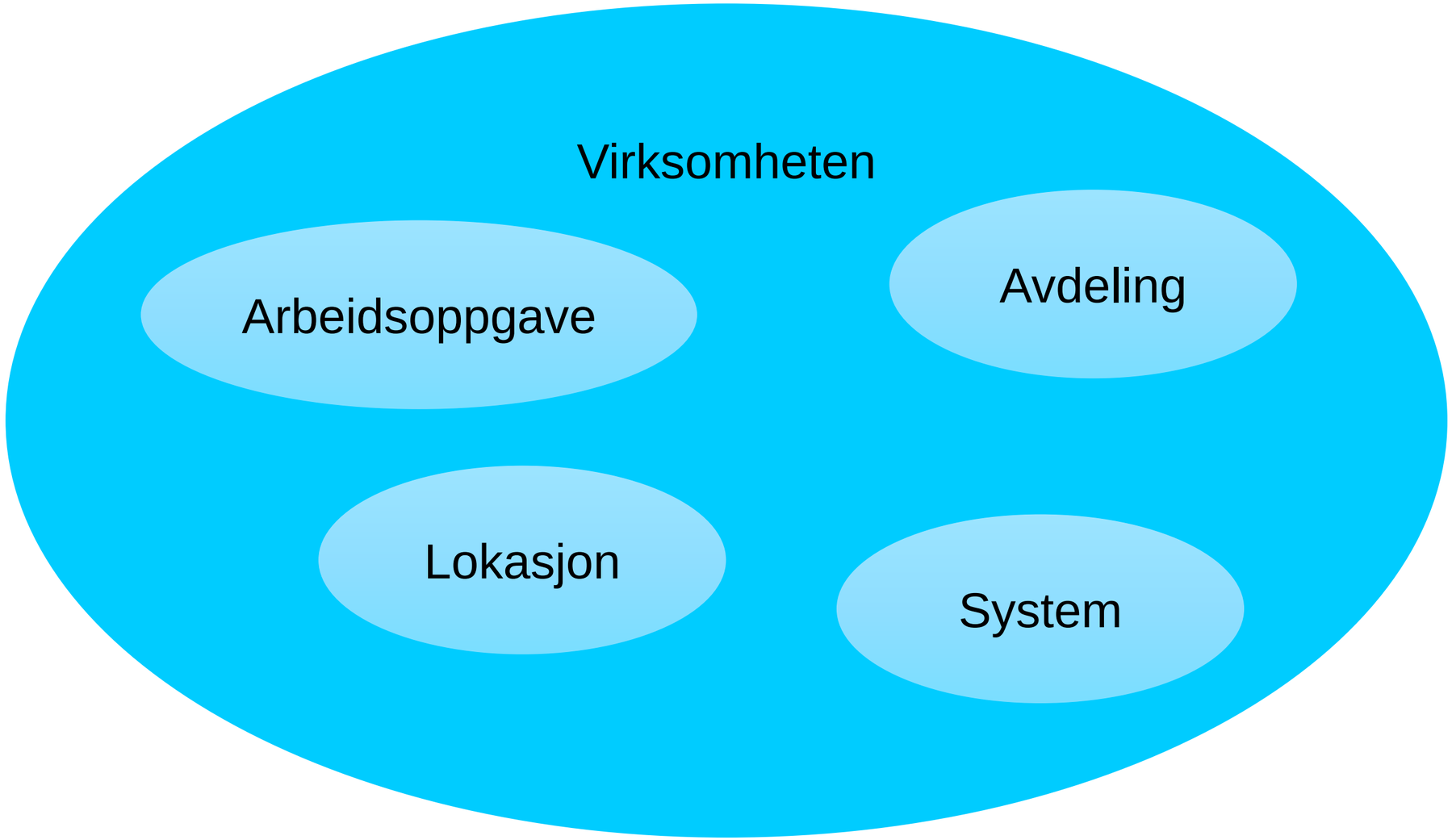
SIKKERHETSTILTAK

Sikkerhetstiltak

- Control: a measure that is modifying risk
- Formål
  - Forebygge
  - Oppdage
  - Reagere
- Typer
  - Organisatoriske tiltak
  - Menneskelige tiltak
  - Tekniske tiltak

Difi

Virkeområde



Tiltaksbanker

- Tips
- Inspirasjon
- Kategorisering | Sortering

- Felles referanse

Foto: Fabian Blank unsplash.com

Tiltaksbanker - eksempler

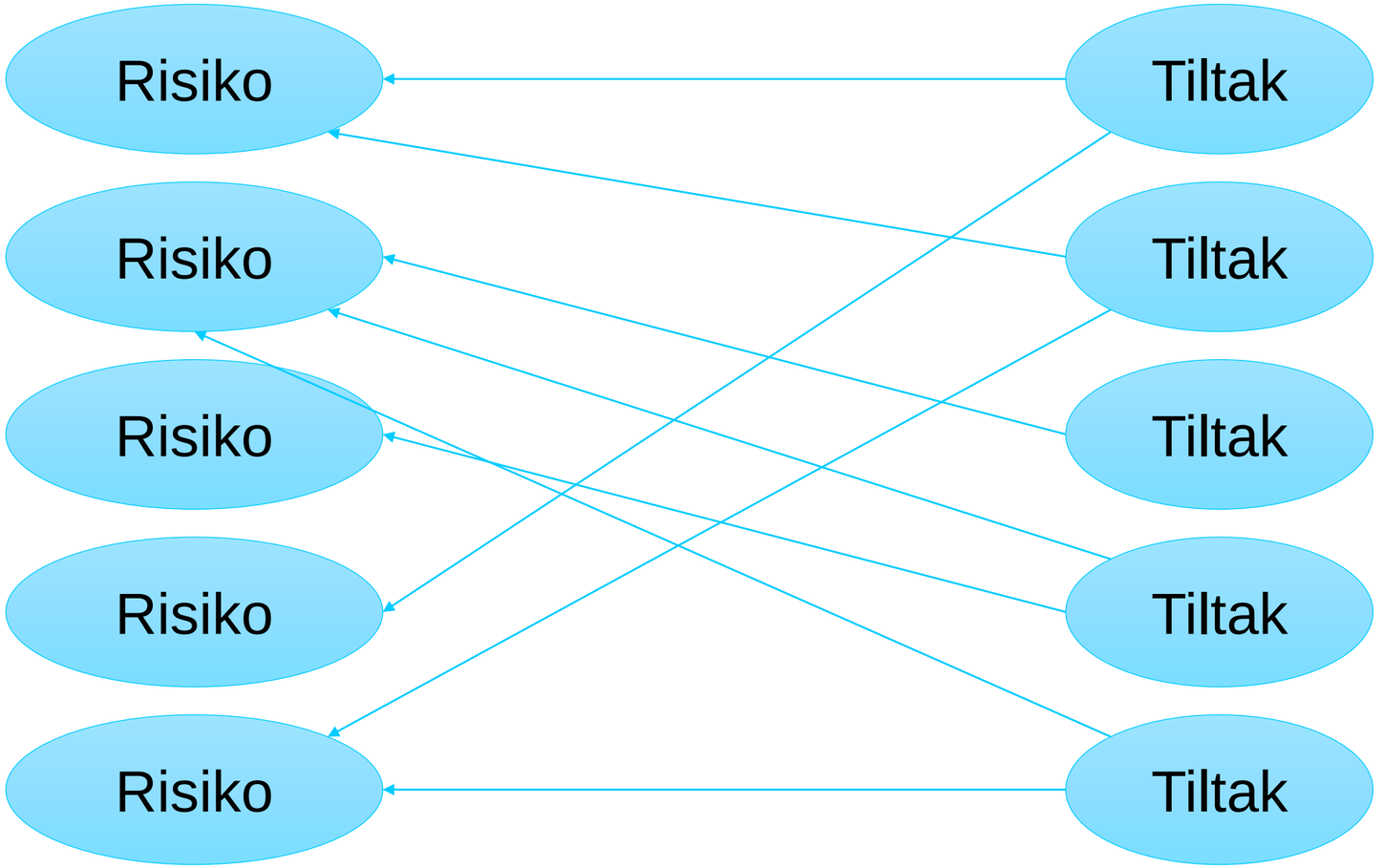
- ISO/IEC 27002:2013
- «Normen»
  - Kap 5 – Gjennomførende del
  - Faktaark
- NSMs Grunnprinsipper for IKT-sikkerhet
- NIST SP 800-53 rev4
  - Appendix F – Security Control Catalog
  - Appendix G – Information Security Programs
- ISF – Standard of Good Practice
  - Control Framework
- Og andre…

Difi

Brukerkrav er sikkerhetstiltak

- Autentisering
- Adgangskontroll
- Hendelseshåndtering
- Osv.

Difi


Risiko
Risiko
Risiko
Risiko
Risiko
Tiltak
Tiltak
Tiltak
Tiltak
Tiltak

Fellessikring

Fellessikring

- Et sett med sikkerhetstiltak
- Et felles grunnleggende sikkerhetsnivå for sentrale områder i virksomheten

Fellessikring gir…

- Felles forståelse av hvilken grunnleggende sikkerhet som er etablert i virksomheten
- Trygghet for at informasjonsbehandling har et visst grunnleggende nivå av sikkerhet
- Oversikt over sikkerhetstiltak på sentrale områder
- En grunnmur som ekstra sikkerhetstiltak kan bygges på der det er spesielle behov

Difi

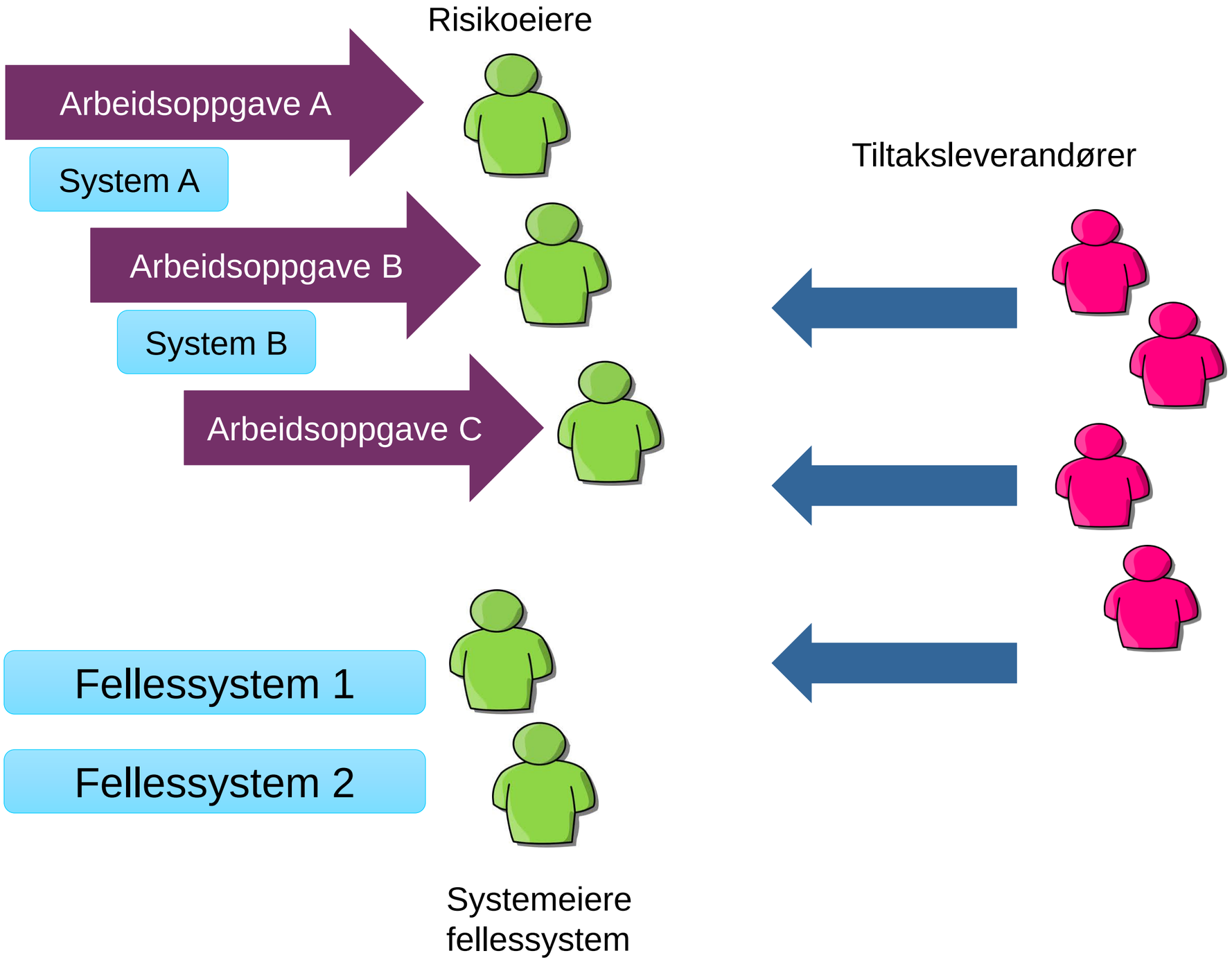
Arbeidsoppgave A

System A

Tilleggssikring

Fellessikring

Difi


Risikoeiere
Arbeidsoppgave A
System A
Arbeidsoppgave B
System B
Arbeidsoppgave C
Tiltaksleverandører
Fellessystem 1
Fellessystem 2
Systemeiere
fellessystem

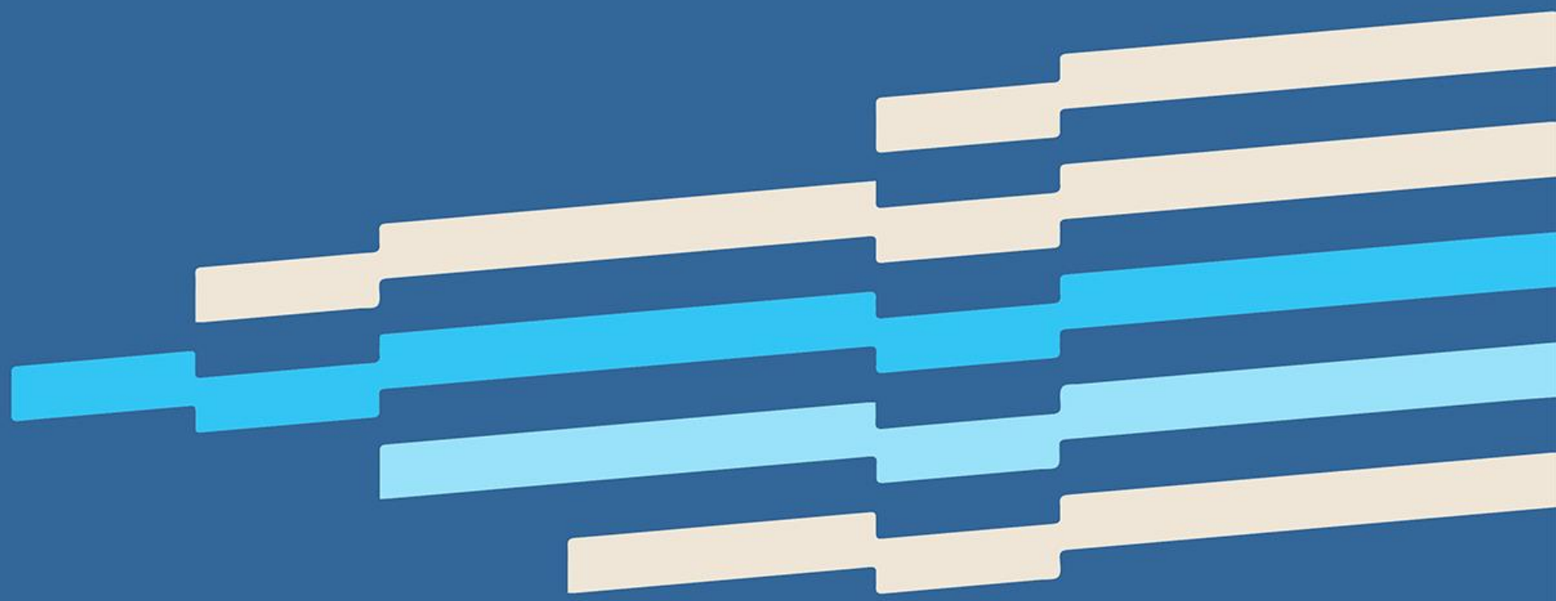
Difi
Direktoratet for
forvaltning og ikt

Økt 5
Risikoforståelse

—

Innføringskurs

Internkontroll i praksis -
informasjonssikkerhet



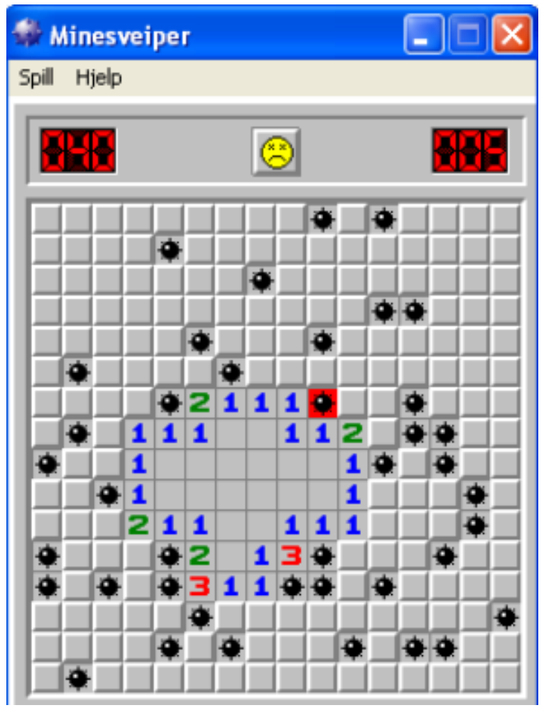
Kjernen i internkontrollarbeidet

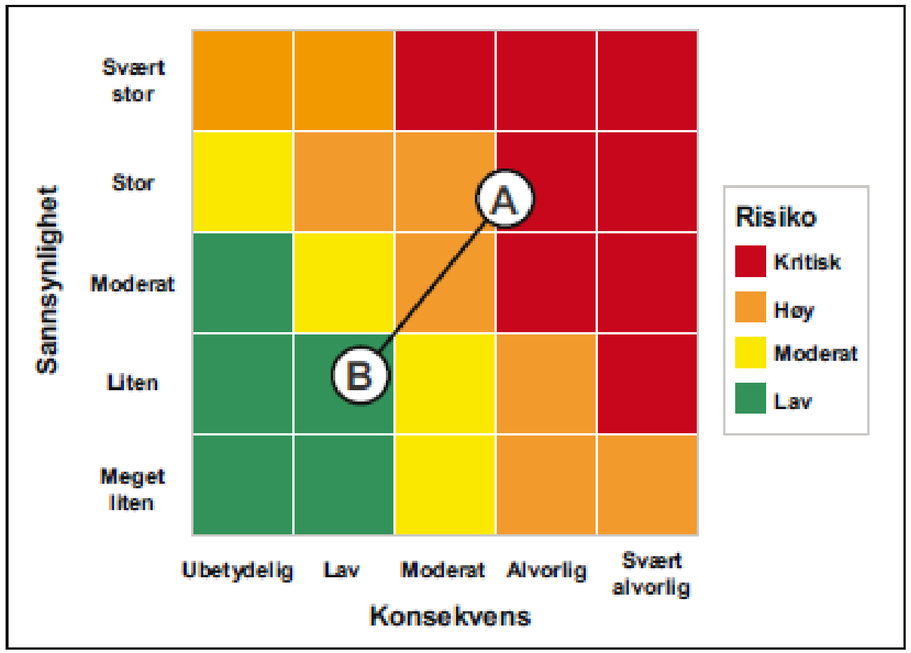
Etablere tillit til at virksomheten har tilfredsstillende identifisering og oppfølging av risikoene

Slik at vi kan nå målene våre

Difi

Hva er dette?



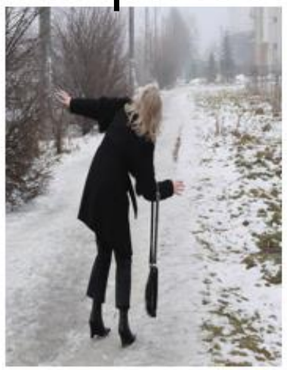


Difi

HVA ER RISIKO?

Difi

Sklir på isen



Liv og helse

Øko-nomi

Tjeneste-nivå

? ?

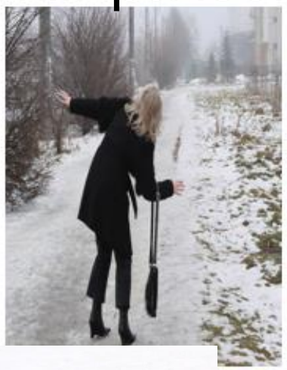
Difi

Uønsket hendelse | Risikobeskrivelse | Scenario

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

Liv og helse | Øko-nomi | Tjeneste-nivå

Sklir på isen



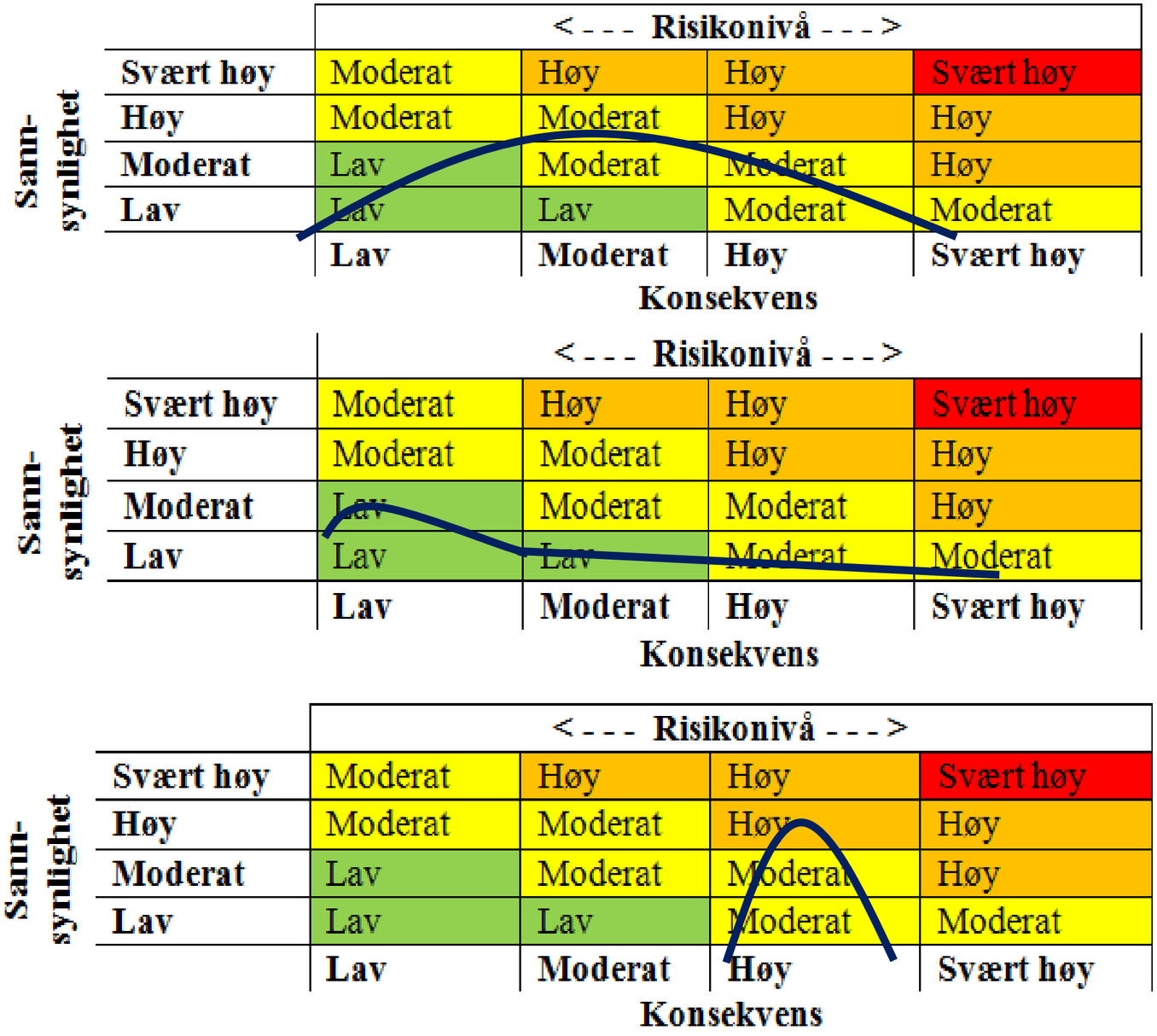
? ?

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

Difi

Sannsynlighetsfordeling på ulike konsekvensnivå

Avhengig av risikobeskrivelsen



Hva er risiko for en virksomhet?

Utgangspunktet er

Våre mål

- Nå mål og resultatkrav
- Ha effektiv ressursbruk
- Etterleve lover og regler
- Pålitelig rapportering

Risiko

- å kanskje ikke nå disse målene
- uttrykkes:
  - potensielt resultat og tilhørende usikkerhet (sannsynlighet)

  eller

  - (mulig) konsekvens og (tilhørende) sannsynlighet
    - av uønsket hendelser
    - som kan medføre

Difi

Viktige sammenhenger (1)

- Risiko blir til vanlig brukt i tilknytning til uønskede hendelser, som kan få konsekvenser
- Konsekvensene er avvik fra mål eller fra ønskede resultat eller tilstander
- Selve risikoen er kombinasjonen av mulige konsekvenser og tilhørende sannsynligheter
- En uønsket hendelse kan ha mange alternative konsekvenser med ulik sannsynlighet

Difi

Viktige sammenhenger (2)

- Anslaget av sannsynlighet må dekke hele hendelsesforløpet, inklusiv at den aktuelle konsekvensen faktisk blir utfallet av hendelsen

- Innen informasjonssikkerhet er ett eller flere informasjonssikkerhetsbrudd en del av den uønskede hendelsen
  - brudd på konfidensialitet, integritet eller tilgjengelighet

- Uønskede hendelser kan omfatte ulykker, uhell, uaktsomhet og tilsiktede handlinger

Difi

Potensielle konsekvenser ved brudd på informasjonssikkerheten

Vår egen jobb

- feil beslutninger
- brudd på rettssikkerhet
- feil i øk. transaksjoner
- ikke korrekt og forsvarlig saksbehandling
- økonomiske tap
- ineffektivt arbeid
- tapt arbeidstid
- …

Personer og virksomheter

- tap av anseelse, integritet og rettigheter
- økonomiske tap
- ødelagte muligheter, arbeidsforhold, livssituasjon og eksistensgrunnlag
- bedriftshemmeligheter
- rikets sikkerhet
- liv og helse
- ikke korrekt og forsvarlig saksbehandling
- …

Difi

Risikovurderinger kan skje på flere organisatoriske nivå

- Strategisk
- Taktisk
- Operativt | operasjonelt

*****

Innen informasjonssikkerhet:
Fokus på operative risikoer – det som kan skje
i tilknytning til utføring av arbeidsoppgavene våre

Risikovurderinger

Mål og konsekvenskategorier

Utgangspunkt i mål

- Mål 1
  - Risiko 1
  - Risiko 2
  - Risiko 3
  - …
- Mål 2
  - Risiko 1
  - Risiko 3
  - Risiko 5
  - …

Utgangspunkt i ansvarsområder/ arbeidsoppgaver

- Risiko 1
  - kan påvirke mål / målområde 1
  - kan påvirke mål / målområde 2
- Risiko 2
  - kan påvirke mål / målområde 2
  - kan påvirke mål / målområde 3
- …

NB! målene/målområdene blir ofte kalt konsekvenskategorier e.l.

Operative risikoer og mål/konsekvenskategorier har ofte et mange til mange forhold

Difi

Formål med risikovurdering

- Identifisere risikoer som må håndteres
  - Det avgjørende er
    - risikostørrelse og
    - kriterier for å akseptere risiko

- Kommunisere risiko
  - til ledere og andre

For å få effektive risikovurderinger og effektiv risikokommunikasjon benytter vi ofte

FORENKLINGER

Konsekvenskategorier

- Er en forenkling og gruppering av våre mål med basis i
  - Nå mål og resultatkrav
  - Ha effektiv ressursbruk
  - Etterleve lover og regler
  - Pålitelig rapportering

Eksempel på konsekvenskategorier
Tjenestenivå
Personvern
HMS
Regelverk (for øvrig)
Vår økonomi
Delmål

Difi

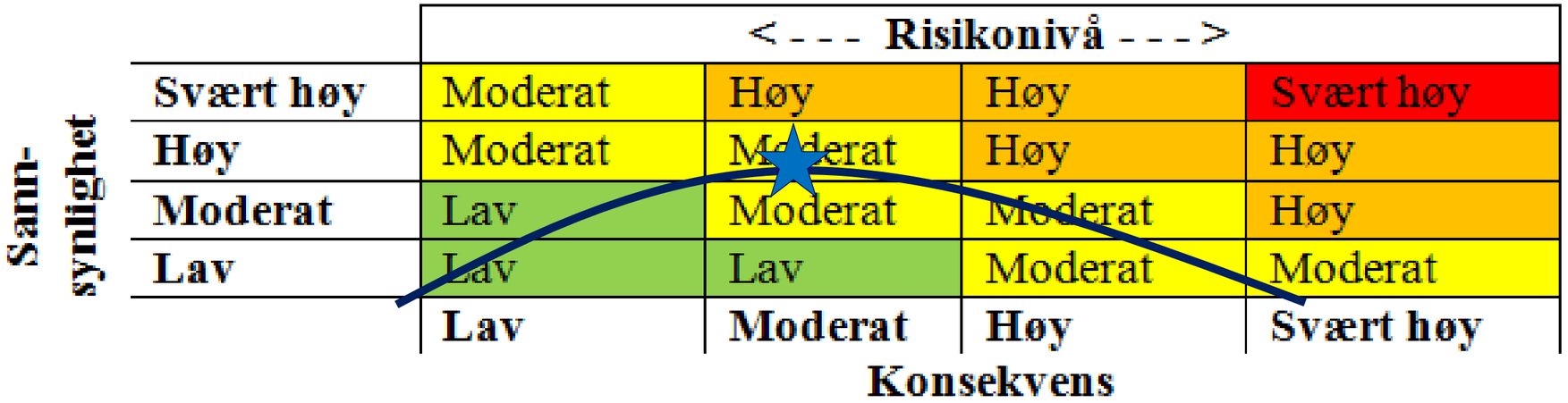
Nivåinndeling på konsekvens, sannsynlighet og risiko

- Er en forenkling for å effektivisere risikovurderinger og kommunikasjon om risiko
  - Vi deler det samlede utfallsrommet opp i ruter og nivå

Sann-synlighet	< - - - Risikonivå - - - >			
Svært høy	Moderat	Høy	Høy	Svært høy
Høy	Moderat	Moderat	Høy	Høy
Moderat	Lav	Moderat	Moderat	Høy
Lav	Lav	Lav	Moderat	Moderat
	Lav	**Moderat**	**Høy**	**Svært høy**
		Konsekvens		

Nivåinndeling på konsekvens, sannsynlighet og risiko

- Er en forenkling for å effektivisere risikovurderinger og kommunikasjon om risiko
  - Vi deler det samlede utfallsrommet opp i ruter og nivå

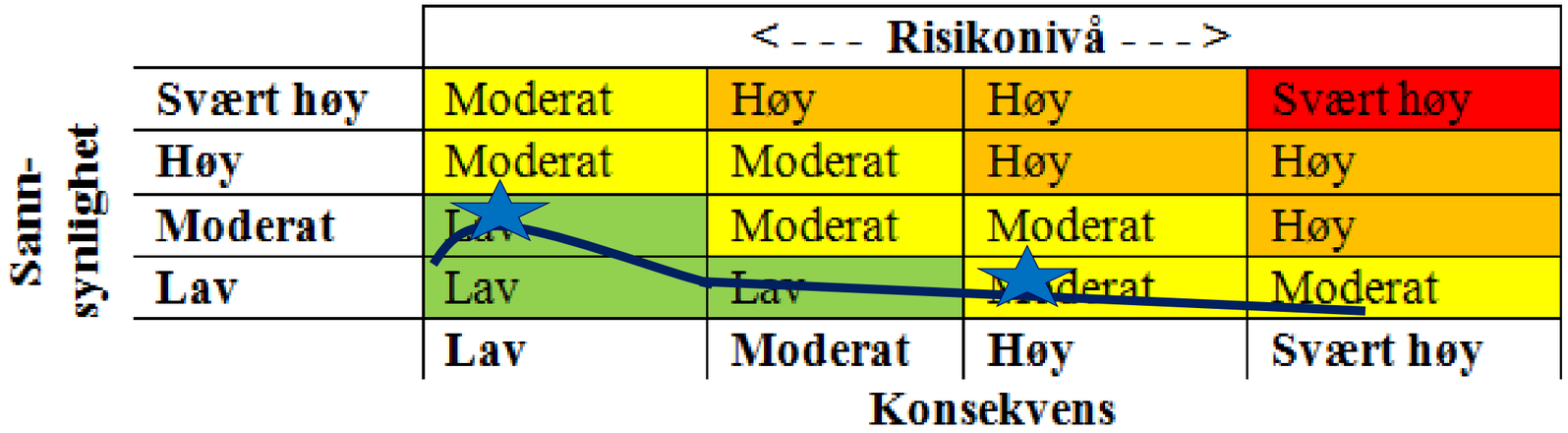


- Vi uttrykker ett av flere mulige utfall /risikoer
  - oftest det mest forventede
  - Selv om risikoene ligger i hele utfallsrommet (under buen)

Difi

Glem ikke forskjellen på

mest forventet risikonivå og mulige risikonivå (mulige utfall med annen sannsynlighet)

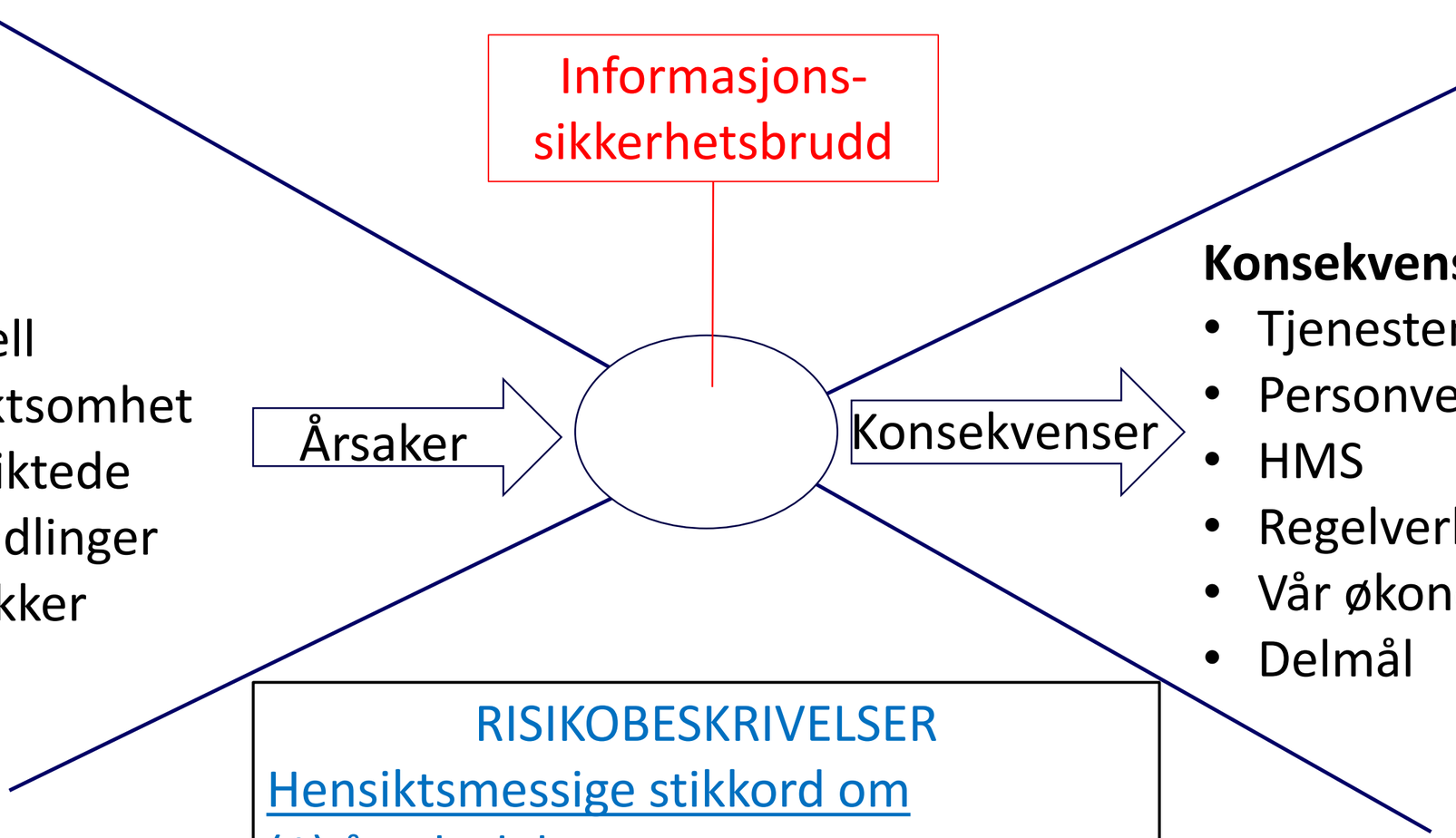


- Spesielt når mest forventet gir risikonivå «Lav»

UTTRYKKE RISIKO

Difi

Formuler helhetlige risikobeskrivelser
Visuell støtte i sløyfediagram



Kilder

- Uhell
- Uaktsomhet
- Tilsiktede handlinger
- Ulykker

Konsekvenskategori

- Tjenestenivå
- Personvern
- HMS
- Regelverk
- Vår økonomi
- Delmål

RISIKOBESKRIVELSER

Hensiktsmessige stikkord om

(1) årsaksdelen

(2) informasjonssikkerhetsbruddet

(3) konsekvensdelen

Difi

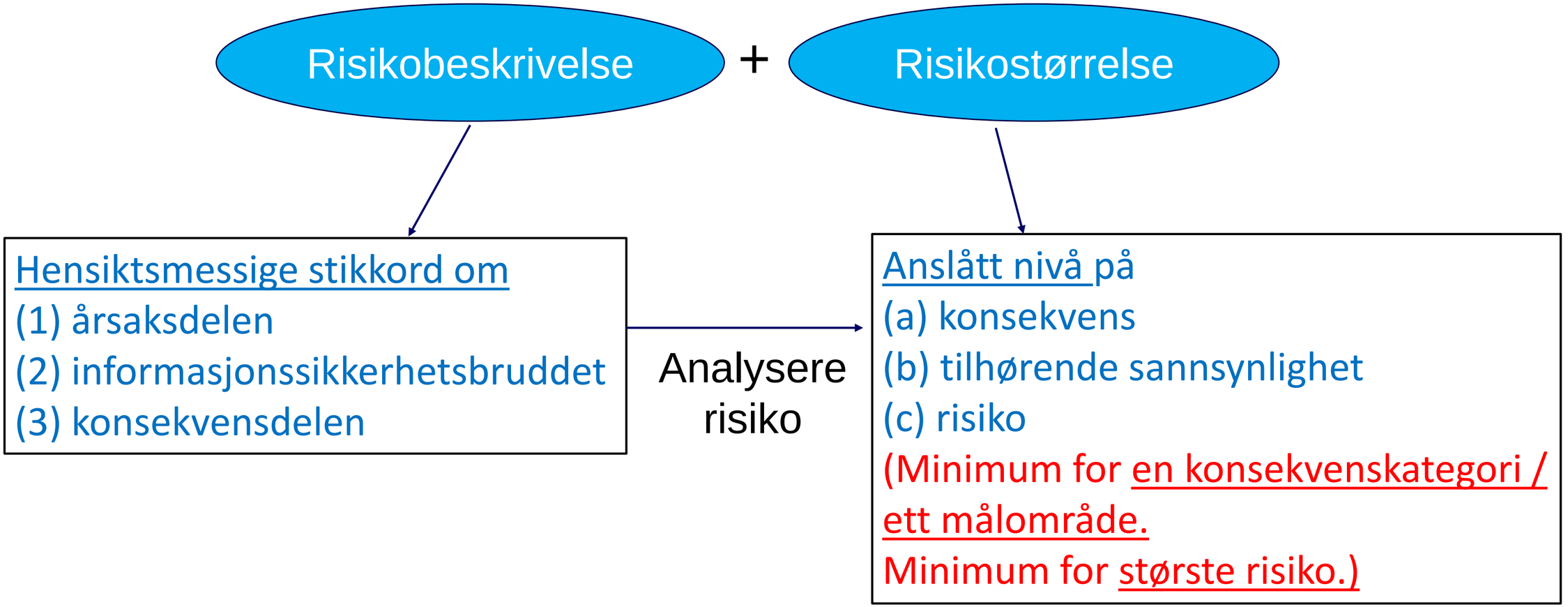
Eksempel på risikobeskrivelser

---------- Hendelse / Risikobeskrivelse / Scenario ----------			
ID	Årsak (1)	Informasjonssikkerhets-brudd (skadestart) (2)	Konsekvensbeskrivelse (3)
1	(1) Ansatte prater om sosialsaker i kantina, naboer til klienter overhører	(2) Brudd på taushetsplikt	(3) Naboer snakker om ting de ikke skulle vite, klienter opplever ubehag, barn utestenges
2	(1) Ansatte legger hemmelige adresser på internett	(2) Hemmelige adresser kommer på avveie	(3) Voldspersoner får fatt i personer med hemmelig adresse, gir personskade
3	(1) Organiserte kriminelle, sosial manipulering av ansatte via ekstern IKT-tilgang	(2) Kriminelle endrer beløp og utbetalings-konto i økonomisystem	(3) Feil utbetalinger, vi taper penger, andre får ikke det de har krav på
4	(1) Ansatte gjør feil	(2) Sletter info i tilskuddssystem	(3) Feil beslutninger og utbetalinger
5	(1) Brann i serverrom	(2) Alle system detter ned	(3) All aktivitet ute av drift, ulik grad av skad

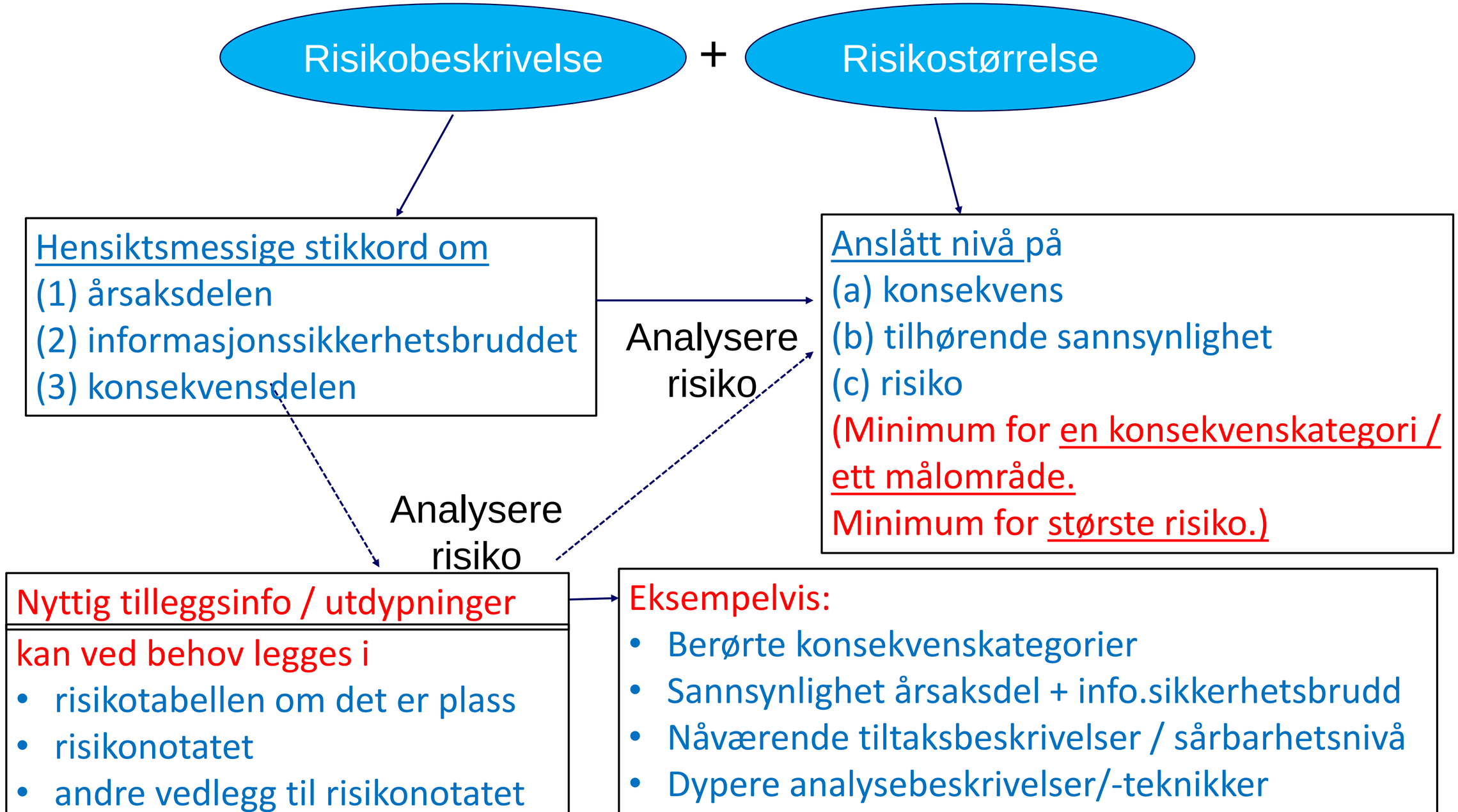
Beskrivelsene kan ha ulikt detaljeringsnivå på alle tre delene avhengig av hva som anses hensiktsmessig

Difi

Uttrykke risiko



Uttrykke risiko



OBS! Sannsynlighet for flere ting

- Husk at det er forskjell på sannsynlighet for
  1. at innledende hendelse skjer
  2. at innledende hendelse skjer og medfører informasjonssikkehetsbrudd (eller annen type målavvik)
  3. at et bestemt konsekvensnivå blir resultatet av pkt. 2

- Pkt. 3 er det vi må bruke for å uttrykke risiko riktig
- Pkt. 2 er ofte nyttig støtte for å komme frem til pkt. 3

Difi

Eksempel: NISTs risikomodell

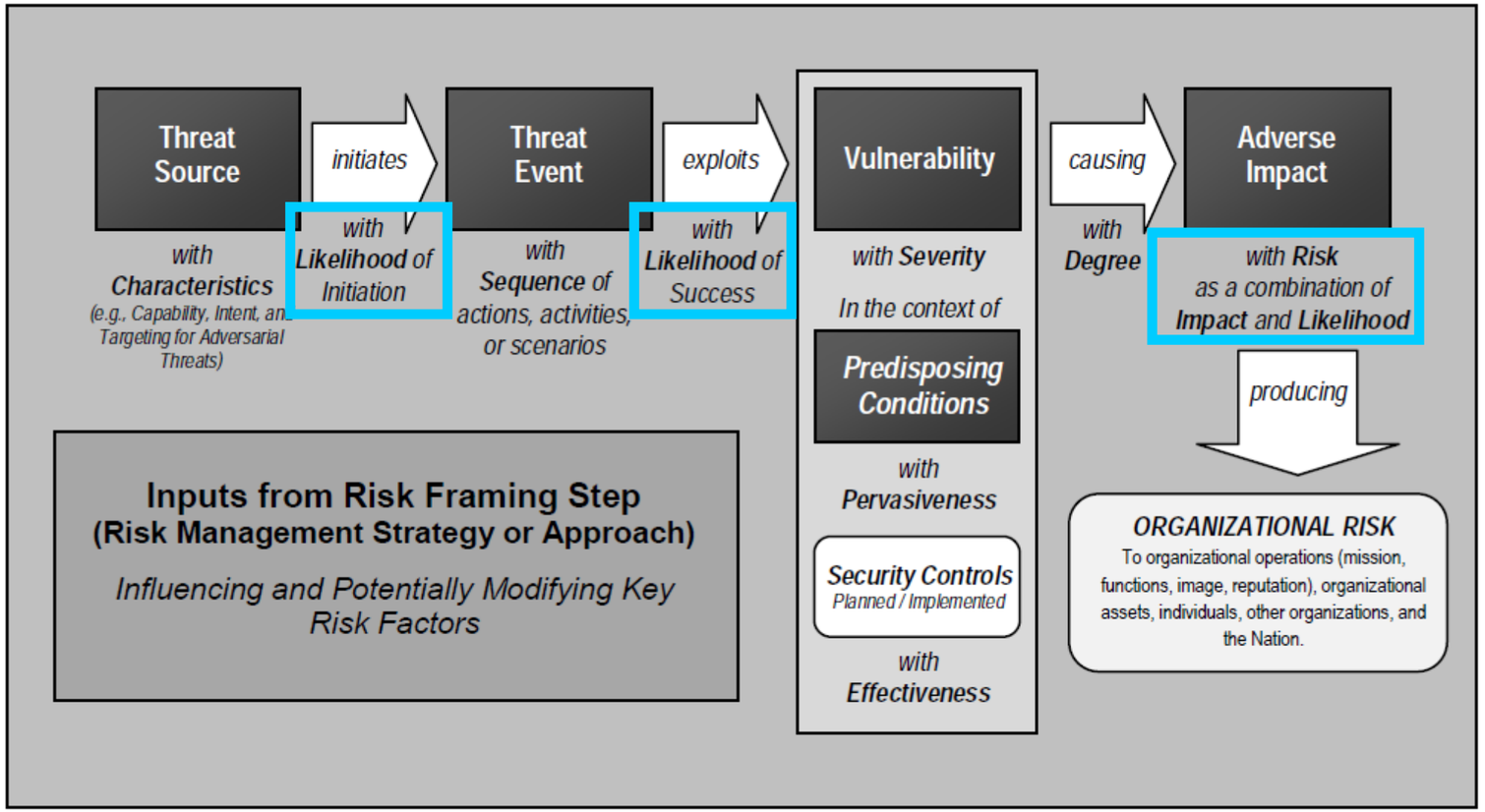


FIGURE 3: GENERIC RISK MODEL WITH KEY RISK FACTORS

Det finnes mer komplekse risikomodeller som anslår sannsynlighet for flere faktorer

Difi

Selv om vi bruker forenklinger må vi

vite hva vi gjør

og

hva som ligger bak forenklingene

Difi

Difi
Direktoratet for
forvaltning og ikt

Økt 6
Ledelsens styring og oppfølging

Innføringskurs

Internkontroll i praksis -
informasjonssikkerhet

Ledelsens styring og oppfølging
- «Hjernen» i internkontrollen

Tonen på toppen

Virksomhetsledelsen – viktige oppgaver

- Få gjennomført etableringsaktiviteter
  - Gi føringer for organisering, systematiske aktiviteter mv.
- Tilføre nødvendige ressurser
- Følge opp at de systematiske aktivitetene blir gjennomført
- Følge opp at ting fungerer som forutsatt
- Gjøre endringer ved behov

Etableringsaktivitet

Utforme overordnede styrende dokumenter

- Virksomhetsledelsens føringer for internkontrollarbeidet
- Gjelder for både virksomhetens ledere og ansatte for øvrig

- Deler kan utformes som fellesdokumenter for flere internkontrollområder

Ledelsens styring og oppfølging

SYSTEMATISKE AKTIVITETER

Difi

Ledelsens styring og oppfølging - delaktiviteter

- Virksomhetsledelsens gjennomgang
  - Minimum en gang årlig
- Ledere på alle nivå
  - Delegere og følge opp gjennom linjen
  - Sikre finansielle rammer
  - Kommunisere viktighet
  - Løfte og håndtere problemstillinger gjennom linjen
  - Beredskap og krisehåndtering

Virksomhetsledelsens gjennomgang

- Sentrale temaer over tid:
  - Status på vedtatte tiltak
  - Bakgrunnskunnskap
    - Trender
    - Sammenhenger, konflikter, balanse K-I-T
    - Betydning i virksomheten
  - Status på det helhetlige internkontrollarbeidet
  - Tilbakemeldinger på informasjonssikkerhetsnivået
  - Status på spesielle risikoer/risikoområder
  - Muligheter for forbedring

Delegere og følge opp gjennom linjen

- Tildeling av roller
  - Risikoeiere
  - Systemeiere fellessystemer
  - Tiltaksleverandører

- Bør kobles til og gjennomføres som del av den ordinære årsplanleggingen og årlige evalueringen på andre områder.

Ledelsens styring… - delaktiviteter

- Virksomhetsledelsens gjennomgang
- Delegere og følge opp gjennom linjen
- Sikre finansielle rammer
- Kommunisere viktighet
- Løfte og håndtere problemstillinger gjennom linjen
- Beredskap og krisehåndtering

Koble til ordinær virksomhetsstyring

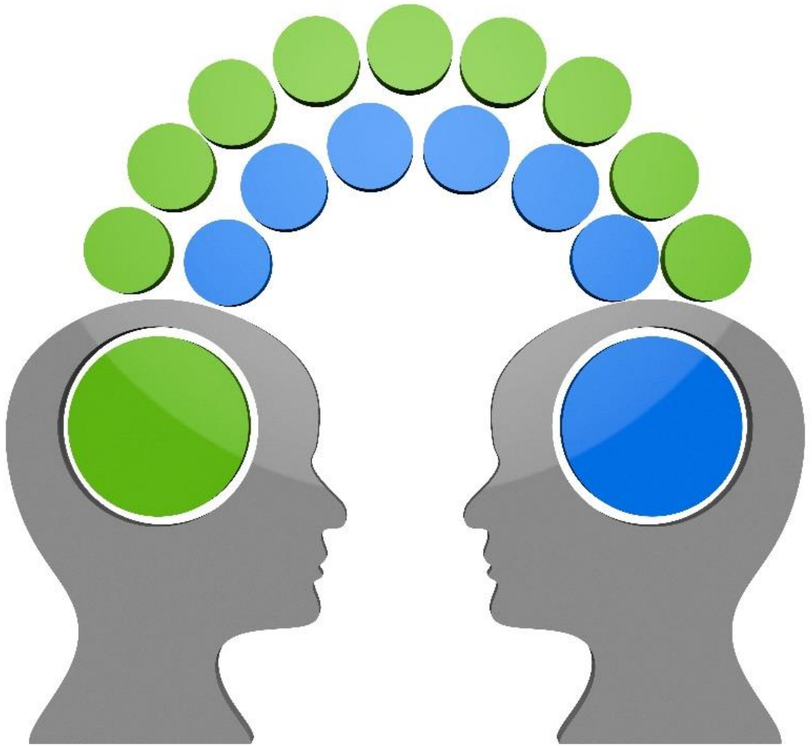
- Sikre finansielle rammer
  - Primært i ordinære budsjettprosesser
  - Budsjetter må settes opp med handlingsrom til nødvendige tiltak identifisert gjennom året
- Kommunisere viktighet
  - Tonen på toppen
- Løfte og håndtere gjennom linjen
  - Når problemer ikke kan løses på det organisatoriske nivået de oppstår, for eksempel
    - Manglende budsjettrammer
    - Aksept av (rest)risikoer
    - Uenighet om prioriteringer

Ledelsens styring… - delaktiviteter

- Virksomhetsledelsens gjennomgang
- Delegere og følge opp gjennom linjen
- Sikre finansielle rammer
- Kommunisere viktighet
- Løfte og håndtere problemstillinger gjennom linjen
- Beredskap og krisehåndtering

Krise- og beredskapshåndtering

- Konsekvensreduserende tiltak
- Ledere på ulikt nivå er sentrale aktører
- Øvelser er vesentlig!
- Virksomhetens samlede krise- og beredskapsarbeid bør henge sammen
- Bør baseres på:
  - ansvarsprinsippet
  - likhetsprinsippet
  - nærhetsprinsippet
  - samvirkeprinsippet



REFLEKSJONSOPPGAVE

Difi

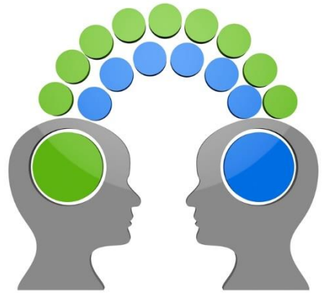
Vurderingskoder

I hvilken grad gjennomfører vi de systematiske aktivitetene og lager anbefalte dokumenter? (eller)
I hvilken grad har vi gjennomført etableringsaktivitetene og laget anbefalte dokumenter?

0	Ikke i det hele tatt, eller i liten grad
1	Noe samsvar i praksis eller i formaliserte krav, men behov for store forbedringer
2	En god del samsvar i praksis eller i formaliserte krav, men behov for en del justeringer og forbedringer
3	Tilstrekkelig samsvar i praksis, men mangler noe i formalisering/dokumentasjon
4	Tilstrekkelig samsvar i praksis og god formalisering/dokumentasjon. Ingen forbedring er nødvendig.

Difi

Refleksjonsoppgave 2



Velg noen av delaktivitetene under og diskuter i hvilken grad de gjennomføres hos dere i dag – innen informasjonssikkerhet. Bruk vurderingskodene (0 - 4) på side 1 i oppgavearkene.

Ledelsens styring og oppfølging

- Virksomhetsledelsens gjennomgang
- Delegere og følge opp gjennom linjen
- Sikre finansielle rammer for internkontroll- og sikkerhetsarbeidet
- Kommunisere viktighet
- Håndtere problemstillinger løftet gjennom linjen
- Krise- og beredskapshåndtering

Difi

Difi
Direktoratet for
forvaltning og ikt

Økt 7
Risikovurdering – del 1

–

Innføringskurs

Internkontroll i praksis -
informasjonssikkerhet

Risikovurdering
- «Hjertet» i internkontrollen

Ledelsens styring og oppfølging

- Risikovurdering
- Risikohåndtering
- Overvåkning og hendelseshåndtering
- Måling, evaluering og revisjon
- Kompetanse- og kulturutvikling

Kommunikasjon

Difi

Ansvar

- Risikoeiere (ledere på ulike nivå)
  - for egne ansvarsområder
- Systemeiere fellessystem
  - på vegne av flere risikoeiere – som må involveres

- Jf.
  - Delegering og oppfølging gjennom linjen
    - i Ledelsens styring og oppfølging

Formål med risikovurdering

- Identifisere risikoer som må håndteres
  - Det avgjørende er risikostørrelse og kriterier for å akseptere risiko

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				

- Kommunisere risiko
  - til ledere og andre

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 12 Førende prinsipper for risikohåndtering)
	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 12 Førende prinsipper for risikohåndtering)
	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 12 Førende prinsipper for risikohåndtering)
	Nytten ved at oppgaven/tjenesten utføres er større enn risikoen.
	Kan kun aksepteres av direktør eller assisterende direktør.

Difi

Utfordringer

- Bruke tid og ressurser riktig
- Ha tilstrekkelig oversikt over helheten
- Gå i dybden ved behov

Et grunnlag for sentrale aktiviteter

- Gjennomført etableringsaktivitetene
  - Felles analyse av eksterne krav
  - Identifisere typiske oppgave- og informasjonstyper

- Forenkler det praktiske arbeidet med å få oversikt og prioritere i risikovurdering

Difi

Risikovurdering

Startpunkt

- Hvilke arbeidsoppgaver utfører vi?
- Hvilken informasjon behandler vi?

Uten trening eller hjelp kan dette være vanskelig å identifisere på hensiktsmessig nivå

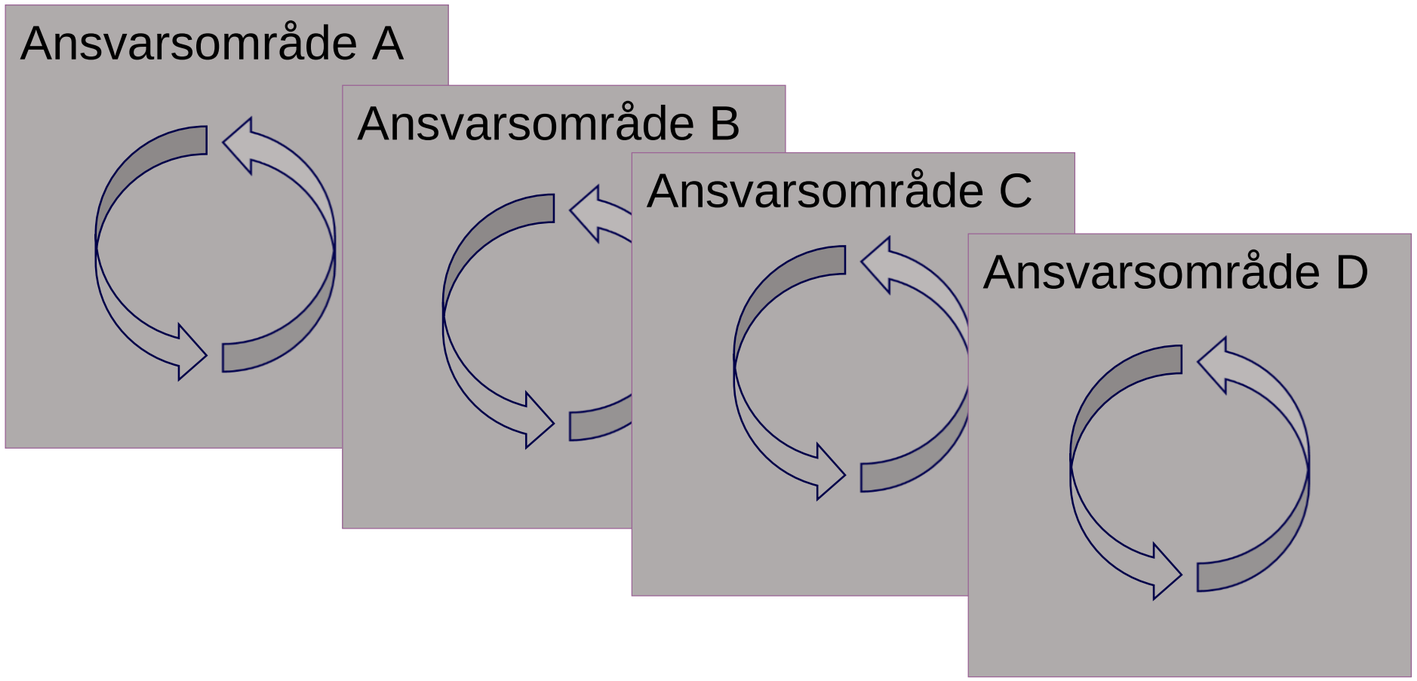
Difi

Felles identifisering og analyse

Arbeidsoppgaver

Informasjonstyper

Eksterne krav



Difi

Risikovurdering

SYSTEMATISKE AKTIVITETER

Difi

Risikovurdering - delaktiviteter

- Få oversikt og prioritere
- Analysere eksterne krav

Del 1

- Planlegge risikovurdering
- Gjennomføre risikovurdering
- Spesielle situasjoner:
  - Risikovurdere i hendelseshåndteringen
  - Risikovurdere ved anskaffelser og utvikling

Delaktiviteten

Få oversikt og prioritere

- Foranalyse
- Gruppere og dele opp
- Vurdere behov for risikovurderinger
- Oversikt over risikovurderinger
- Oppdateringer

Foranalyse (1) – Risikoeiere

- Identifisere hvilke arbeidsoppgaver (overordnet) som utføres
- For hver arbeidsoppgave identifisere
  - formål/mål med oppgaven
  - hvilke typer informasjon (overordnet) behandles
  - taushetsplikt/u.off.? personoppl.? sensitive personoppl.?
  - spesielt obs. mht. konfidensialitet, integritet, tilgjengelighet
  - hvilke IKT-system benyttes i arbeidsoppgavene
  - hvilke lover, regler, avtaler inneholder relevante krav
  - behandlingsgrunnlag, melding og konsesjon etter personopplysningsloven

Difi

Eksempel fra Difis maler

Samme skjema som i etableringsaktiviteten Identifisere typiske oppgave- og informasjonstyper

Kortnavn:	**Undersøkelser generelt**	**Oppdatert:**	30.10.2015
Fullt navn:	Gjennomføre undersøkelser generelt		
Formål med arbeidsoppgaven:	Gi råd og anbefalinger under utøving av vårt oppdrag og myndighet		

Informasjonstype	**Potensiell taushetsplikt / u.off.**	**Normalt personoppl.**		**Spesielt obs mht. info.sikkerhet**		
		Ja?	**Sensi-tiv?**	**K**	**I**	**T**
Kontaktinfo informanter		J				T
Prosessinformasjon (planer mm)	offl§14 (1)					T
Resultat datafangst	? (2)	?	?	?	I	T
Uferdig bearbeidet stoff	offl§14 (1)				I	T
Utkast sluttprodukt	offl§14 (1)				I	T
Godkjent sluttprodukt						T

Merknader
(1) Meroffentlighet skal alltid vurderes på det som kan unntas offentlighet. (2) Normalt ikke, men avhengig av undersøkelsens innretning og innhold
IKT-system som benyttes til behandling og lagring av informasjon
Fillagring prosjektområde, epost, sak-arkivsystem
Spesielle krav til informasjonssikkerhet
pof? (I den grad man behandler personopplysninger)
Spesielle krav til gjennomføring av arbeidsoppgaven
offl, fvl, arkl
Behandlingsgrunnlag for personopplysninger
pol §8 samtykke eller §8 d, e, f (I den grad man behandler personopplysninger)
Melding eller konsesjonssøknad til Datatilsynet
Meldeplikt hvis man behandler personopplysninger. Hvis sensitive behandles vil det normalt også være konsesjonsplikt.

Difi

Foranalyse (2) – Risikoeiere

- Finne høyeste konsekvensnivå
  - på arbeidsoppgavene som utføres og systemene som benyttes
  - ved brudd på konfidensialitet, integritet eller tilgjengelighet
    - Informasjonen som behandles og målet med oppgavene er vurderingsgrunnlaget (jf. kartleggingen foran)
    - Støtte hentes i felles beskrivelser av konsekvensnivåene til risiko-vurderinger

	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

- En forenklet variant av såkalt verdivurdering og klassifisering

Difi

Eksempel fra Difis maler
Foranalyse – Potensielt konsekvensnivå

Organisatorisk enhet SSDI Dato sist oppdatert	Oppgavene samlet, informasjons-systemer og hjelpemidler			Arbeidsoppgave 1 (Navn under) Tilskuddsforvaltning - Skogbruk			
	Potensielt konsekvensnivå			Potensielt konsekvensnivå oppgaven og hjelpemidler mv.			Merknad (f.eks. brukes ikke til spesiell informasjon i oppgaven
	Konfiden-sialitet	Integritet	Tilgjenge-lighet	Konfiden-sialitet	Integritet	Tilgjenge-lighet	
(Arbeidsoppgaven(e) samlet)	Lav	Høy	Moderat	Lav	Høy	Moderat	
Hjelpemidler							
Papirutskrifter							
Tynnklient (terminal)							
Jobb-pc	Høy	Høy	Moderat	Lav	Høy	Moderat	
Jobb-Mobiltelefon							
Jobb - Nettbrett o.l.							
Privat utstyr							
Fjernkommunikasjon							
Eksterne databehandlere	Svært høy	Moderat	Høy				
Felles informasjonssystem							
Journal- og arkivsystem	Lav	Lav	Moderat	Lav	Lav	Moderat	
E-post	Ubetydelig	Ubetydelig	Moderat	Ubetydelig	Ubetydelig	Moderat	Brukes kun til purring
Filserver	Lav	Høy	Moderat	Lav	Høy	Moderat	
Kontorstøtte(word, excel m.v.)	Lav	Høy	Moderat	Lav	Høy	Moderat	
Egne informasjonssystem							
Fagsystem A	Lav	Høy	Moderat	Lav	Høy	Moderat	

Difi

Foranalyse (2) – Systemeiere fellessystem

- Finne høyeste konsekvensnivå
  - på «sine» fellessystem
  - ved brudd på konfidensialitet, integritet eller tilgjengelighet

- Vurderingene fra Risikoeierne er viktig bakgrunnsinformasjon

Organisatorisk enhet SSDI Dato sist oppdatert	Oppgavene samlet, informasjons-systemer og hjelpemidler			Arbeidsoppgave 1 (Navn under) Tilskuddsforvaltning - Skogbruk			
	Potensielt konsekvensnivå			Potensielt konsekvensnivå oppgaven og hjelpemidler mv.			Merknad (f.eks. brukes ikke til spesiell informasjon i oppgaven
	Konfiden-sialitet	Integritet	Tilgjenge-lighet	Konfiden-sialitet	Integritet	Tilgjenge-lighet	
(Arbeidsoppgaven(e) samlet)	Lav	Høy	Moderat	Lav	Høy	Moderat	
Hjelpemidler							
Papirutskrifter							
Tynnklient (terminal)							
Jobb-pc	Høy	Høy	Moderat	Lav	Høy	Moderat	
Jobb-Mobiltelefon							
Jobb - Nettbrett o.l.							
Privat utstyr							
Fjernkommunikasjon							
Eksterne databehandlere	Svært høy	Moderat	Høy				
Felles informasjonssystem							
Journal- og arkivsystem	Lav	Lav	Moderat	Lav	Lav	Moderat	
E-post	Ubetydelig	Ubetydelig	Moderat	Ubetydelig	Ubetydelig	Moderat	Brukes kun til purring
Filserver	Lav	Høy	Moderat	Lav	Høy	Moderat	
Kontorstøtte(word, excel m.v.)	Lav	Høy	Moderat	Lav	Høy	Moderat	
Egne informasjonssystem							
Fagsystem A	Lav	Høy	Moderat	Lav	Høy	Moderat	

Difi

Foranalyse (3) – Risikoeiere og systemeiere fellessystem

- Overordnede vurderinger rundt størrelsen på typiske
  - trusselaktører
  - farekilder
  - sårbarheter

Eksempel fra Difis maler
Foranalyse - Trusselaktører

	Grunnlag			Konklusjon	Merknad (ev. spesielt utsatte arbeidsoppgaver, informasjonstyper, system e.l.)
	Intensjon		Kapasitet	Trusselnivå	
Trusselaktør	Motiv	Vilje			
Utro tjenere internt i virksomheten					
Utro tjenere hos ekstern databehandler					
Nærstående person med fysisk tilgang					
Nærstående person uten fysisk tilgang					
Forfølgere av trusselutsatte					
Vinningskriminelle					
Pøbel					
Hacktivister					
Fremmed makt (land)					
Terrorister					
(Andre?)					

Eksempel fra Difis maler
Foranalyse - Farer

Farekilde	Område	Sannsynlighet (kan skje og gi vesentlig skade)	Forventet skadenivå (om det skjer)	Merknad (ev. spesielle forhold som påvirker forannevnte nivå)
Brann	Hos ekstern databehandler			
Brann	I eget serverrom			
Brann	I arbeidslokaler			
Vannlekkasje	Hos ekstern databehandler			
Vannlekkasje	I eget serverrom			
Vannlekkasje	I arbeidslokaler			
Annen naturhendelse	Hos ekstern databehandler			
Annen naturhendelse	I eget serverrom			
Annen naturhendelse	I arbeidslokaler			
Annen hendelse	I nærområdet			

Eksempel fra Difis støtteverktøy
Foranalyse - Sårbarheter

Område / Sentrale mål-utsagn for området	Sårbarhets-nivå	Merknad
1) I egen organisatoriske enhet		
Ledelsen har og følger gode rutiner for å gi, endre og fjerne brukernes tilgang og rettigheter til IKT-system		
Klare prosedyrer og rutiner for arbeidet generelt og bruken av ulike IKT-løsninger spesielt		
Ansatte rapporterer alltid sikkerhetsbrudd og andre uønskede hendelser		
Ledelsen har systematisk oppfølging av rapporterte sikkerhetsbrudd og uønskede hendelser		
God kompetanse blant ledelse og ansatte mht. info.sikkerhet generelt og gjeldende rutiner spesielt		
God kultur blant ledelse og ansatte mht. viktighet av info.sikkerhet og etterlevelse av gjeldende rutiner		
Annet?		
2) IKT-systemer der man selv er systemeier		
Gode løsninger og rutiner for pålogging, tilgangs- og rettighetsstyring		
Trygge løsninger og rutiner for pålogging og tilgang til bakenforliggende databaser		
Tilfredsstillende logger som enkelt kan følges opp		
God brukerinvolvering i anskaffelse, forbedringer og risikovurderinger		
Godt tilpasset arbeidsoppgavene og gir ikke behov for å finne personlige omveier		
Profesjonelt utviklede		

Foranalyse (4) – Risikoeiere og systemeiere fellessystem

- Refleksjon over resultatet
- Oppsummere spesielle obs-områder

Delaktiviteten

Få oversikt og prioritere

- Foranalyse
  - Identifisere arbeidsoppgaver, informasjonstyper, system mv.
  - Anslå potensielt konsekvensnivå
  - Vurdere trusler, farer og sårbarheter
  - Oppsummere spesielle obs-områder
- Gruppere og dele opp
- Vurdere behov for risikovurderinger
- Oversikt over risikovurderinger
- Oppdateringer

Foranalysen gir grunnlag for

- Gruppere og dele opp
- Vurdere behov for risikovurderinger

- Rekkefølgen her kan være litt frem og tilbake
- Formålet er å prioritere og effektivisere arbeidet med «tradisjonelle» risikovurderinger

Difi

Få oversikt og prioritere

Gruppere og dele opp

- Homogene / enkle arbeidsoppgaver, gode rutiner, profesjonelle systemer, og høy kompetanse
  - Vi grupperer og foretar videre vurderinger samlet
- Større organisatoriske enheter, eller enheter med stor variasjon i oppgaver, prosjekter, systemer, rutiner og/eller kompetanse
  - Ofte behov for en oppdeling av vurderingsarbeidet
- Komplekse eller kritiske enheter, prosjekter, arbeidsoppgaver eller IKT-systemer
  - Vi skiller disse ut fra resten og vurderer de enkeltvis videre
- Komplekse eller kritiske IKT-systemer
  - Kan i enkelte tilfeller med fordel deles opp i ulike deler som vurderes for seg

Få oversikt og prioritere

Vurdere behov for risikovurderinger

- Overordnet behovsvurdering
  - Hvor usikker er jeg på om risikoene jeg har ansvaret for kan aksepteres iht. virksomhetens kriterier?
  - Krever det nye/oppdaterte risikovurderinger?
- Foreslått gjennomføring
  - en enkel kvalitativ og skjønnsmessig vurdering
    - Enkle støttespørsmål
    - Kategoriene lav, moderat og høy usikkerhet
    - Et sett beslutningskriterier
      - ut fra usikkerhetsnivå kombinert med potensielt konsekvensnivå
- Forankring og føringer
  - Retningslinje Vurdere behov for risikovurderinger
    - i de overordnede styrende dokumentene

Fra Difis eksempel på retningslinje Støttespørsmål

Vedlegg A: Støttespørsmål

Etter hvert temaområde i spørsmålene under, bør man fortløpende kort reflektere over, og ved behov notere, både antatt høyeste risikonivå og nivå på egen usikkerhet på om risikoene kan aksepteres som de er. Dette konkluderes det på til slutt i støttespørsmålene.

Høyeste konsekvensnivå:

1. Hva er høyeste konsekvensnivå innen området
   - ved brudd på konfidensialitet, integritet og tilgjengelighet? (når risikoer ved informasjonssikkerhet er relevant for vurderingen)
   - ved brudd på kvalitetskrav? (dersom det er relevant for vurderingen)

(Det siste kulepunktene fjernes dersom retningslinjen kun skal gjelde informasjonssikkerhet)

Oversikt:

2. Hvor god oversikt har vi over området?
   - Mål for arbeidet eller tjenesten, system som benyttes og hvem som utfører arbeidet
   - Trusler, farer og sårbarheter

Tidligere risikovurderinger og risikohåndtering:

3. Er det tidligere gjort gode risikovurderinger og en systematisk risikohåndtering på dette eller direkte sammenlignbare områder?
   - av oss eller andre vi har stor tillit til
4. I hvilken grad føler vi oss trygge på at tidligere arbeid med identifisering og valg rundt alternative arbeidsmåter og risikoreduserende sikkerhetstiltak, dekker våre risikoer og kravene rundt disse i våre kriterier for å akseptere risikoer?
   - gjennom bl.a. virksomhetens fellessikring og vår tilleggssikring
5. Er det vesentlige delområder eller risikoer som ikke er vurdert eller håndtert godt nok?
   - pga. manglende tid og kompetanse
   - pga. usikkerhet rundt sentrale deler av området eller usikkerhet rundt trusler, farer og sårbarheter

Nye faktorer:

Difi

Fra Difis eksempel på retningslinje Beslutningskriterier

Vedlegg B: Beslutningskriterier

Velg prioriteringsgruppe for området ut fra

- Høyeste konsekvensnivå fra spørsmål 1
- Nivå på usikkerhet fra spørsmål 10

Usikkerhet om risikoene kan aksepteres					
Nivå usikkerhet		Prioritetsgruppe for risikovurderinger			
	Høy	5	4	2	1
	Moderat	0	5	3	2
	Lav	0	0	6	6
		Lav	Moderat	Høy	Svært høy
		Konsekvensnivå			

Planlegg risikovurderinger iht. tabellen under

Prioritets-gruppe	Beslutning
0	• Det er **ikke behov** for å gjennomføre nye eller oppdaterte risikovurderinger
1 - 2	• Ny/oppdatert risikovurdering skal gjennomføres **uten ugrunnet opphold** • Prioritering skal skje etter prioritetsgruppe • Nye arbeidsoppgaver skal ikke startes og nye system skal ikke tas i bruk før ny eller oppdatert risikovurdering er gjennomført og fulgt opp • Det skal straks vurderes om det er behov for eventuelle midlertidige ekstratiltak eller stopp i gjennomføring av oppgaver og bruk av IKT-system og annet utstyr.
3 - 5	• Ny/oppdatert risikovurdering skal gjennomføres **innen rimelig tid** • Prioritering skal skje etter prioritetsgruppe og ut fra kunnskapsstyrken[5] på tidligere vurderinger • Nye arbeidsoppgaver kan startes og nye system kan tas i bruk dersom de etableres innen virksomhetens fellessikring og oppgaven som skal løses er svært viktig for å nå virksomhetens overordnede mål

Delaktiviteten

Få oversikt og prioritere

- Foranalyse
- Gruppere og dele opp
- Vurdere behov for risikovurderinger
- Oversikt over risikovurderinger
  - Planlagte og gjennomførte
- Oppdateringer

Få oversikt og prioritere

Oppdateringer

- Sjekk endringsbehov en gang i året

- Vurdere behov for oppdateringer
  - når vesentlige svakheter i tidligere arbeid blir identifisert
  - ved vesentlige endringer i oppgaveinnhold, arbeidsmåter, hvilken type informasjon som behandles, eller omgivelsene
  - ved nye arbeidsoppgaver

- Hovedjobben er m.a.o. første gang man skal få oversikt og prioritere

Difi

Få oversikt og prioritere

Suksesskriterium

- Prosessleder
  - Minimum ved første gangs gjennomføring
  - Planlegging og forarbeid
  - Strukturert ledelse av arbeidet
- Hensiktsmessige maler / støtteverktøy

Delaktiviteten

Analysere eksterne krav

- Relevante regler og avtaler
  - bør ofte analyseres nærmere
  - Få oversikt over tiltak eller typer tiltak som kreves
- Mye kan ofte gjøres i tilsvarende etableringsaktivitet

- Resultatet er input til risikovurderinger og risikohåndtering
- Risikoeier må forsikre seg om at kravene er
  - inne i fellessikringen
  - eller kommer inn som tilleggssikring

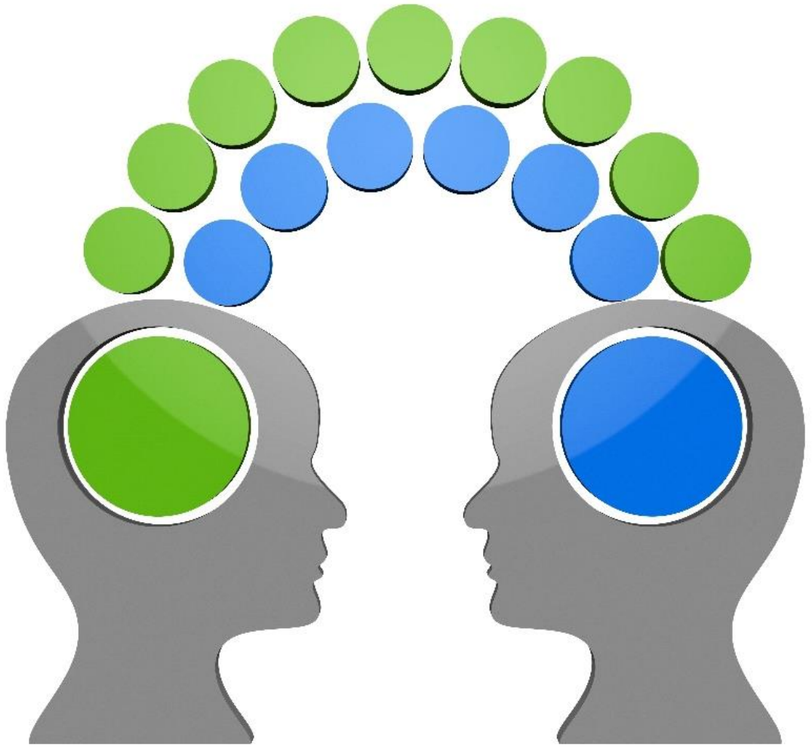
Risikovurdering - delaktiviteter

- Få oversikt og prioritere
- Analysere eksterne krav

Del 1

- Planlegge risikovurdering
- Gjennomføre risikovurdering
- Spesielle situasjoner:
  - Risikovurdere i hendelseshåndteringen
  - Risikovurdere ved anskaffelser og utvikling

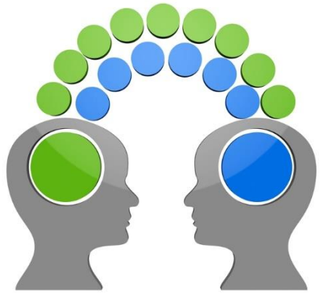
Difi



REFLEKSJONSOPPGAVE

Difi

Refleksjonsoppgave 3



Velg noen av delaktivitetene under og diskuter i hvilken grad de gjennomføres hos dere i dag – innen informasjonssikkerhet.
Bruk vurderingskodene (0 - 4) på side 1 i oppgavearkene.

Risikovurdering

- Få oversikt og prioritere
  - Foranalyse av eget ansvarsområde
  - Gruppere og dele opp
  - Vurdere behov for risikovurderinger
  - Holde oversikt over risikovurderinger
- Analysere eksterne krav

Difi

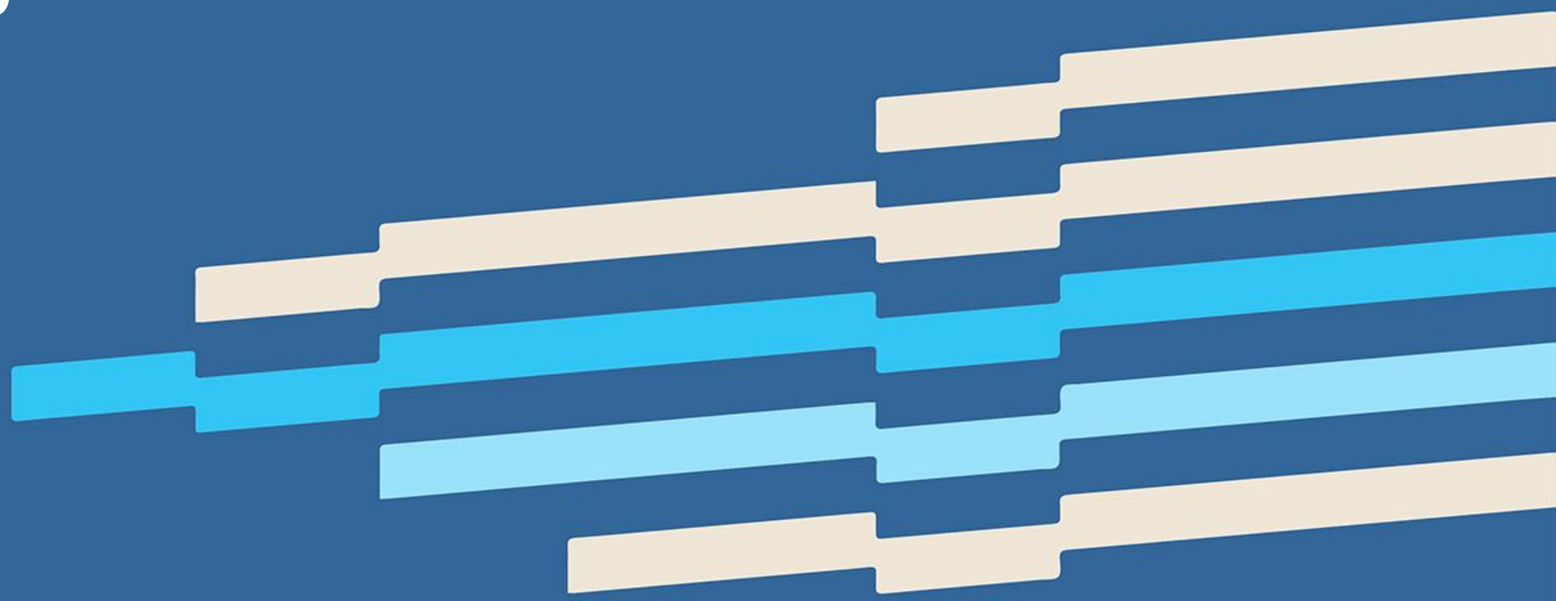
Difi
Direktoratet for
forvaltning og ikt

Økt 8
Risikovurdering – del 2

—

Innføringskurs

Internkontroll i praksis -
informasjonssikkerhet



Risikovurdering - delaktiviteter

- Få oversikt og prioritere
- Analysere eksterne krav
- Planlegge risikovurdering
- Gjennomføre risikovurdering
- Spesielle situasjoner:
  - Risikovurdere i hendelseshåndteringen
  - Risikovurdere ved anskaffelser og utvikling

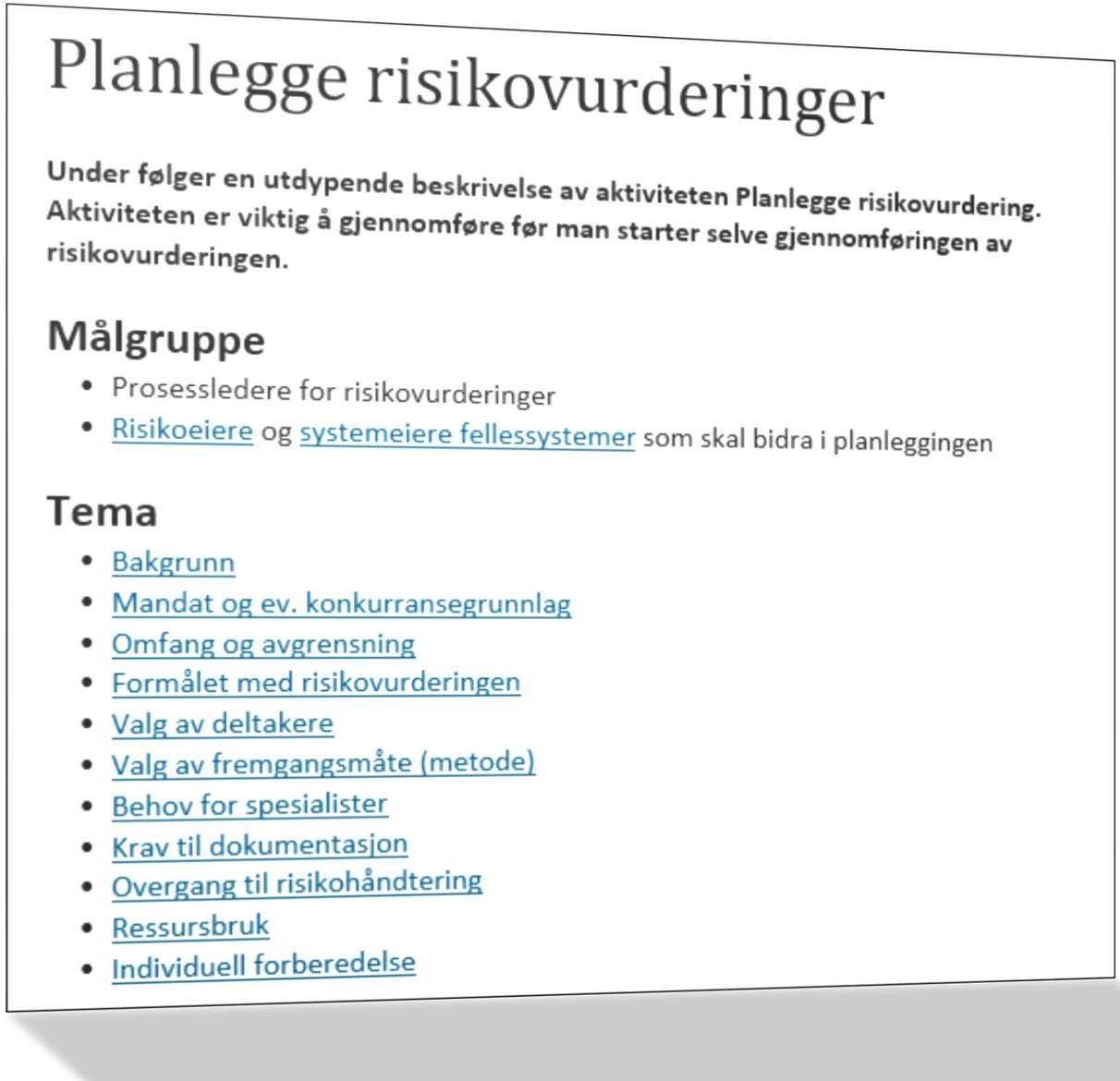
Del 2

Difi

Planlegge risikovurdering

- Utforme mandat
  - Omfang og avgrensinger
  - Formål
  - Skal gruppen også identifisere tiltak?
    - Første del av risikohåndteringen
- Velge deltakere
- Ta stilling til fremgangsmåte
- Vurdere behov for spesialister
- Hvordan skal arbeidet dokumenteres?

Utdypende veiledning



Planlegge risikovurderinger

Under følger en utdypende beskrivelse av aktiviteten Planlegge risikovurdering. Aktiviteten er viktig å gjennomføre før man starter selve gjennomføringen av risikovurderingen.

Målgruppe

- Prosessledere for risikovurderinger
- Risikoeiere og systemeiere fellessystemer som skal bidra i planleggingen

Tema

- Bakgrunn
- Mandat og ev. konkurransegrunnlag
- Omfang og avgrensning
- Formålet med risikovurderingen
- Valg av deltakere
- Valg av fremgangsmåte (metode)
- Behov for spesialister
- Krav til dokumentasjon
- Overgang til risikohåndtering
- Ressursbruk
- Individuell forberedelse

Difi

Gjennomføre risikovurdering

Forutsetning for arbeidet

Føringer fra ledelsen

- Etablere felles forståelse av
  - hva risiko er
  - hvordan risikoer skal
    - uttrykkes
    - estimeres
    - håndteres
  - hvilke kriterier som gjelder for å akseptere risiko

- Gis f.eks. i Retningslinje:
  - Forstå, vurdere og håndtere operativ risiko

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				

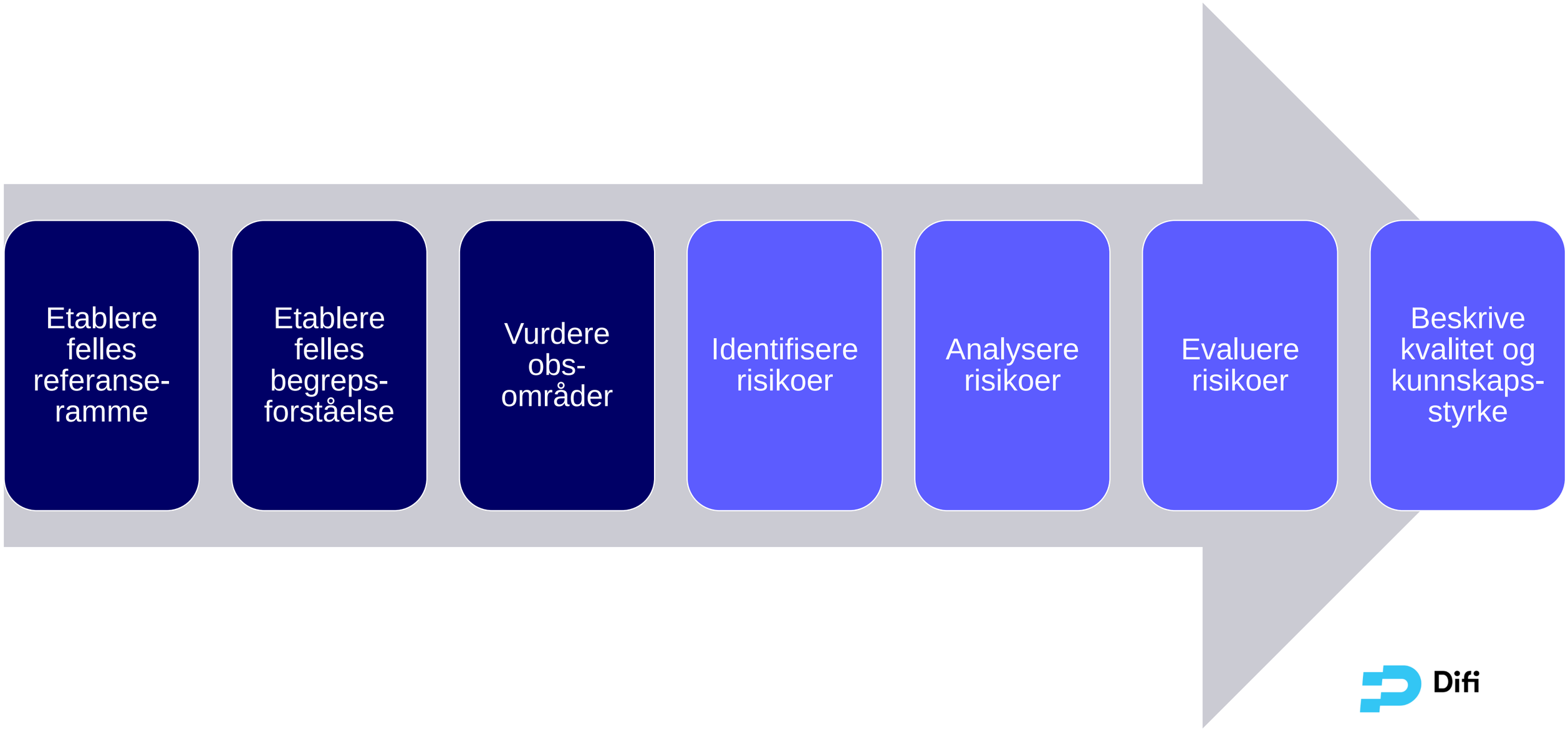
Risikonivå	Kriterier for å akseptere risiko
Lav	Kan aksepteres **uten å lete etter eller vurdere nytten av** alternative arbeidsmåter eller flere risikoreduserende tiltak. Merk at dette gjelder når hele utfallsrommet for en risiko har risikostørrelse på nivå lav innen alle berørte konsekvenskategorier.
	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 12 Førende prinsipper for risikohåndtering)
	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 12 Førende prinsipper for risikohåndtering)
	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 12 Førende prinsipper for risikohåndtering)
	Nytten ved at oppgaven/tjenesten utføres er større enn risikoen.
	Kan kun aksepteres av direktør eller assisterende direktør.

Difi

Suksesskriterium

- Prosessleder
  - Planlegging og forarbeid
  - Strukturert ledelse av arbeidet
- Hensiktsmessige maler / støtteverktøy

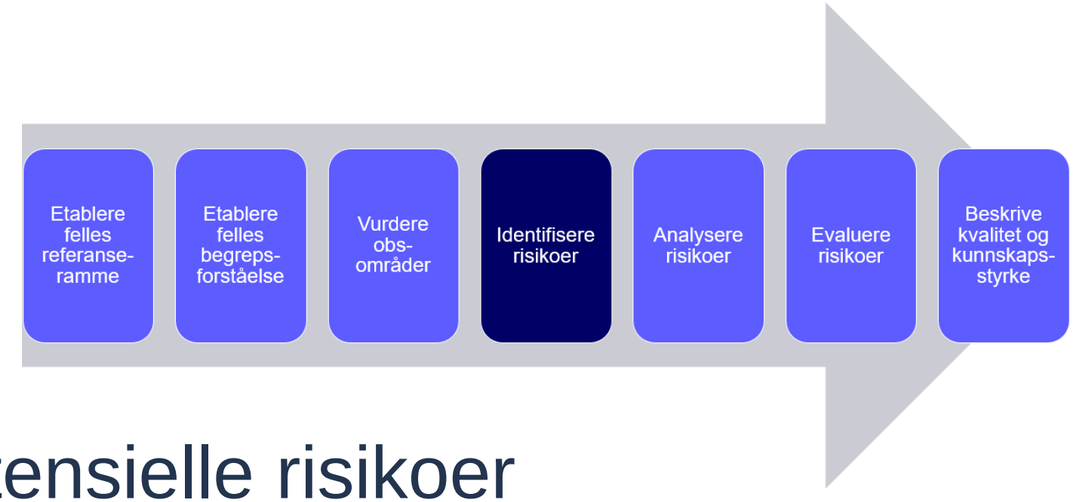
Gjennomføre risikovurdering



Difi

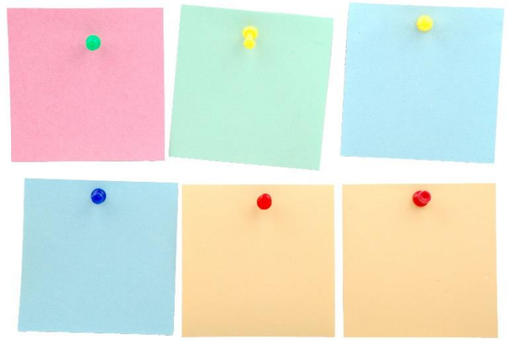
Trinn 4

Identifisere risikoer



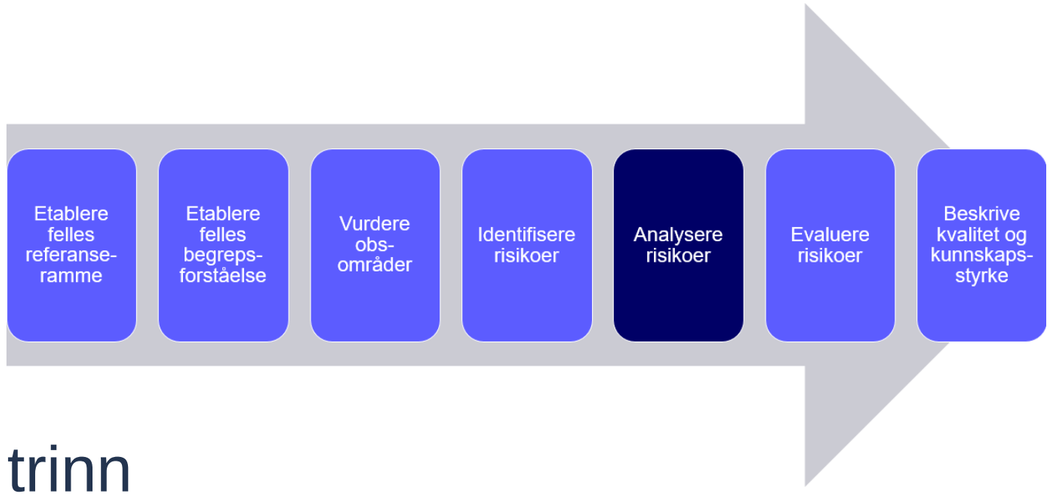
- Identifiser et sett av relevante potensielle risikoer
- Formuler dem i helhetlige risikobeskrivelser
- Prioriter dem i noen hovedgrupper for arbeidet videre

- Idédugnad og gruppediskusjon



Trinn 5

Analysere risikoer



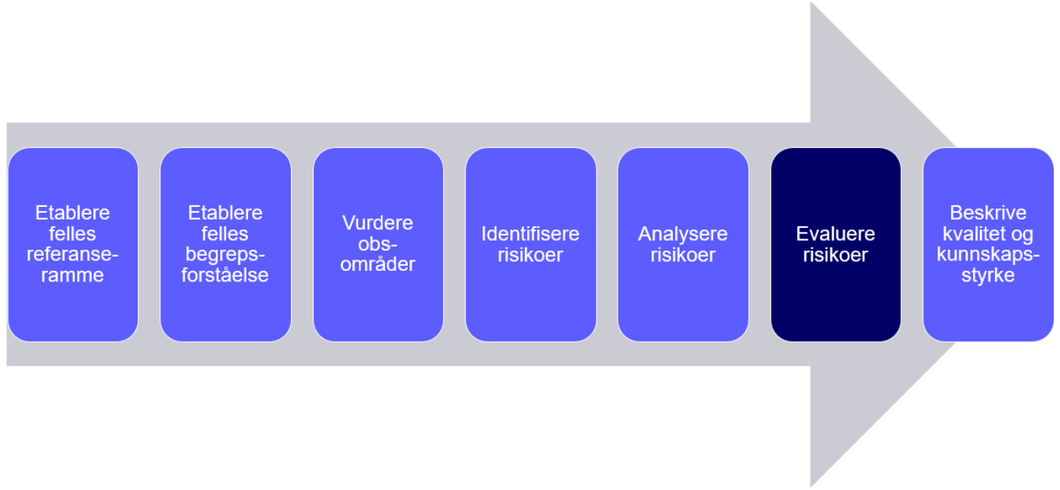
- Analyser risikobeskrivelsene fra forrige trinn
  - Hva kan skje underveis og hvorfor?
- Estimere / anslå nivået på
  - konsekvens
  - tilhørende sannsynlighet
  - risiko

  på største risiko ved risikobeskrivelsen
- Utdyp analyse og dokumentasjon av enkelte risikoer ved behov

Difi

Trinn 6

Evaluere risikoer



- Evaluer hver av risikoene fra forrige trinn opp mot virksomhetens kriterier for å akseptere risiko

- Synliggjør hvilke risikoer
  - som kan aksepteres slik de er
  - som trenger mer tiltaksvurdering (risikohåndtering) før de eventuelt kan aksepteres

Difi

Trinn 7

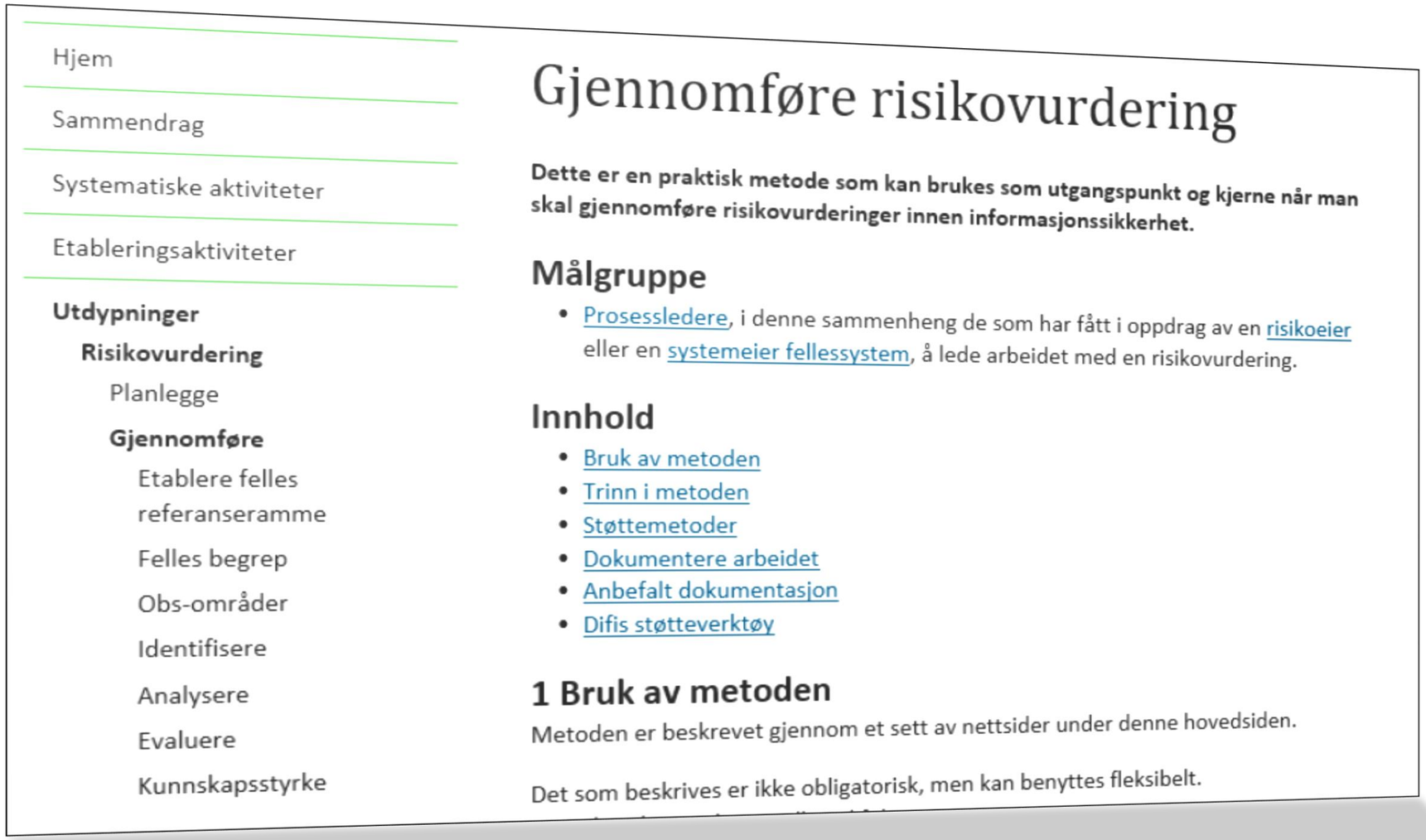
Beskrive kvalitet og kunnskapsstyrke

- Kvalitet:
  - Metoder som er brukt
  - Tilpasninger
  - Tidsbruk
  - Hva var bra, hva kunne vært gjort bedre/grundigere?

- Kunnskapsstyrke:
  - Høy, moderat, lav – ut fra
    - Hvor god bakgrunnskunnskap
    - Kompetanse
      - Kjennskap til objektet
      - Fagkompetanse
      - Analysekompetanse
    - Grundighet

Difi

Utdypende veiledning



Difi

Risikovurdering - delaktiviteter

- Få oversikt og prioritere
- Analysere eksterne krav
- Planlegge risikovurdering
- Gjennomføre risikovurdering
- Spesielle situasjoner:
  - Risikovurdere i hendelseshåndteringen
  - Risikovurdere ved anskaffelser og utvikling

Difi

Risikovurdere i hendelseshåndteringen

- Hendelsen har ikke har vært inkludert i tidligere risikovurderinger

…eller

- Analysen har ikke vært tilstrekkelig

Gjennomføre avgrensede behovsvurderinger og evt. risikovurderinger

Difi

Risikovurdere ved anskaffelser og utvikling

- Sikkerhetsmessige behov må identifiseres for å stille tilstrekkelige sikkerhetsmessige krav

…gjennom

- Samme fremgangsmåte som funksjonelle krav
- Analyse av eksterne krav
- Risikovurdering(er)

- Sikkerhetskrav = Risikoreduserende tiltak
  - Vurderes opp mot kriterier for å akseptere risiko
  - Godkjennes av risikoeier

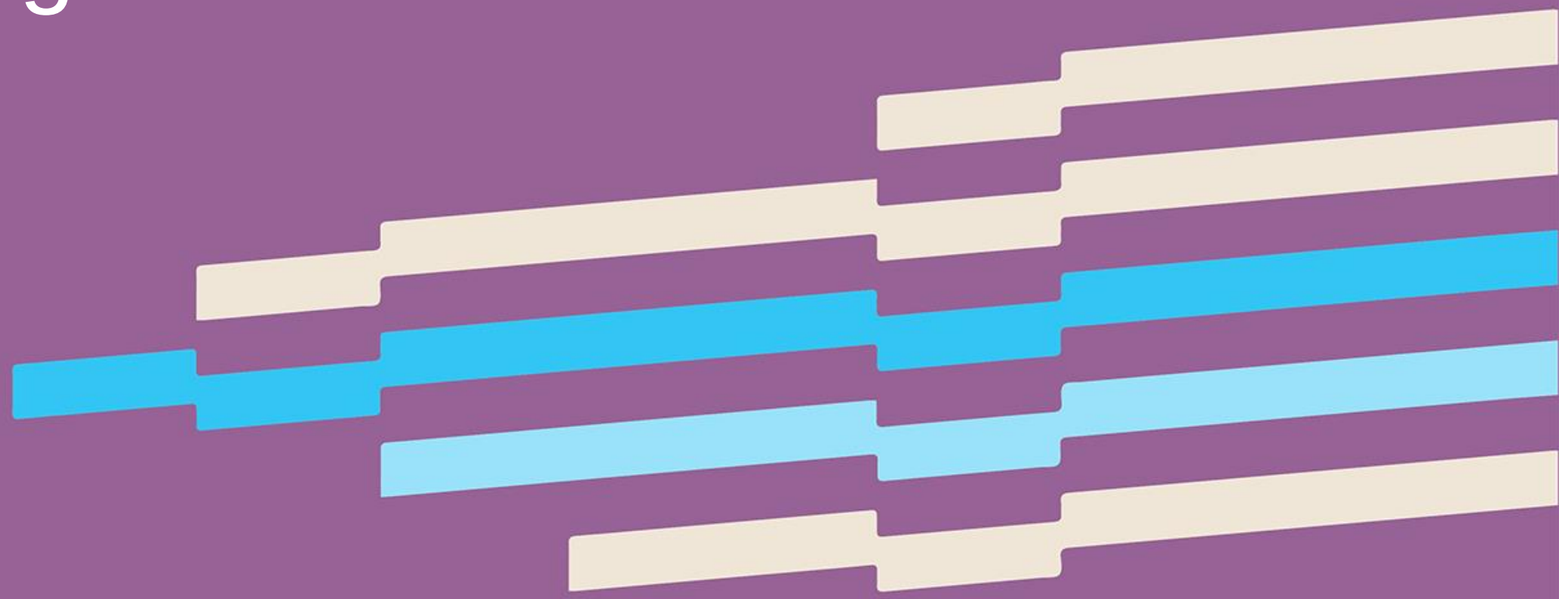
Difi

Difi
Direktoratet for
forvaltning og ikt

Økt 9
Risikohåndtering – del 1

Innføringskurs

Internkontroll i praksis -
informasjonssikkerhet



Risikohåndtering
- «Hendene» i internkontrollen

Håndteringsalternativer

- Unngå risiko
  - finne andre fremgangsmåter / arbeidsmåter
  - eller
  - la være å gjøre oppgaven
- Dele risiko
- Redusere risiko
  - tiltak for å redusere sannsynlighet
  - og/eller
  - tiltak for å redusere konsekvens
  - forebygge
  - oppdage
  - reagere
- Akseptere risiko

Engangstiltak og varige tiltak

- Engangstiltak:
  - Reduserer ofte risikoen på kort sikt, men har mindre verdi på lang sikt
  - Eks: installere sikkerhetspatcher

- Varige tiltak:
  - Tiltak som iverksettes for å virke over tid
  - Eks: etablere gode prosesser for kontinuerlig oppfølging av kjente sårbarheter

- I denne sammenhengen er det stort sett varige tiltak vi mener når vi snakker om sikkerhetstiltak

Difi

Virkning, kostnad og sideeffekter

- Tiltak har ulik
  - risikoreduserende effekt - innvirkning på risikoen
  - direkte økonomisk kostnad
  - negative sideeffekter

- Må veies opp mot hverandre ved valg av tiltak

Risikohåndtering

SYSTEMATISKE AKTIVITETER

Risikohåndtering - delaktiviteter

- Foreslå håndtering av risikoer
- Godkjenne forslag til risikohåndtering
- Iverksette godkjente tiltak
- Utforme og implementere tiltakene
- Oppdatere fellessikringen

Foreslå håndtering av risikoer

- Følger i forlengelsen av Gjennomføre risikovurdering
  - Dersom det er risikoer som ikke kan aksepteres som de er

- Mandatet til risikovurderingen styrer
  - om «Foreslå håndtering …» er en egen aktivitet
  - eller skal gjøres sammen med risikovurderingen

- Resultatet av både Risikovurdering og Foreslå håndtering av risikoer er beslutningsgrunnlag for risikoeier

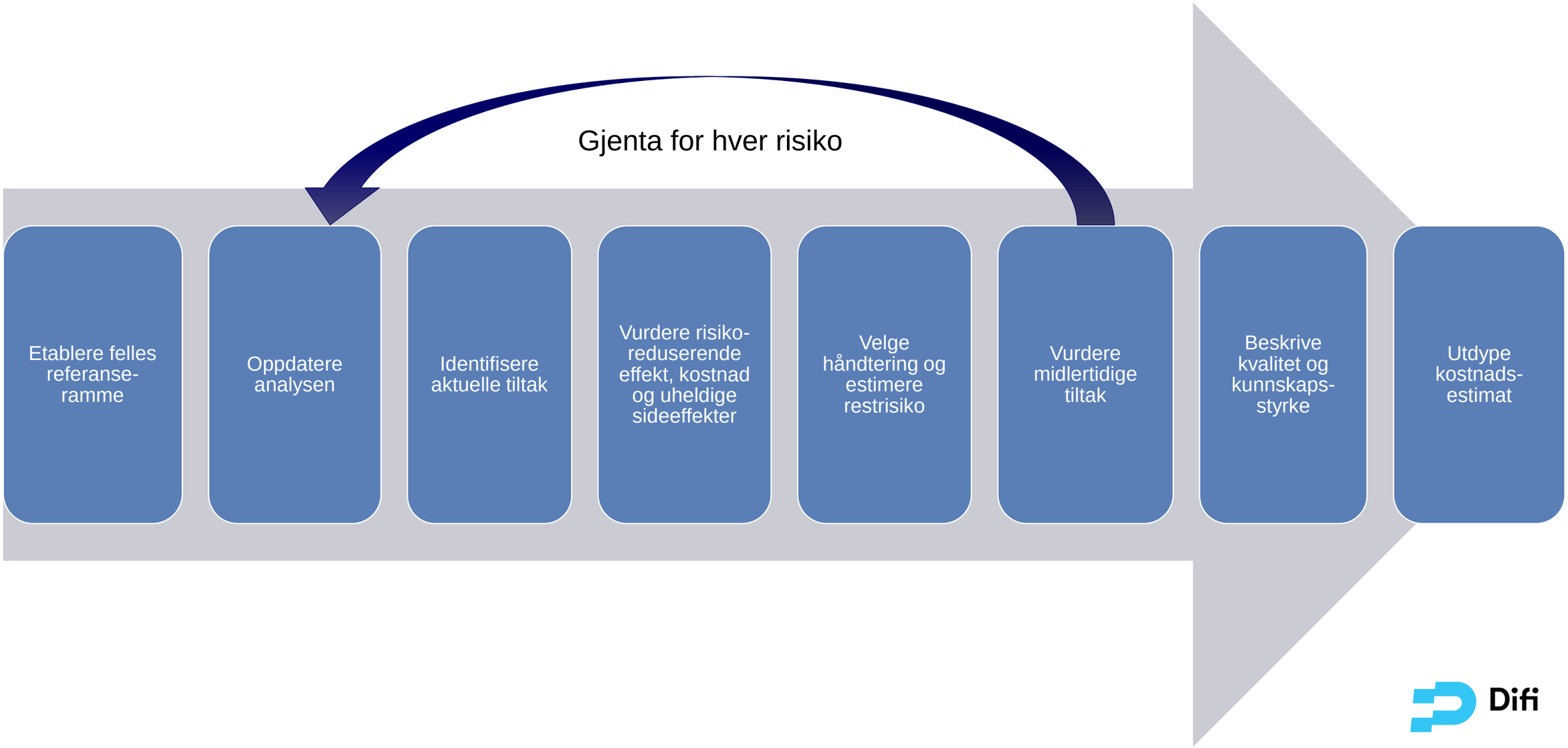
Difi

Foreslå håndtering av risikoer

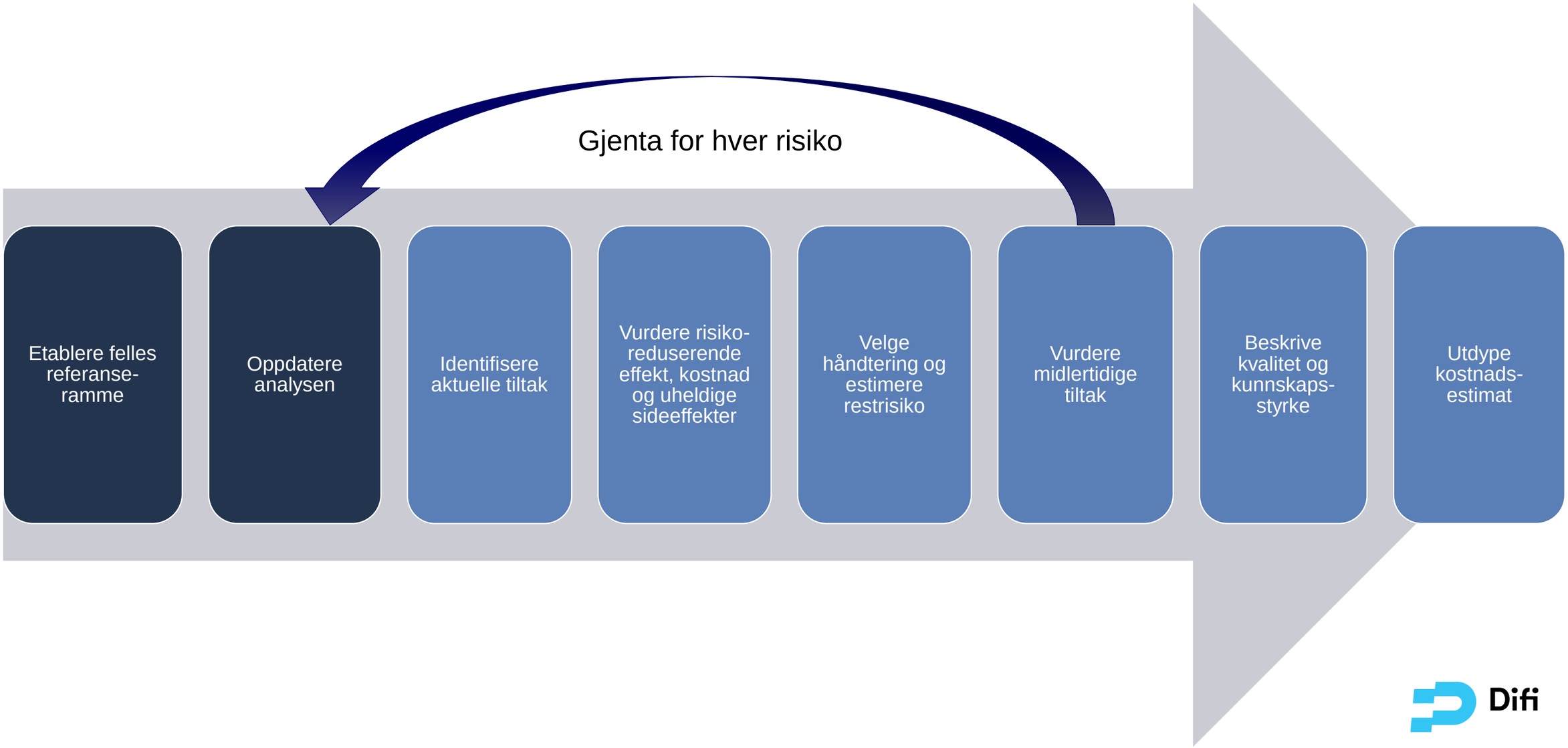
Suksesskriterium

- Prosessleder
  - Planlegging og forarbeid
  - Strukturert ledelse av arbeidet
- Hensiktsmessige maler og støtteverktøy

Foreslå håndtering av risikoer



Foreslå håndtering av risikoer



Trinn 3

Identifisere aktuelle tiltak

- Identifiser tiltak som kan være relevante i håndteringen av den aktuelle risikoen

3 Støttespørsmål

3.1 Har vi allerede relevante tiltaksforslag?

Dette hovedspørsmålet kan også stilles slik:

- Har vi allerede tiltaksforslag på andre risikoer som også virker vesentlig inn på den risikoen vi ser på nå?

Spørsmålet er ikke aktuelt på den første risikoen som er til vurdering, men aktuelt for alle senere risikoer. Ulike tiltak kan ha vesentlig innvirkning på flere risikoer.

3.2 Kan vi unngå risikoen?

Aktuelle delspørsmål kan være:

- Hvor viktig er oppgaven som ligger bak informasjonsbehandlingen og risikoen?
- Kan vi la være å gjøre oppgaven?
- Kan arbeidet som skal gjøres tilrettelegges annerledes slik at risikoen unngås?
- Kan hele eller deler av oppgaven eller informasjonsbehandlingen gjennomføres på en annen måte eller med andre hjelpemidler for den aktuelle informasjonen?

3.3 Er det mulig å dele risikoen med noen?

Aktuelle delspørsmål kan være:

- Kan vi kjøpe forsikring slik at risikoen forsvinner eller blir mindre?
- Kan vi tjenesteutsette noe og inngå tjenestenivåavtaler (SLA), slik at vi kan få økonomisk erstatning som kan fjerne eller redusere risikoen?
- Kan regelverks- eller avtaleendring være aktuelt slik at ansvaret forskyves?

3.4 Kan vi redusere risikoen?

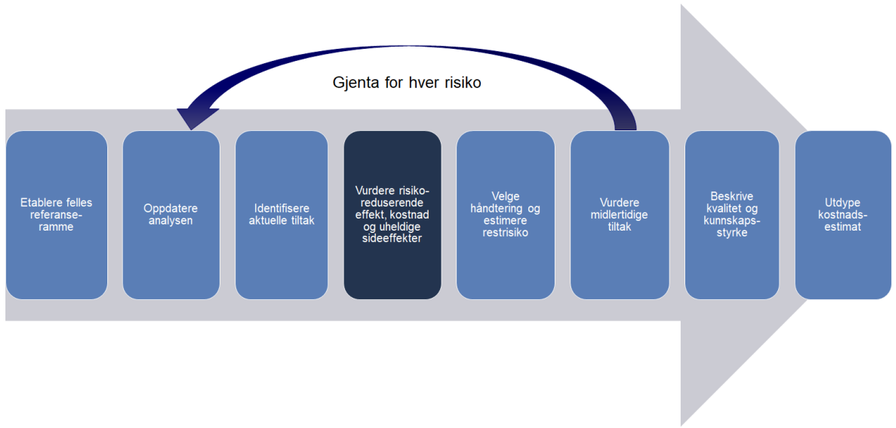
- Strukturert idémyldring
- Noter forslag på tiltak fortløpende

Difi

Trinn 4

Vurdere risikoreduserende effekt, kostnad og negative sideeffekter

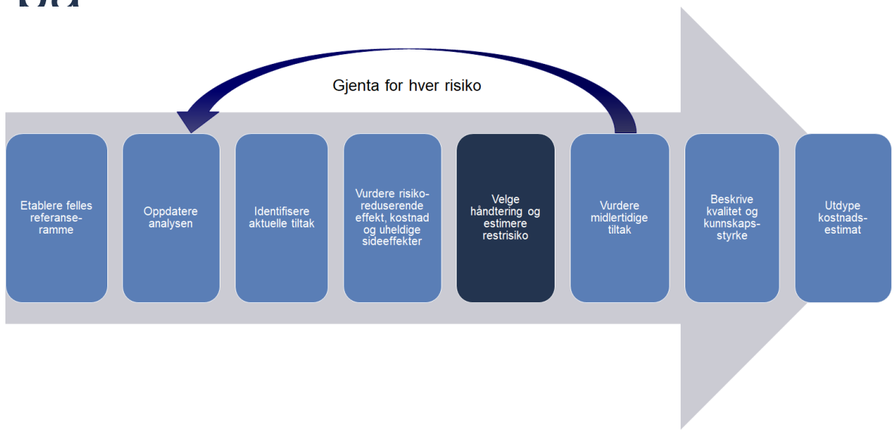
- For hvert tiltak:
  - Få en grov oversikt over nivåene på
    - risikoreduserende effekt
    - direkte økonomiske kostnader
    - eventuelle negative sideeffekter
  - Bruk nivåene Høy | Moderat | Lav
    - på hvert av de tre perspektivene



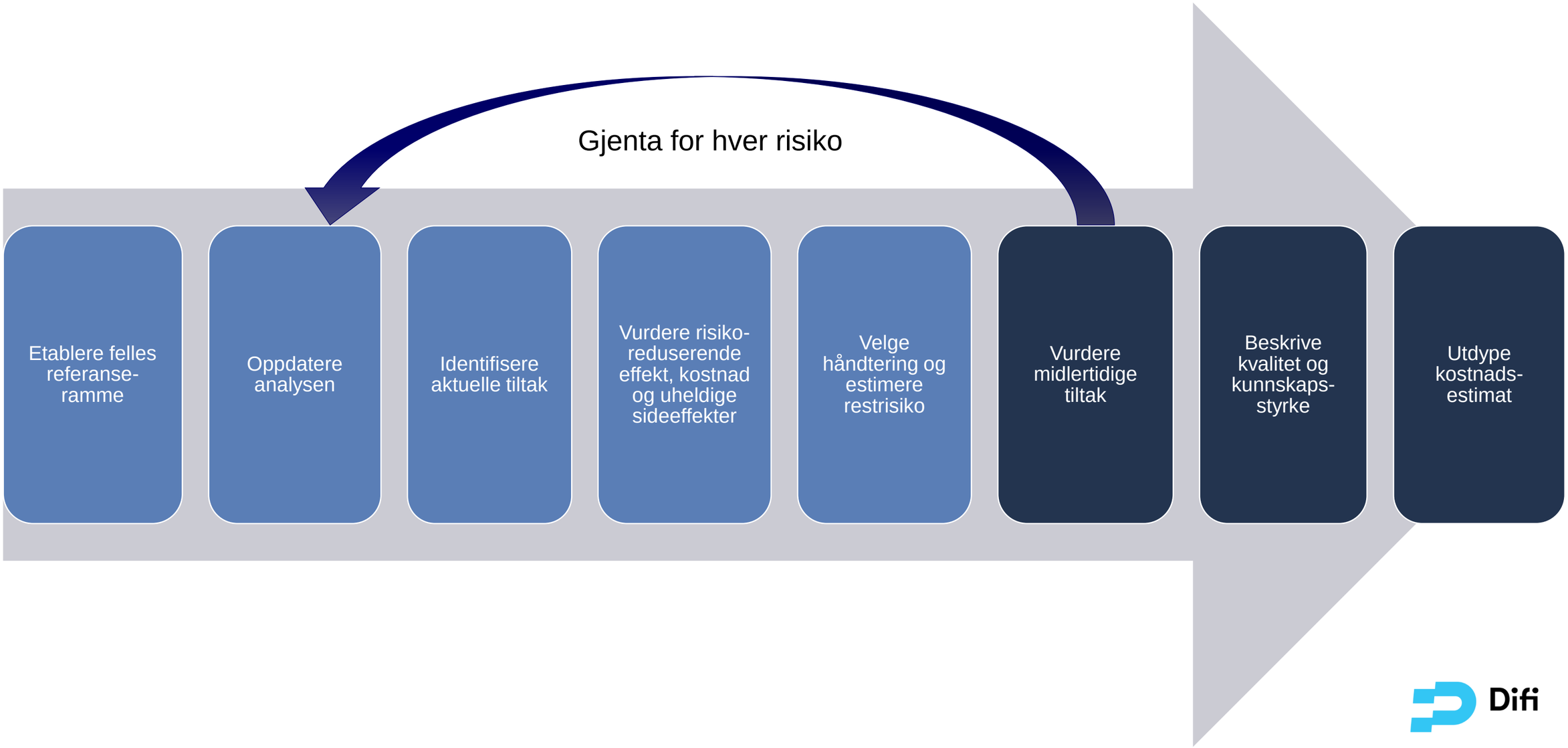
Trinn 5

Velge håndtering og estimere restrisiko

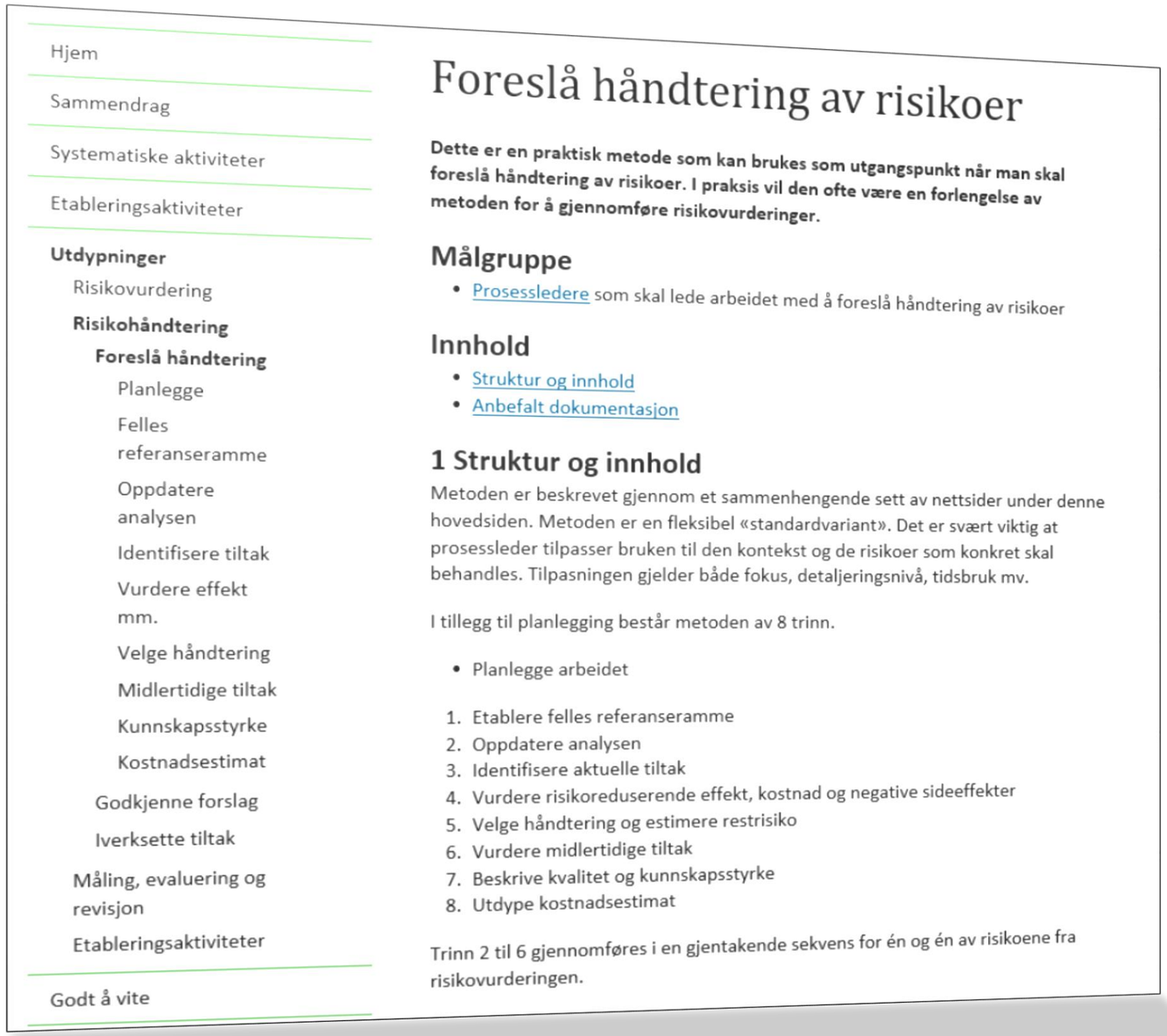
- Velg eller avvis potensielle tiltak ut fra
  - Vurdering av kombinasjonene Høy, Moderat, Lav på
    - risikoreduserende effekt
    - direkte økonomiske kostnader
    - negative sideeffekter
  - Grundigere nytte/kost-vurderinger ved behov
- Oppdater risikohåndteringsskjemaet
  - Hvilke potensielle tiltak som faktisk blir foreslått valgt
- Oppdatere risikovurderingsskjemaet
  - Estimere restrisiko – basert på forslag til valgte tiltak
  - Gjennomføres som i analysetrinnet i risikovurdering



Foreslå håndtering av risikoer



Utdypende veiledning



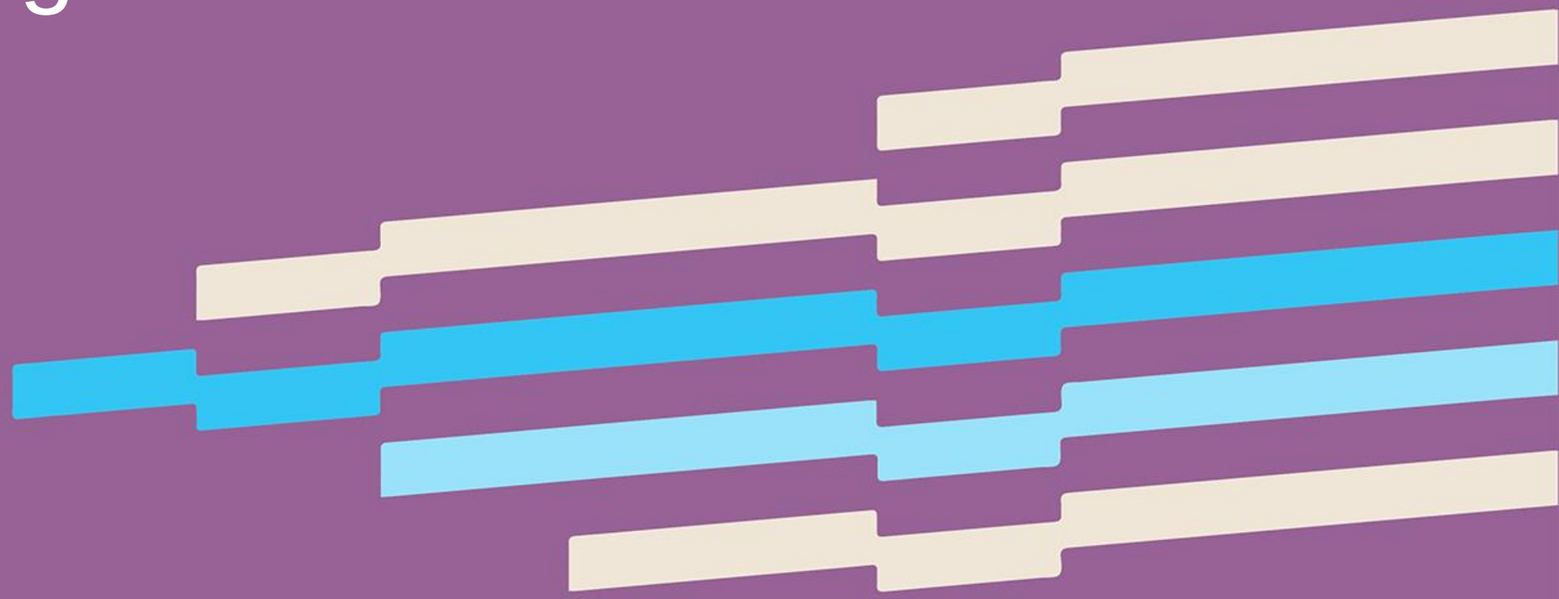
Difi
Direktoratet for
forvaltning og ikt

Økt 10
Risikohåndtering – Del 2

—

Innføringskurs

Internkontroll i praksis -
informasjonssikkerhet



Risikohåndtering
- «Hendene» i internkontrollen

Ledelsens styring og oppfølging

- Risikovurdering
- **Risikohåndtering**
- Overvåking og hendelseshåndtering
- Måling, evaluering og revisjon
- Kompetanse- og kulturutvikling

Kommunikasjon

Risikohåndtering

- Foreslå håndtering av risikoer ✔
- Godkjenne forslag til risikohåndtering
- Iverksette godkjente tiltak
- Utforme og implementere tiltakene
- Oppdatere fellessikringen

Godkjenne forslag

- Analysens kvalitet
- Kunnskapsstyrke
- Restrisiko
- Kost/nytte
- Finansiering
- Involvere andre?
- Ny vurdering?

Tiltakets effekt

Direkte kostnad
Negative sideeffekter

Utdypende veiledning

Godkjenne forslag til risikohåndtering

Under følger en utdypning av delaktiviteten Godkjenne forslag til risikohåndtering under hovedaktiviteten Risikohåndtering.

Målgruppe

- Risikoeiere eller systemeiere for felles informasjonssystem. Vi kaller dem beslutningstaker her.

Innhold

- Utgangspunkt og bakgrunn
- Vurdere kvalitet
- Vurdere restrisiko og kunnskapsstyrke
- Vurdere kost/nytte
- Finansiere tiltakene
- Avstemme med andre oppgaveeiere
- Dokumentere
- Be om ny vurdering
- Godkjenne og sikre oppfølging

Iverksette tiltak

- Utføres av: Håndteringsansvarlig
- Handlingsplan for gjennomføring | etablering av godkjente tiltak
- Plan utformes i dialog med de som skal gjennomføre
  - Inkl. gjøre avtaler med tiltaksleverandører
- Handlingsplan bør godkjennes av risikoeier
- Håndteringsansvarlig følger opp
  - inkl. nødvendig rapportering

Utforme og implementere

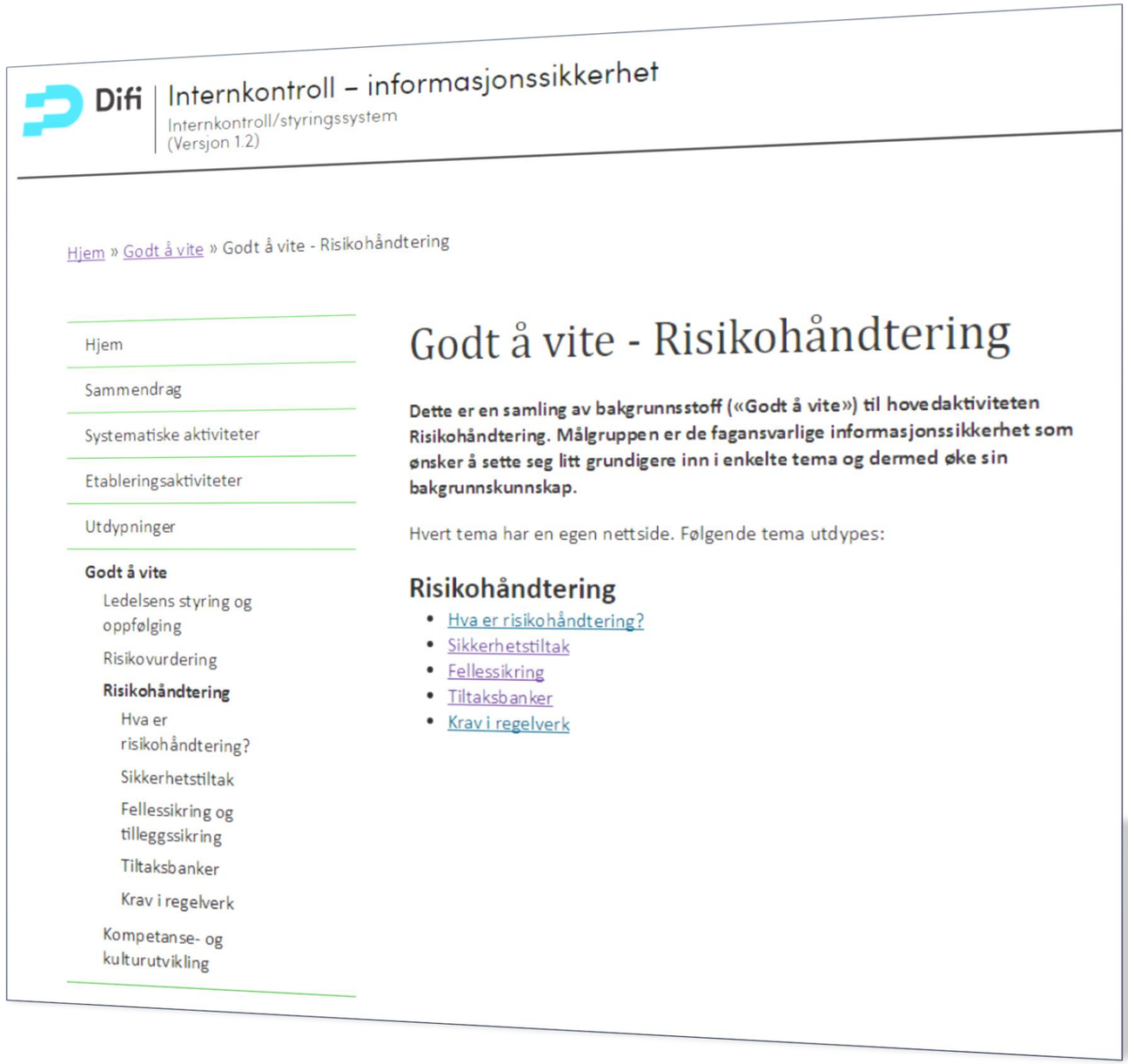
- Utføres av tiltaksleverandører
  - interne og eksterne
- Risikoeier kan selv være ansvarlig
  - eks: rutiner, kompetanseheving
- Tiltak kan ta mange former
  - type og omfang
- Testing
  - Etter behov
  - Alle faser aktuelle: utforming | implementering | iverksatt

Oppdatere fellessikringen

- Systematisk vurdering av nye tiltak
- Oppdatere fellessikring og tilleggssikring
- Samme typer vurderinger som ved etablering av fellessikring
  - Kostnadseffektiv drift av sikkerhetsarbeidet
  - Negative sideeffekter
  - Beslutning på riktig nivå

Godt å vite - Risikohåndtering

- Sikkerhetstiltak
- Tiltaksbanker
- Fellessikring



Difi

Difi
Direktoratet for forvaltning og ikt

Økt 11
Oppsummering risikovurdering og -håndtering

—

Innføringskurs

Internkontroll i praksis - informasjonssikkerhet

Deks Direktoratet for eksempler

Difi

Difi

Ledelsens styring og oppfølging

- Sikre finansielle rammer
- Kommunisere viktighet
- Løfte problemstillinger i linjen

Risikovurdering

- Ha tilstrekkelig oversikt og vurdere behov for risikovurderinger
- Identifisere konkrete krav i relevante lover og regler som må følges
- Planlegge og gjennomføre nødvendige risikovurderinger

Risikohåndtering

- Foreslå håndtering av risikoer
- Godkjenne forslag til risikohåndtering
- Iverksette godkjente tiltak

Måling, evaluering og revisjon

- Vurdere status på eget ansvarsområde

Difi

Få oversikt og prioritere

Få oversikt og prioritere

- Foranalyse av eget ansvarsområde

Arbeidsoppgave:	Tilskuddsforvaltning		**Oppdatert:**	(dato)		
Kort beskrivelse:	(Område, ordning e.l.)					
Formål:						
Informasjonstype	**Paragraf for potensiell taushetsplikt / u.off.**	**Normalt personoppl.**		**Spesielt obs mht. info.sikkerhet**		
		Ja?	**Sensi-tiv?**	**K**	**I**	**T**
Kunngjøring					I	T
Søkerinfo		?	N		I	
Søknad		?	N		I	?
Vurdering og anbefaling					I	?
Beslutning					I	?
Tilskuddsbrev (utbetalingsbrev)					I	T
Klage og klagevurdering						
Aksept / bekreftelse					I	
Godkjenne utbetaling					I	
Merknader						
IKT-system som benyttes til behandling og lagring av informasjon						
Tilskuddsportalen, Sak-arkiv, Word, Excel, Filserver, e-post						
Hvilke eksterne virksomheter benyttes til behandling og lagring av informasjon						
Regelverk med spesielle krav til informasjonssikkerhet						
Regelverk med spesielle krav til gjennomføring av arbeidsoppgaven						

Få oversikt og prioritere

- Foranalyse av eget ansvarsområde

Organisatorisk enhet	Oppsummering for alle arbeidsoppgavene			Arbeidsoppgave 1				Arbeidsoppgave 2			
Tilskuddsseksjonen				Tilskuddsforvaltning				Oppfølging av mottakere			
Dato sist oppdatert	Høyeste konsekvensnivå			Høyeste konsekvensnivå				Høyeste konsekvensnivå			
10.09.2017	Konfidensialitet	Integritet	Tilgjengelighet	Konfidensialitet	Integritet	Tilgjengelighet	Merknad	Konfidensialitet	Integritet	Tilgjengelighet	Merknad
Arbeisdsoppgaven(e)	Svært høy	Høy	Moderat	Svært høy	Høy	Moderat		Lav	Moderat	Moderat	
Hjelpemidler/utstyr											
Papirutskrifter											
Jobb-pc											
Jobb-mobiltelefon/nettbrett/o.l											
Privat-pc											
Privat-mobiltelefon/nettbrett/o.l											
Felles IKT-system											
Journal- og arkivsystem											
E-post											
Filserver											
Word											
Excel											
Enhetens egne IKT-system											
Tilskuddsportalen											

Difi

Få oversikt og prioritere

- Foranalyse av eget ansvarsområde
- Gruppere og dele opp

Få oversikt og prioritere

- Foranalyse av eget ansvarsområde
- Gruppere og dele opp
- Vurdere behov for risikovurderinger

Deks Direktoratet for eksempler

Vurdere behov for risikovurderinger

(EKSEMPEL per 15.6.2017 - utarbeidet av Difi)

Vedlegg A: Støttespørsmål

Etter hvert temaområde i spørsmålene under, bør man fortløpende kort reflektere over, og ved behov notere, både antatt høyeste risikonivå og nivå på egen usikkerhet på om risikoene kan aksepteres som de er. Dette konkluderes det på til slutt i støttespørsmålene.

Høyeste konsekvensnivå:

1. Hva er høyeste konsekvensnivå innen området
   - ved brudd på konfidensialitet, integritet og tilgjengelighet? (når risikoer ved informasjonssikkerhet er relevant for vurderingen)
   - ved brudd på kvalitetskrav? (dersom det er relevant for vurderingen)

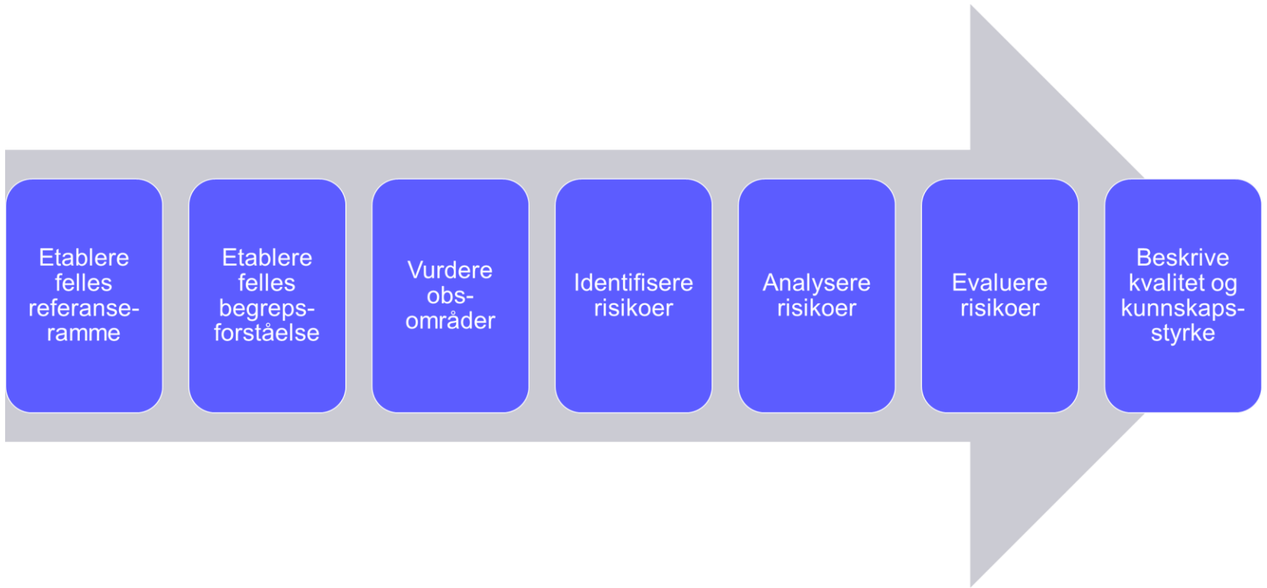
Oversikt:

2. Hvor god oversikt har vi over området?
   - Mål for arbeidet eller tjenesten, system som benyttes og hvem som utfører arbeidet
   - Trusler, farer og sårbarheter

Tidligere risikovurderinger og risikohåndtering:

3. Er det tidligere gjort gode risikovurderinger og en systematisk risikohåndtering på dette eller direkte sammenlignbare områder?
   - av oss eller andre vi har stor tillit til

Gjennomføre risikovurdering



Difi

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

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.

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

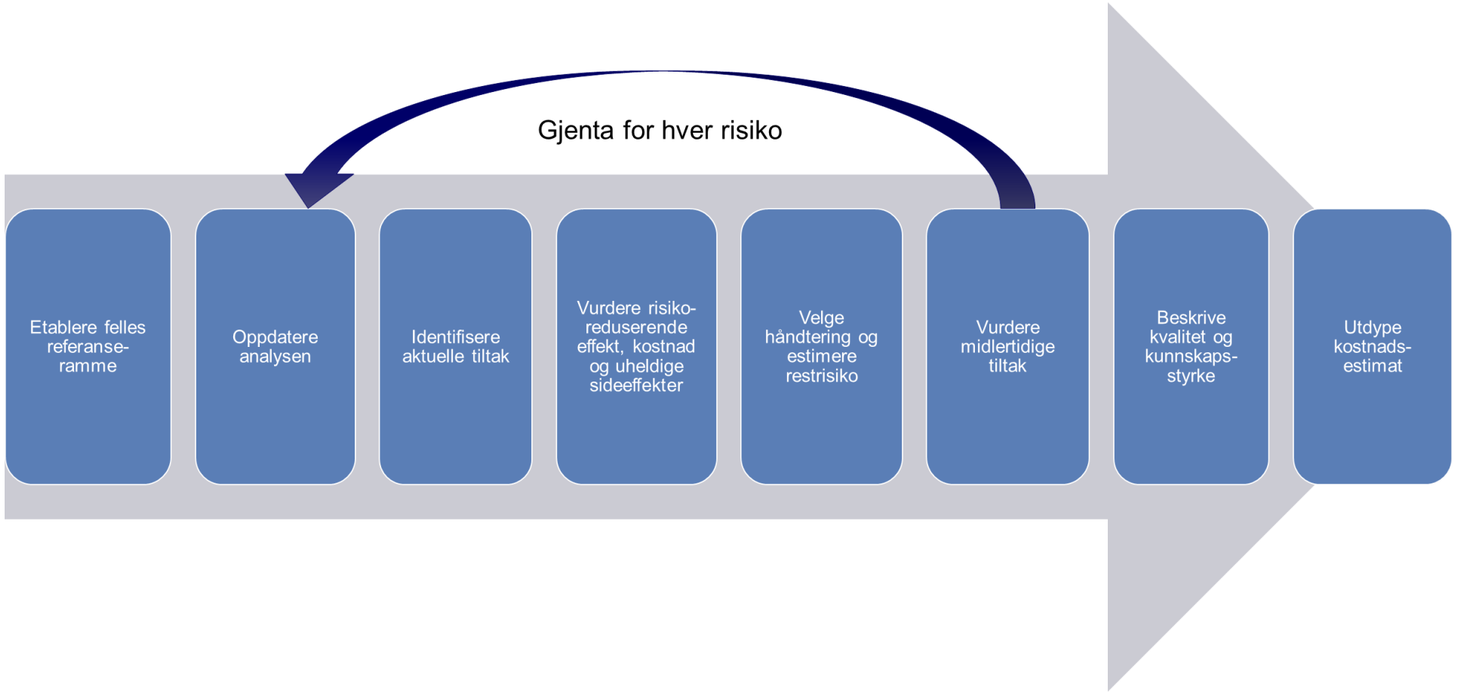
Normerende beskrivelser - sannsynlighetsnivå

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	

Difi

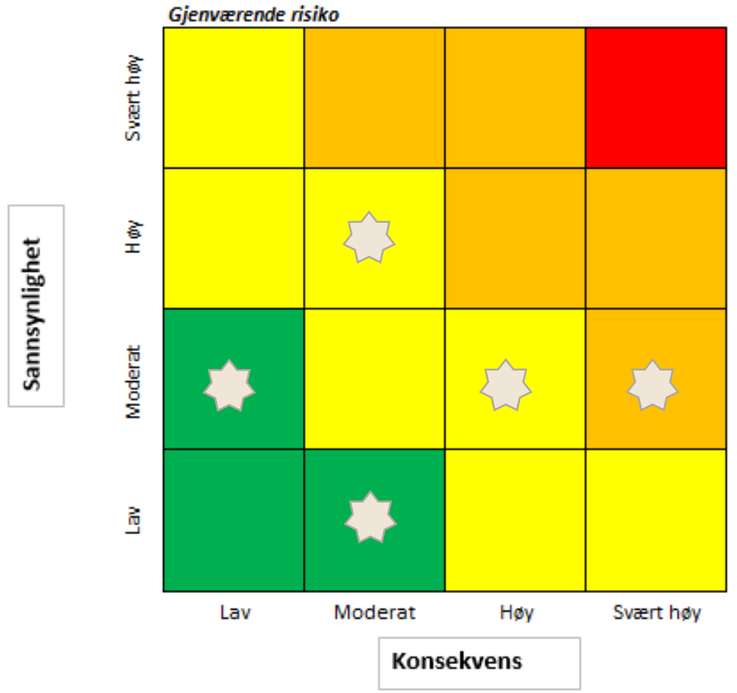
Foreslå håndtering av risiko



Difi

Godkjenne forslag til risikohåndtering

- Vurdere
  - kvaliteten på analysen
  - kunnskapsstyrken
  - restrisiko
  - kost/nytte
  - finansiering
- Involvere andre?
- Ny vurdering?



Difi

Del av retningslinje (eksempel)

Forstå, vurdere og håndtere operativ risiko

Vedlegg B: Kriterier for å akseptere risiko

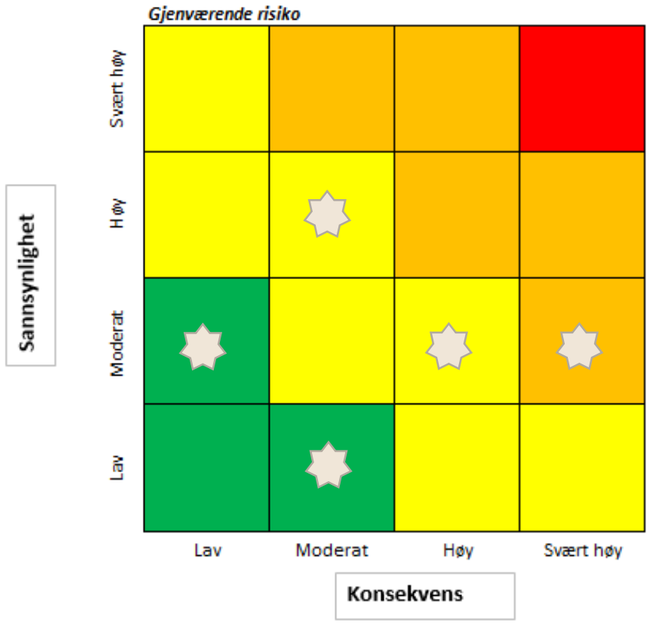
Risikonivå	Kriterier for å akseptere risiko
Lav	Kan aksepteres **uten å lete etter eller vurdere nytten av** alternative arbeidsmåter eller flere risikoreduserende tiltak. Merk at dette gjelder når hele utfallsrommet for en risiko har risikostørrelse på nivå lav innen alle berørte konsekvenskategorier.
	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.

Difi

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.

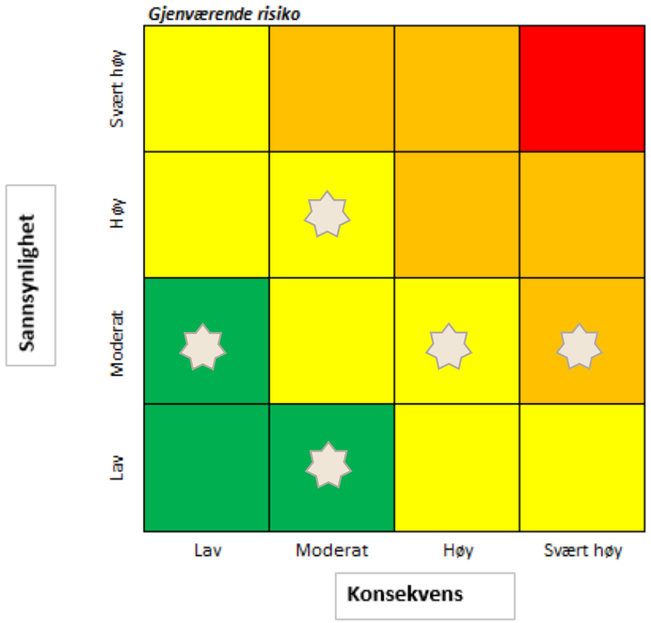
Difi

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.



Difi

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.



Difi

Iverksette godkjente tiltak

- Etablere handlingsplan

Iverksette godkjente tiltak

- Etablere handlingsplan
- Avtale gjennomføring

Iverksette godkjente tiltak

- Etablere handlingsplan
- Avtale gjennomføring
- Godkjenne handlingsplan og avtaler

Iverksette godkjente tiltak

- Etablere handlingsplan
- Avtale gjennomføring
- Godkjenne handlingsplan og avtaler
- Gjennomføre og følge opp

Utforme og implementere tiltakene

- Utforme og sette i verk tiltak
- Teste som avtalt
- Justere ved behov

Følge opp arbeidet

- Etablere handlingsplan
- Avtale gjennomføring
- Godkjenne handlingsplan og avtaler
- Gjennomføre og følge opp
- Håndtere endringer underveis
- Testing og evaluering

Difi

GRUPPEOPPGAVE

Difi

Gruppeoppgave 1

Gjennomføre risikovurdering og foreslå håndtering av risikoer innen informasjonssikkerhet

1. Hvor god er deres virksomheter på dette i dag?
   - Mht.: 1) avklart metode/fremgangsmåte, 2) kompetanse, 3) faktisk gjennomføring
   - Grader gjerne på høy, moderat, lav

2. I hvilken grad er ansvaret og gjennomføringen av risikovurderinger hos dere knyttet til linjelederne (risikoeierne) – dvs. de som er ansvarlige for virksomhetens arbeidsoppgaver?

3. Hva skal til for å ansvarliggjøre og aktivisere linjelederne (risikoeierne) i risikovurderingsarbeidet?

4. Hvordan kan praktiske risikovurderinger i linjen organiseres på en hensiktsmessig og effektiv måte?

Difi

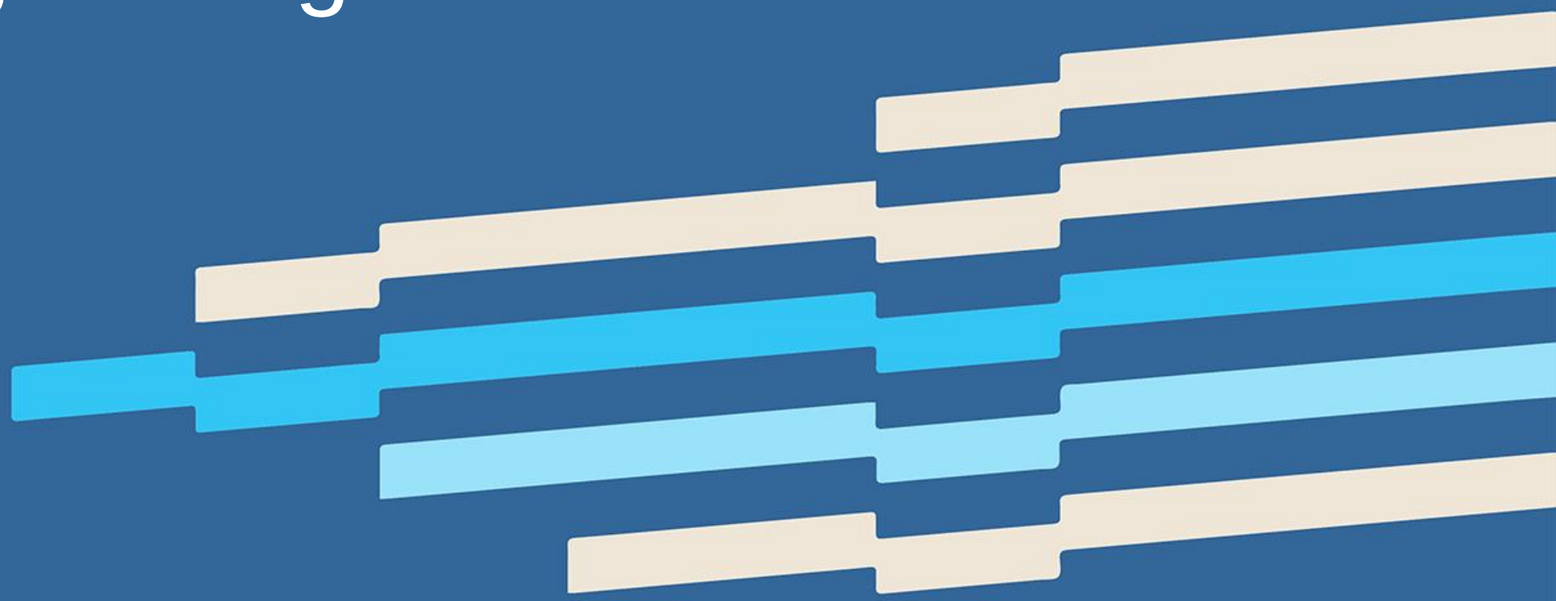
Difi
Direktoratet for
forvaltning og ikt

Økt 12
Oppsummering fra dag 1

—

Innføringskurs

Internkontroll i praksis -
informasjonssikkerhet



Hva er informasjonssikkerhet?

Sikre:

- konfidensialitet
- integritet
- tilgjengelighet

på informasjon som behandles

i tilknytning til våre arbeidsoppgaver

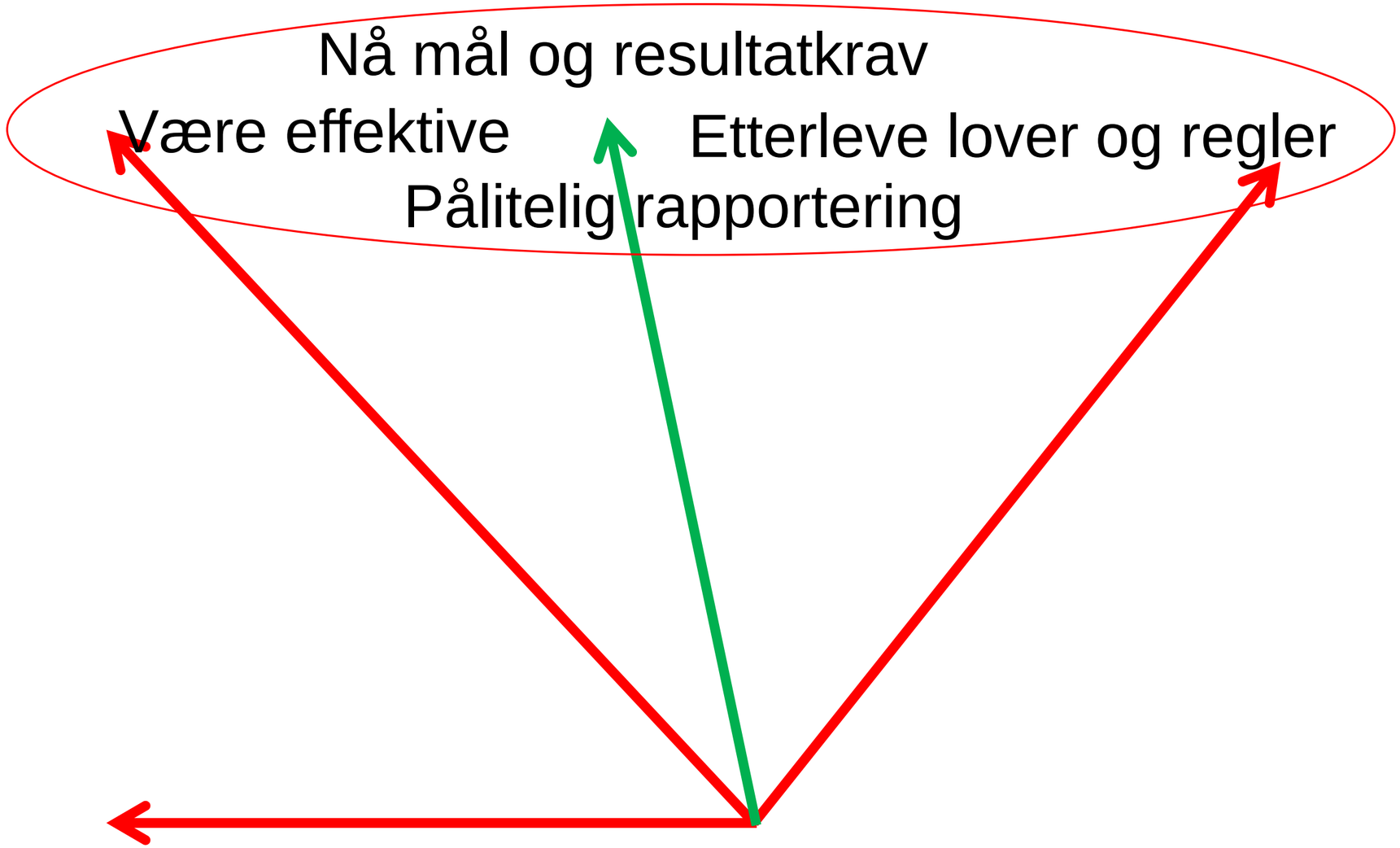
Difi

Hva er informasjonssikkerhet?

- Konfidensialitet
  - Informasjon blir ikke kjent for uvedkommende
- Integritet
  - Informasjon blir ikke endret utilsiktet eller av uvedkommende
- Tilgjengelighet
  - Informasjon er tilgjengelig ved behov

Difi

Hvorfor internkontroll?



Treffer eller bommer vi?

Internkontroll / Styringssystem / Ledelsessystem / ….

- Ulike begrep for det samme
- Det handler om

systematikk og formalisering

for å oppnå

tilstrekkelig

intern

styring og kontroll

slik at vi kan

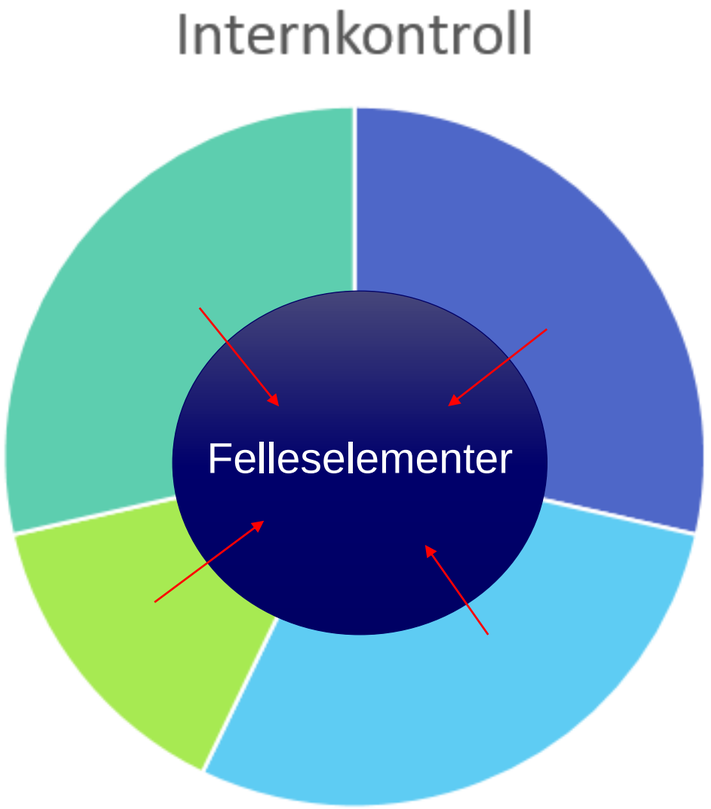
nå målene våre

(nå mål og resultatkrav, være effektive
etterleve lover og regler, ha pålitelig
rapportering)

Difi

Helhetlig internkontroll

Områdespesifikke deler



Omfang av integrering på tvers må tilpasses virksomheten

Difi

Flere har Identifisert «god praksis» for internkontroll (styring og kontroll) i ulike virksomheter

Rammeverk og standarder:

COSO

Internkontroll generelt

ISO

27001 9001 31000 m.m.

Mange områder

BS OHSAS 18001

HMS

++

Veiledninger (konkretiseringer):

Direktoratet for økonomistyring

KS

difi Direktoratet for forvaltning og IKT

Datatilsynet

NSM

dsb Direktoratet for samfunnssikkerhet og beredskap

Arbeidstilsynet Kontroll og veiledning om arbeidsmiljø

Helsedirektoratet

Normen

++

Nødvendig:

Lokal samordning og tilpasning til den enkelte virksomhet sin egenart og historie

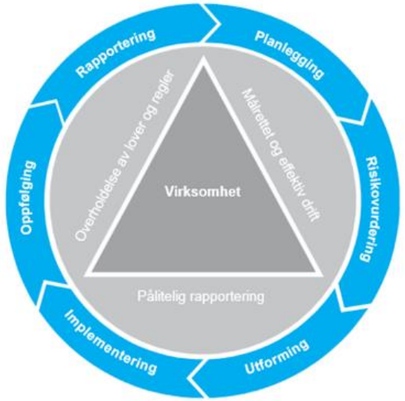
Resultat:

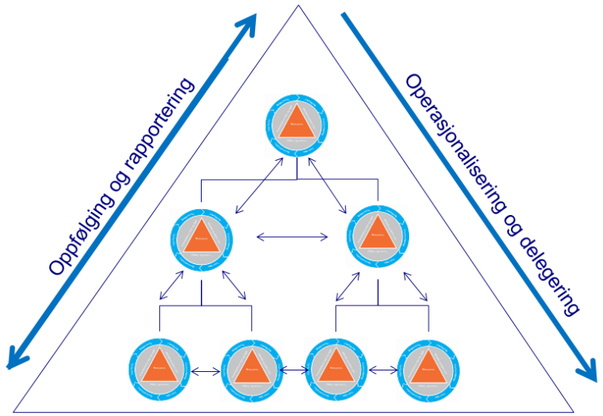
God internkontroll i **vår** virksomhet med kontinuerlig forbedring

Difi

Ulike forklaringsmodeller

DFØ – Staten
Internkontroll generelt





Difi – Stat og kommune
Informasjonssikkerhet

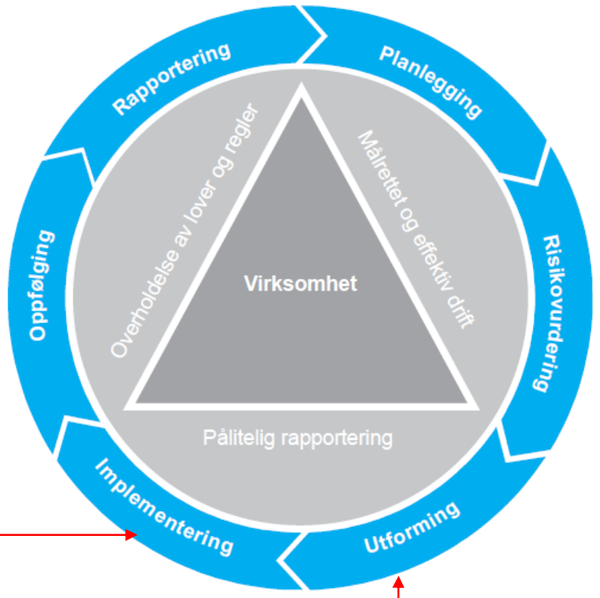
KS – Kommunene
Internkontroll generelt

Difi

Difi vs DFØ veiledningsmateriell

Difis «forklaringsmodell» – internkontroll informasjonssikkerhet

DFØs «metode» – internkontroll generelt



Difi

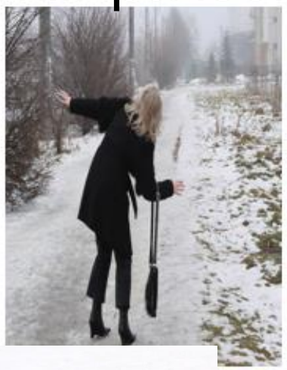
RISIKOFORSTÅELSE

Uønsket hendelse | Risikobeskrivelse | Scenario

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

Liv og helse | Øko-nomi | Tjeneste-nivå

Sklir på isen



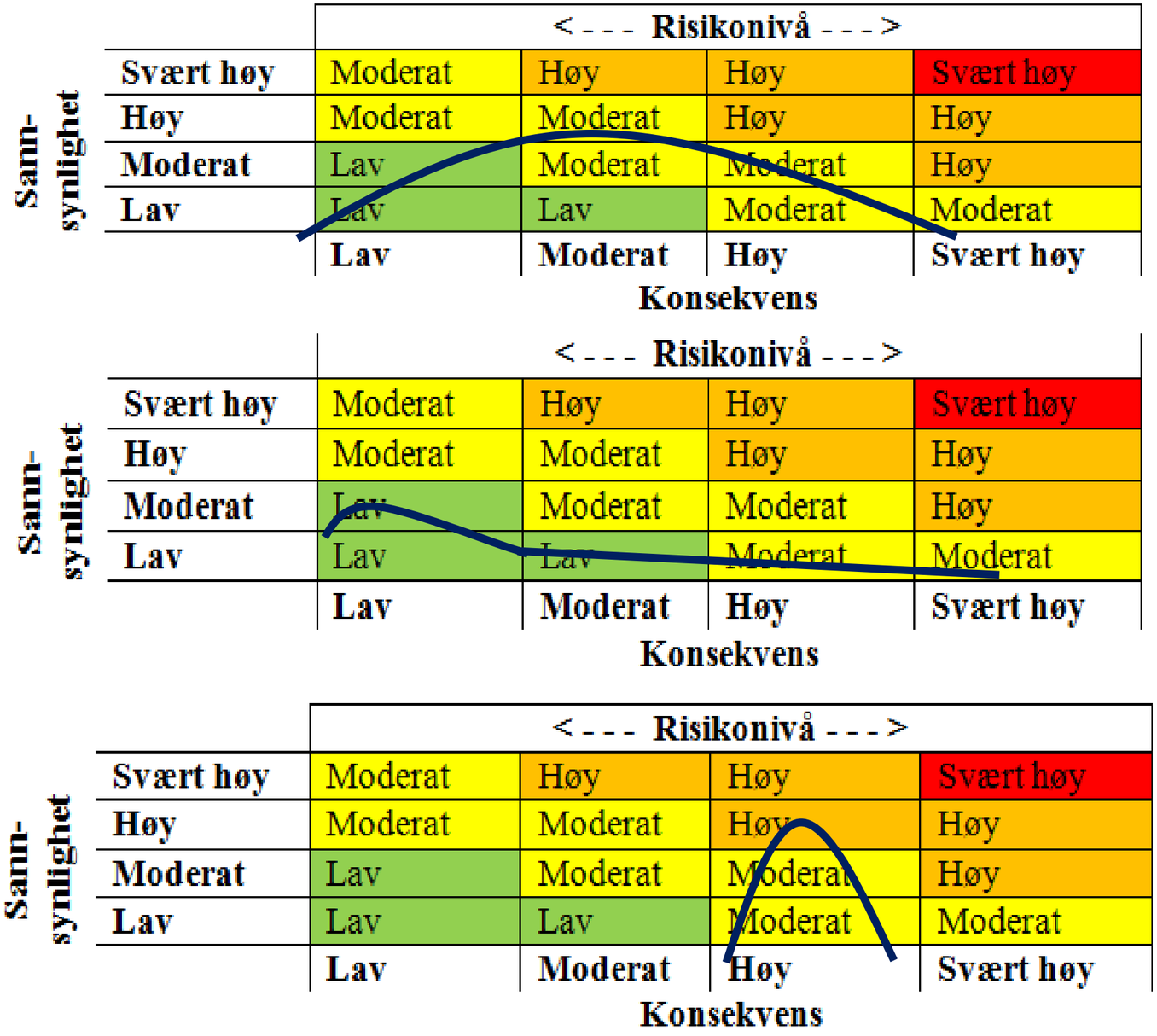
? ?

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

Difi

Sannsynlighetsfordeling på ulike konsekvensnivå

Avhengig av risikobeskrivelsen



Konsekvenskategorier

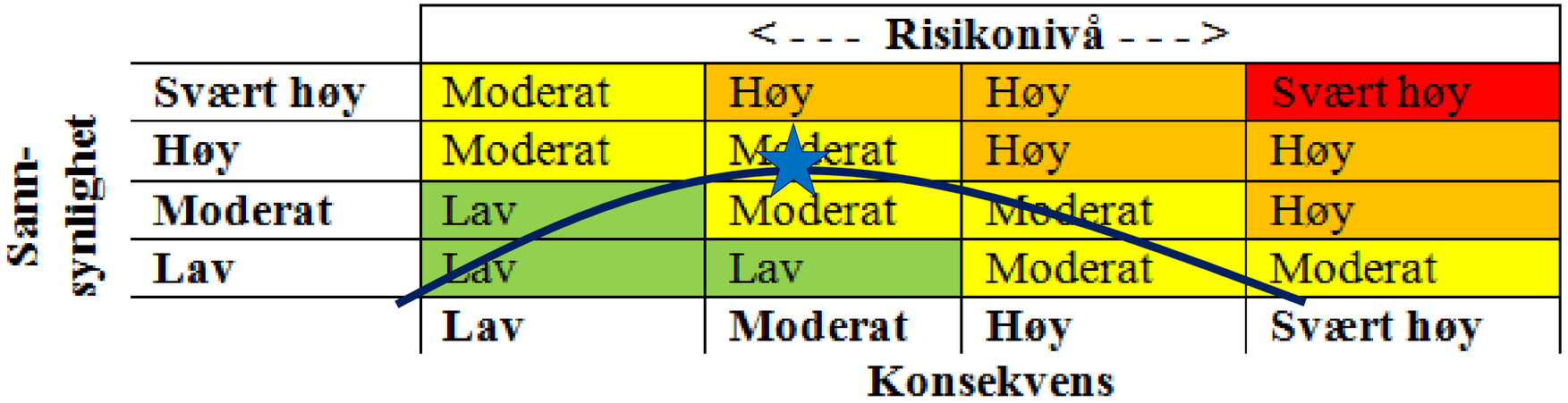
- Er en forenkling og gruppering av våre mål med basis i
  - Nå mål og resultatkrav
  - Ha effektiv ressursbruk
  - Etterleve lover og regler
  - Pålitelig rapportering

Eksempel på konsekvenskategorier
Tjenestenivå
Personvern
HMS
Regelverk (for øvrig)
Vår økonomi
Delmål

Difi

Nivåinndeling på konsekvens, sannsynlighet og risiko

- Er en forenkling for å effektivisere risikovurderinger og kommunikasjon om risiko
  - Vi deler det samlede utfallsrommet opp i ruter og nivå

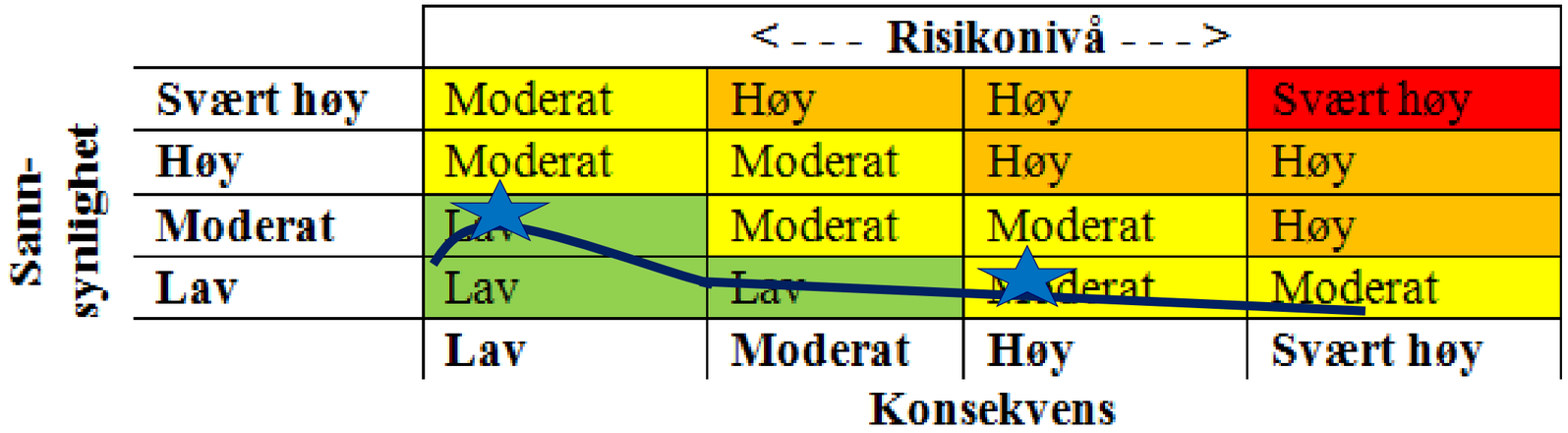


- Vi uttrykker ett av flere mulige utfall /risikoer
  - oftest det mest forventede
  - Selv om risikoene ligger i hele utfallsrommet (under buen)

Difi

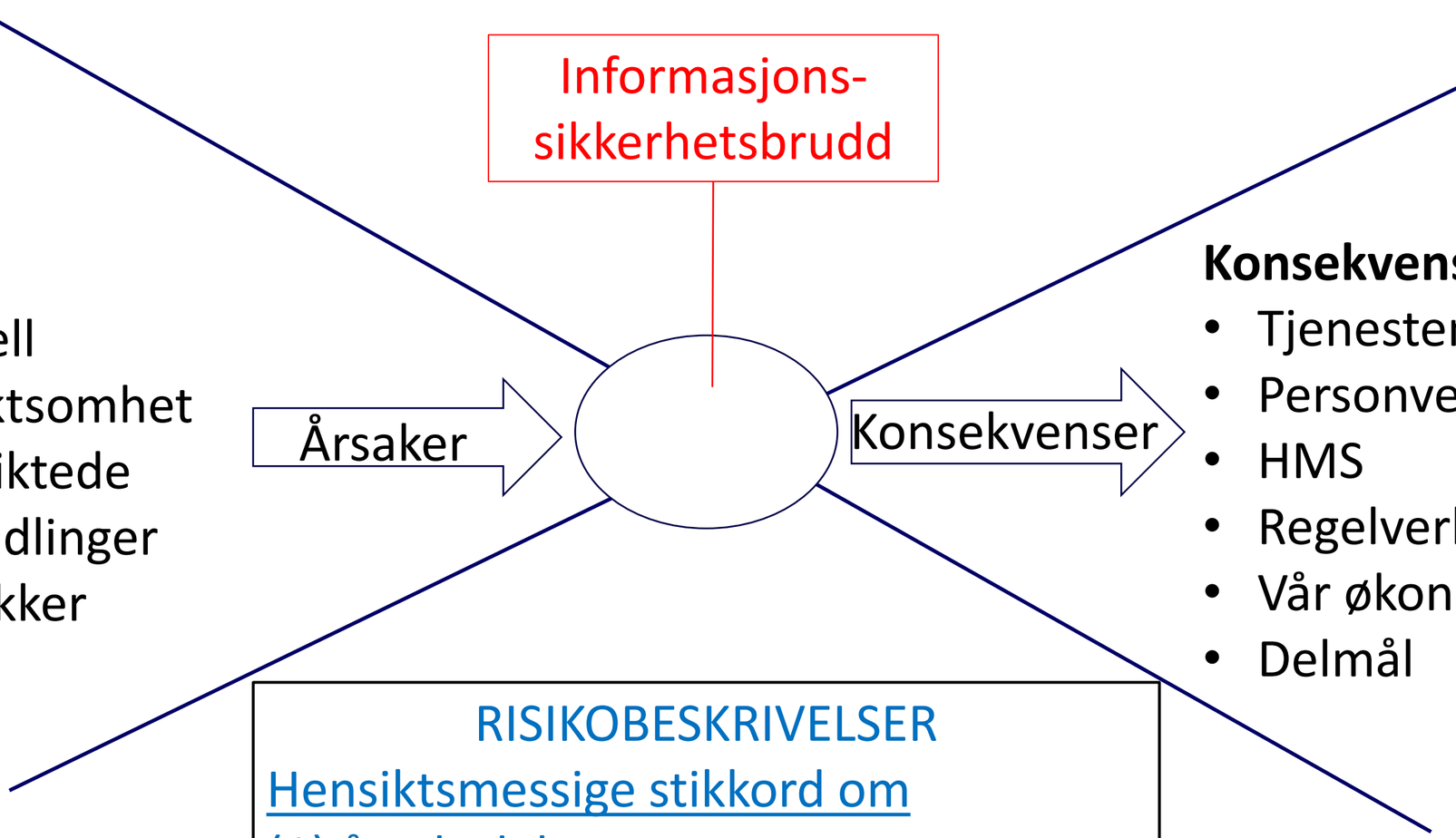
Glem ikke forskjellen på

mest forventet risikonivå og mulige risikonivå (mulige utfall med annen sannsynlighet)



- Spesielt når mest forventet gir risikonivå «Lav»

Formuler helhetlige risikobeskrivelser
Visuell støtte i sløyfediagram



Kilder

- Uhell
- Uaktsomhet
- Tilsiktede handlinger
- Ulykker

Konsekvenskategori

- Tjenestenivå
- Personvern
- HMS
- Regelverk
- Vår økonomi
- Delmål

RISIKOBESKRIVELSER

Hensiktsmessige stikkord om

(1) årsaksdelen

(2) informasjonssikkerhetsbruddet

(3) konsekvensdelen

Difi

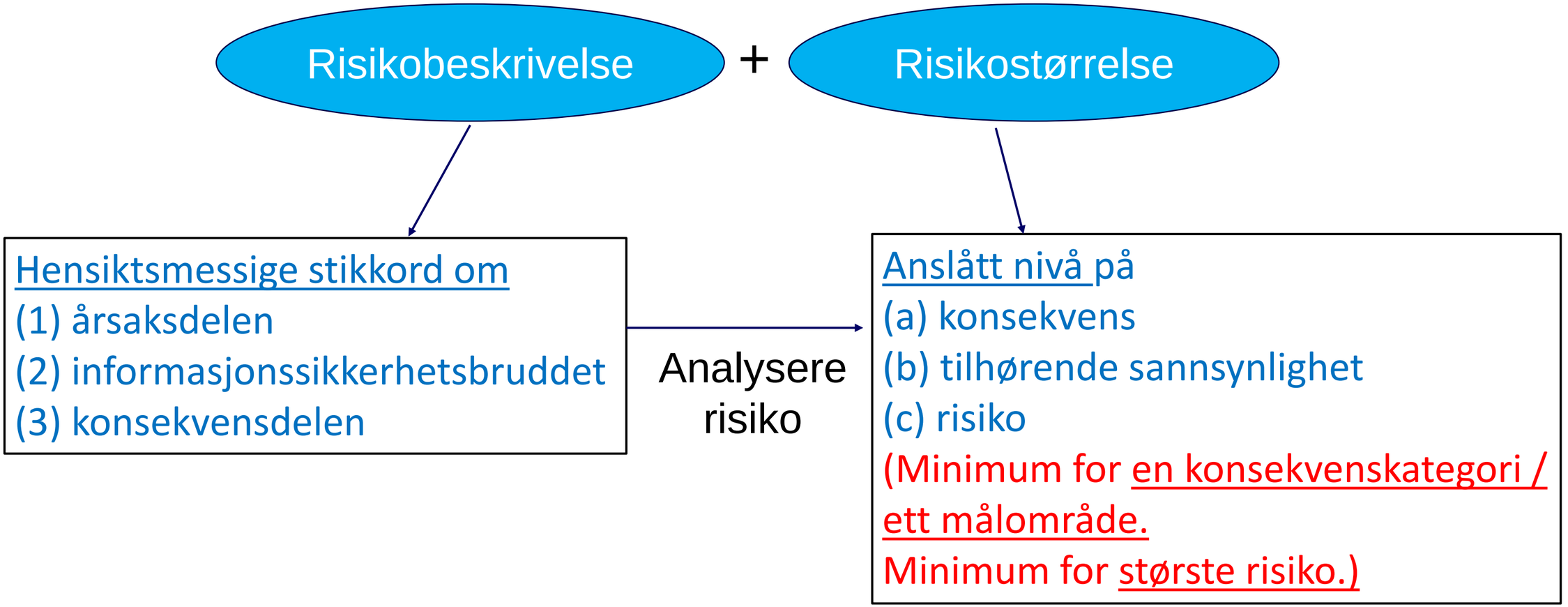
Eksempel på risikobeskrivelser

---------- Hendelse / Risikobeskrivelse / Scenario ----------			
ID	Årsak (1)	Informasjonssikkerhets-brudd (skadestart) (2)	Konsekvensbeskrivelse (3)
1	(1) Ansatte prater om sosialsaker i kantina, naboer til klienter overhører	(2) Brudd på taushetsplikt	(3) Naboer snakker om ting de ikke skulle vite, klienter opplever ubehag, barn utestenges
2	(1) Ansatte legger hemmelige adresser på internett	(2) Hemmelige adresser kommer på avveie	(3) Voldspersoner får fatt i personer med hemmelig adresse, gir personskade
3	(1) Organiserte kriminelle, sosial manipulering av ansatte via ekstern IKT-tilgang	(2) Kriminelle endrer beløp og utbetalings-konto i økonomisystem	(3) Feil utbetalinger, vi taper penger, andre får ikke det de har krav på
4	(1) Ansatte gjør feil	(2) Sletter info i tilskuddssystem	(3) Feil beslutninger og utbetalinger
5	(1) Brann i serverrom	(2) Alle system detter ned	(3) All aktivitet ute av drift, ulik grad av skad

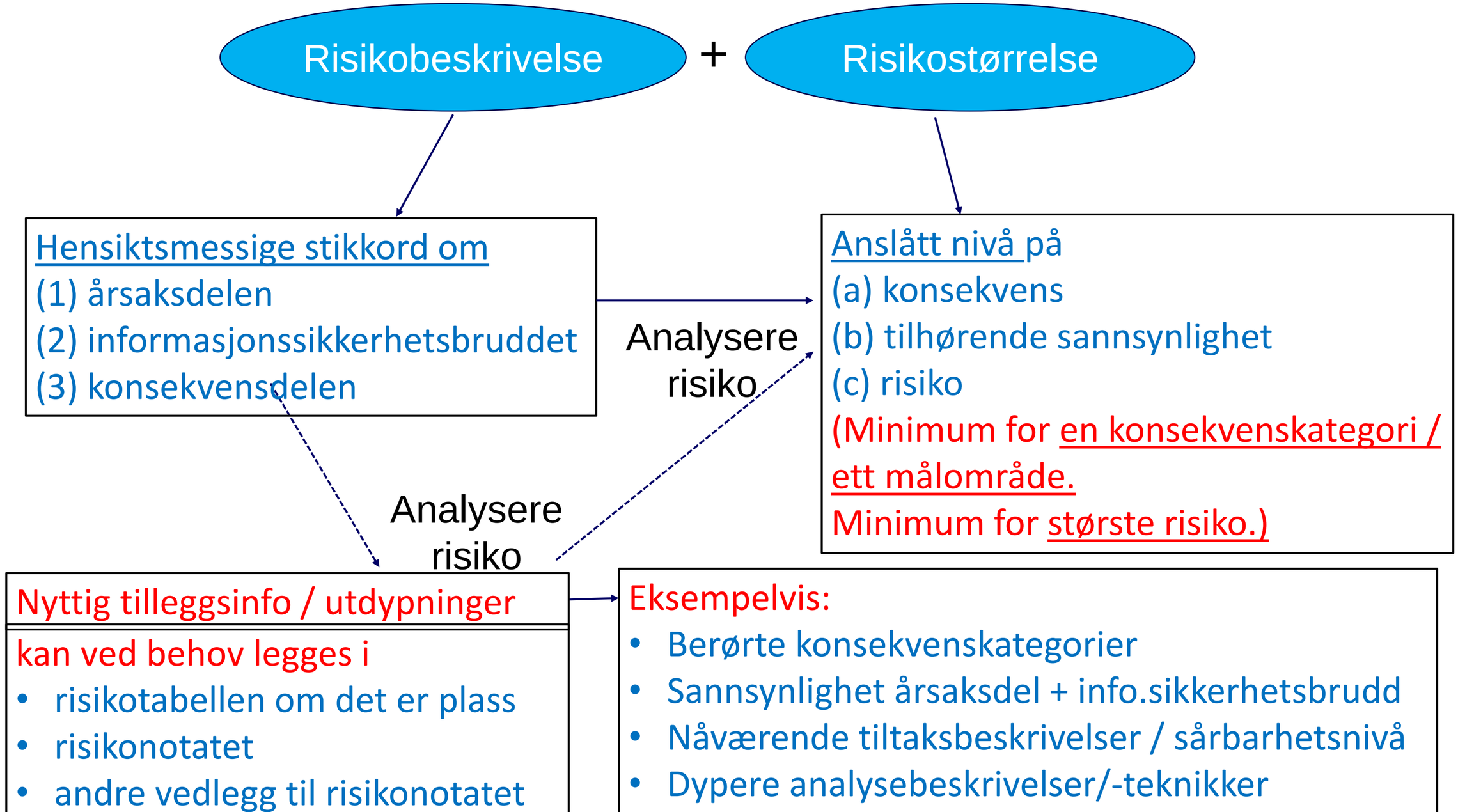
Beskrivelsene kan ha ulikt detaljeringsnivå på alle tre delene avhengig av hva som anses hensiktsmessig

Difi

Uttrykke risiko



Uttrykke risiko



OBS! Sannsynlighet for flere ting

- Husk at det er forskjell på sannsynlighet for
  1. at innledende hendelse skjer
  2. at innledende hendelse skjer og medfører informasjonssikkehetsbrudd (eller annen type målavvik)
  3. at et bestemt konsekvensnivå blir resultatet av pkt. 2

- Pkt. 3 er det vi må bruke for å uttrykke risiko riktig
- Pkt. 2 er ofte nyttig støtte for å komme frem til pkt. 3

Difi

Internkontroll informasjonssikkerhet

FORSKRIFT, STANDARD OG VEILEDNING

eForvaltningsforskriften § 15

- Forvaltningsorganet skal ha en *internkontroll (styring og kontroll)* på informasjonssikkerhets-området som *baserer seg på anerkjente standarder* for styringssystem for informasjonssikkerhet

- Omfang og innretning på internkontrollen skal være *tilpasset risiko*

Standarden ISO/IEC 27001 og Difis veiledningsmateriell

- ISO/IEC 27001
  - er anbefalt standard å basere seg på

- Difis veiledningsmateriell
  - har en pragmatisk og behovsorientert tilnærming til standarden
    - fokus på tilstrekkelig styring og kontroll (ikke sertifisering)
    - baserer seg på standarden
    - dekker det Difi anser som de viktigste kravene
  - konkretiserer hvordan disse kravene kan implementeres og etterleves

Difi

Difis forklaringsmodell

1

- **Analysere** status
- **Planlegge** etablering/forbedring
- Gjennomføre andre **etableringsaktiviteter**

Gjennomføre aktivitetene systematisk

2

Internkontroll-aktiviteter

Difi

1

- **Analysere** status
- **Planlegge** etablering/forbedring
- Gjennomføre andre **etableringsaktiviteter**

Gjennomføre aktivitetene systematisk

2

Internkontroll-aktiviteter

Sikkerhetstiltak

3

Tilleggssikring

Fellessikring

- Instrukser og rutiner
- Avtaler
- Retningslinje for fysisk sikkerhet
- Tilgangsstyring IT-systemer
- Sikkerhetskopiering og gjenoppretting
- Osv.

Difi

Fellessikring og tilleggssikring

- Fellessikring
  - Et sett med sikkerhetstiltak
  - Et felles grunnleggende sikkerhetsnivå for sentrale områder i virksomheten

- Tilleggssikring
  - Ekstra sikkerhetstiltak på oppgaver, system o.l. der noen, men ikke alle, har behov

Difi

Viktige aktører

- Virksomhetsledelsen
- Ledere som delegerer og skal følge opp

- Risikoeiere
- Systemeiere fellessystem
- Tiltaksleverandører

- Utpekt person for lederstøtte og pådriver
  - innen internkontroll informasjonssikkerhet
  - Fagansvarlig informasjonssikkerhet
- Støttepersoner (prosessledere i risikovurderinger o.l.)

Etablering | Systematisk

Etableringsaktiviteter

- Analysere status
- Planlegge etablering | forbedring

- Hjelpeaktiviteter for å lette de systematiske aktivitetene

Etableringsaktiviteter - hjelpeaktiviteter

- Ledelsens styring og oppfølging
  - Utforme overordnede **styrende dokumenter**

- Risikovurdering
  - Identifisering typiske **oppgave- og informasjonstyper**
  - Felles analyse av **eksterne krav**

Systematiske aktiviteter

Ledelsens styring og oppfølging

- Risikovurdering
- Risikohåndtering
- Overvåkning og hendelseshåndtering
- Måling, evaluering og revisjon
- Kompetanse- og kulturutvikling

Kommunikasjon

Difi

Ledelsens styring og oppfølging
- «Hjernen» i internkontrollen

Ledelsens styring og oppfølging

- Virksomhetsledelsens gjennomgang
- Delegere og følge opp gjennom linjen
- Sikre finansielle rammer for internkontroll- og sikkerhetsarbeidet
- Kommunisere viktighet
- Håndtere problemstillinger løftet gjennom linjen
- Krise- og beredskapshåndtering

Risikovurdering
- «Hjertet» i internkontrollen

Ledelsens styring og oppfølging

- Risikovurdering
- Risikohåndtering
- Overvåkning og hendelseshåndtering
- Måling, evaluering og revisjon
- Kompetanse- og kulturutvikling

Kommunikasjon

Difi

Risikovurdering

- Få oversikt og prioritere
- Analysere eksterne krav
- Planlegge risikovurdering
- Gjennomføre risikovurdering
- Spesielle situasjoner:
  - Risikovurdere i hendelseshåndteringen
  - Risikovurdere ved anskaffelser og utvikling

Difi

Delaktiviteten

Få oversikt og prioritere

- Foranalyse
  - Identifisere arbeidsoppgaver, informasjonstyper, system mv.
  - Anslå potensielt konsekvensnivå
  - Vurdere trusler, farer og sårbarheter
  - Oppsummere spesielle obs-områder
- Gruppere og dele opp
- Vurdere behov for risikovurderinger
- Oversikt over risikovurderinger
- Oppdateringer

Risikovurdering

- Få oversikt og prioritere
- Analysere eksterne krav
- Planlegge risikovurdering
- Gjennomføre risikovurdering
- Spesielle situasjoner:
  - Risikovurdere i hendelseshåndteringen
  - Risikovurdere ved anskaffelser og utvikling

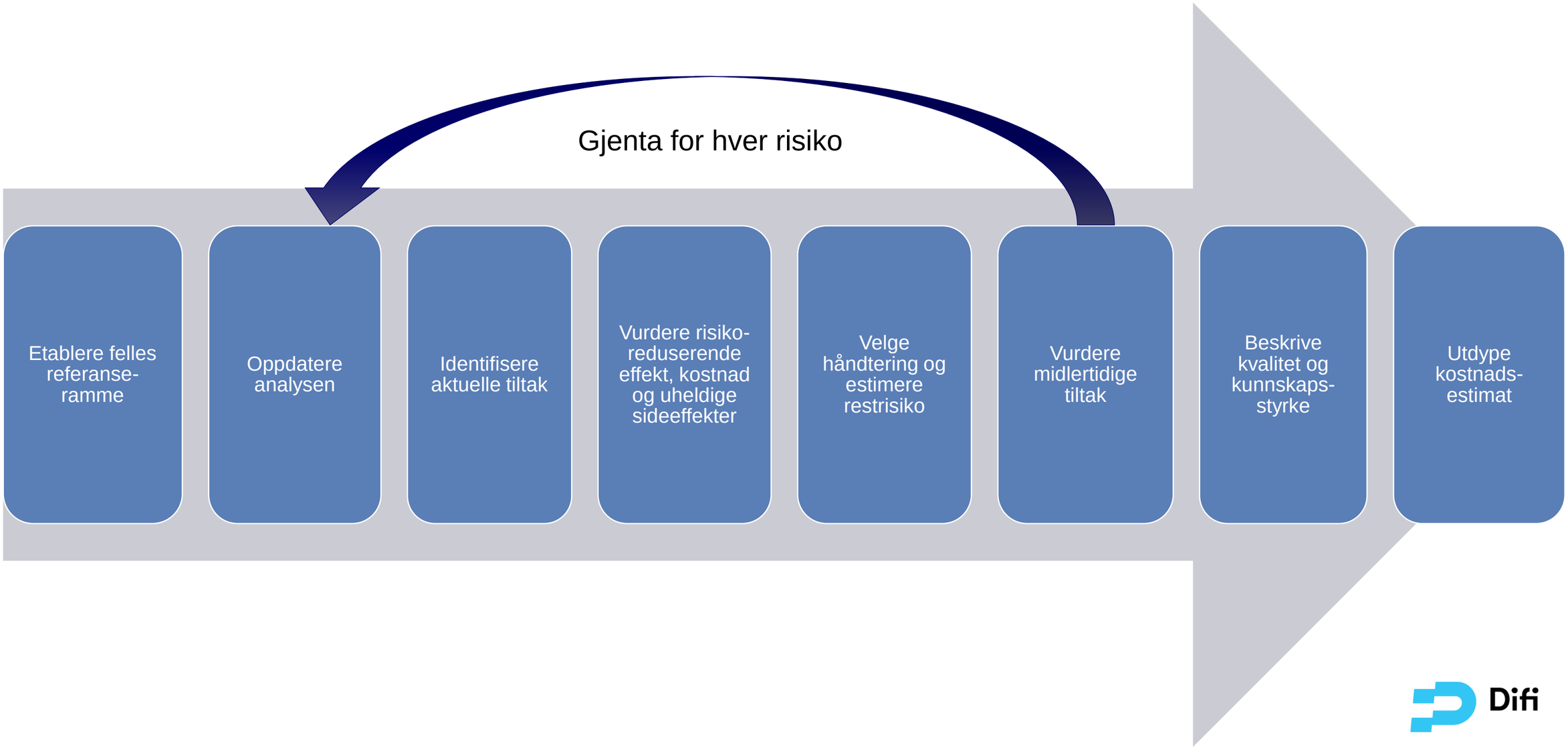
Gjennomføre risikovurdering

Risikohåndtering
- «Hendene» i internkontrollen

Risikohåndtering

- Foreslå håndtering av risikoer
- Godkjenne forslag til risikohåndtering
- Iverksette godkjente tiltak
- Utforme og implementere tiltakene
- Oppdatere fellessikringen

Foreslå håndtering av risikoer



Godkjenne forslag

- Analysens kvalitet
- Kunnskapsstyrke
- Restrisiko
- Kost/nytte
- Finansiering
- Involvere andre?
- Ny vurdering?

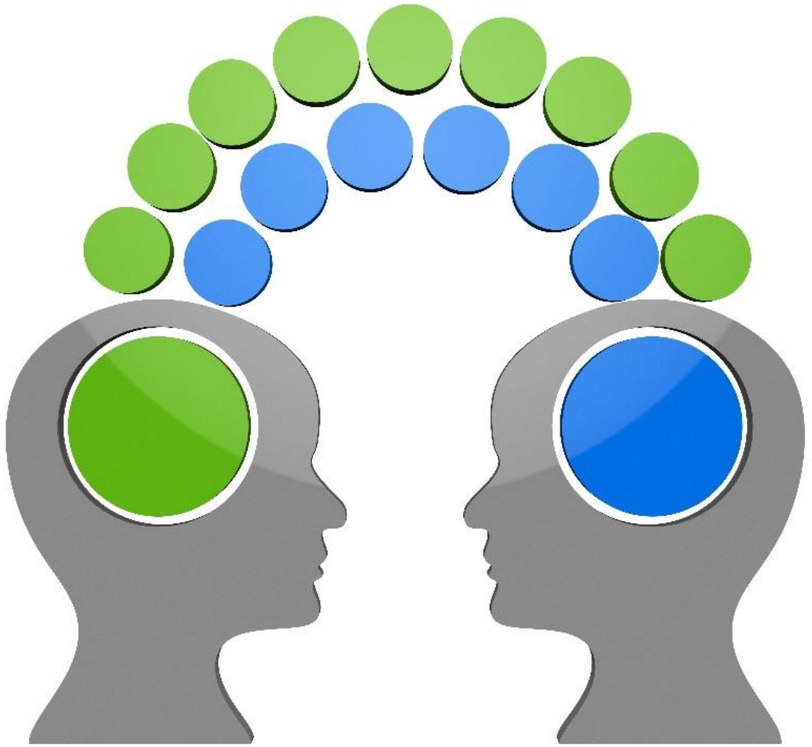
Iverksette tiltak

- Utføres av: Håndteringsansvarlig
- Handlingsplan for gjennomføring | etablering av godkjente tiltak
- Plan utformes i dialog med de som skal gjennomføre
  - Inkl. gjøre avtaler med tiltaksleverandører
- Handlingsplan bør godkjennes av risikoeier
- Håndteringsansvarlig følger opp
  - inkl. nødvendig rapportering

Risikohåndtering

- Foreslå håndtering av risikoer
- Godkjenne forslag til risikohåndtering
- Iverksette godkjente tiltak
- Utforme og implementere tiltakene
- Oppdatere fellessikringen

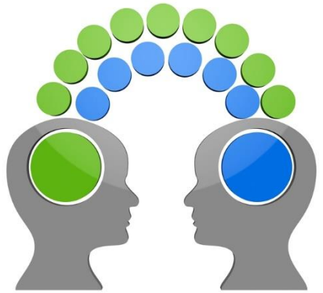
Difi



REFLEKSJONSOPPGAVE

Difi

Refleksjonsoppgave 4



Diskuter i hvilken grad delaktivitetene under gjennomføres hos dere i dag – innen informasjonssikkerhet. Bruk vurderingskodene (0 - 4) på side 1 i oppgavearkene.

Risikohåndtering

- Foreslå håndtering av risikoer
- Godkjenne forslag til risikohåndtering
- Iverksette godkjente tiltak
- Utforme og implementere tiltakene

Difi

Difi
Direktoratet for
forvaltning og ikt

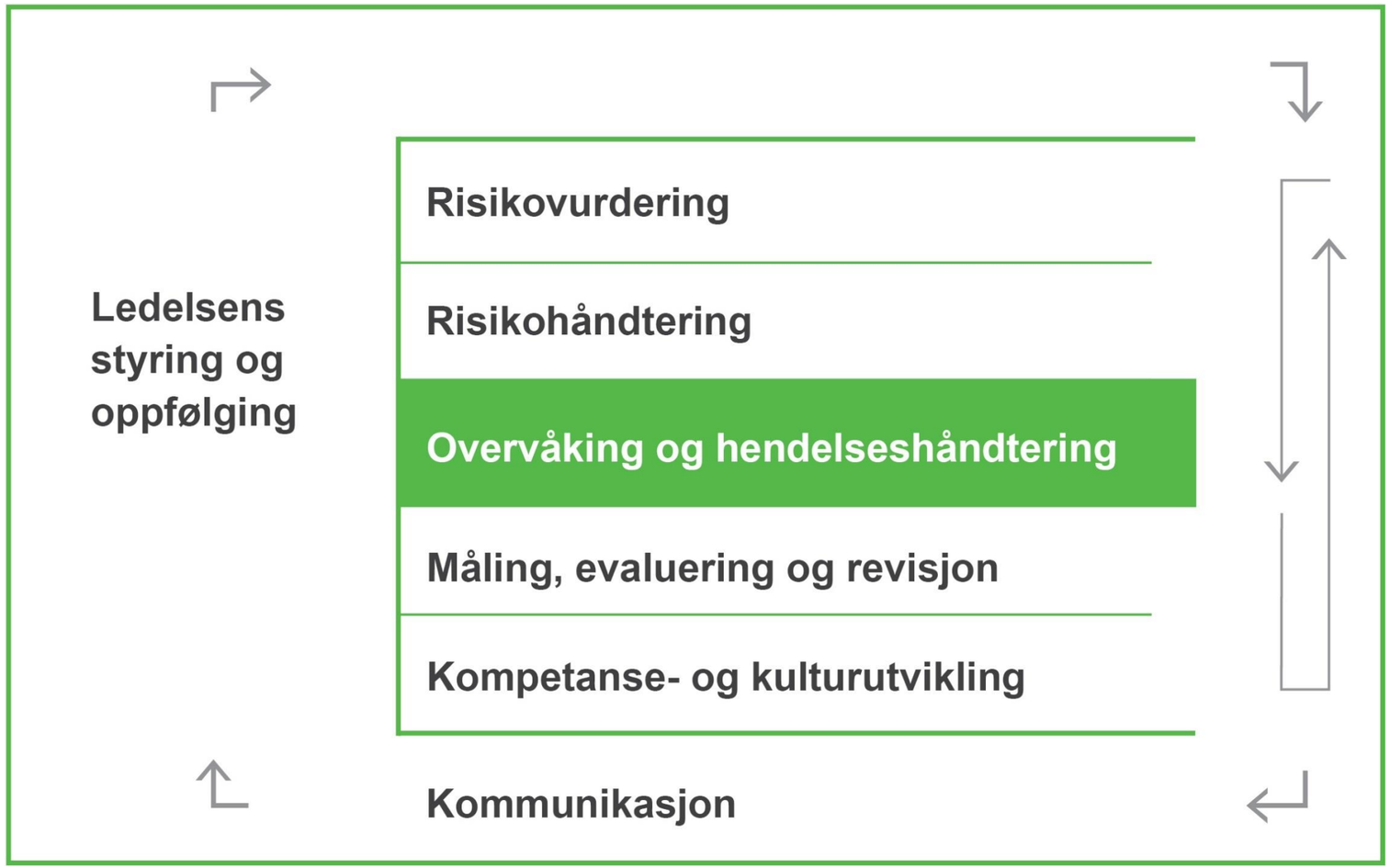
Økt 13
Overvåking og hendelseshåndtering

—

Innføringskurs

Internkontroll i praksis -
informasjonssikkerhet

Overvåking og hendelseshåndtering
- «Vakta» i internkontrollen



Difi

Etableringsaktivitet

Etablere system for hendelses- og avvikshåndtering

- Formål – oppdage og håndtere hendelser så effektivt som mulig for å
  - lettere kunne unngå informasjonssikkerhetsbrudd
  - redusere konsekvensene
  - lære av erfaringer

Overvåking og hendelseshåndtering

SYSTEMATISKE AKTIVITETER

Difi

Overvåking og hendelseshåndtering - delaktiviteter

- Overvåke i henhold til avtale
- Rapportere hendelser, avvik og informasjons-sikkerhetsbrudd
- Følge opp hendelser, avvik og informasjons-sikkerhetsbrudd

Overvåke i henhold til avtale

- Overvåking er et sikkerhetstiltak
  - Identifiseres og velges etter risikovurderinger
  - Kan gjelde
    - fysiske områder
    - tekniske komponenter
    - logger
    - etc.
- Beskrivelsen av tiltaket definerer:
  - Hva som skal overvåkes
  - Hvordan overvåkingen skal skje
  - Når og hvordan uønskede hendelser skal rapporteres

Difi

Rapportere hendelser og avvik

- Systemet for hendelses- og avvikshåndtering bør omfatte krav om
  - hva som skal rapporteres
  - hvem som skal rapportere
  - hvordan rapporteringen skal skje
  - hvem som skal håndtere hva

Følge opp hendelser

- Håndtere uønskede hendelser så effektivt som mulig
- Informasjonsflyt for ulike typer hendelser bør være klart definert
- Håndterte hendelser brukes til læring
  - Må risiko revurderes?
  - Bør sikkerhetstiltak justeres?
  - Grunnlag i fremtidige risikovurderinger

Difi
Direktoratet for
forvaltning og ikt

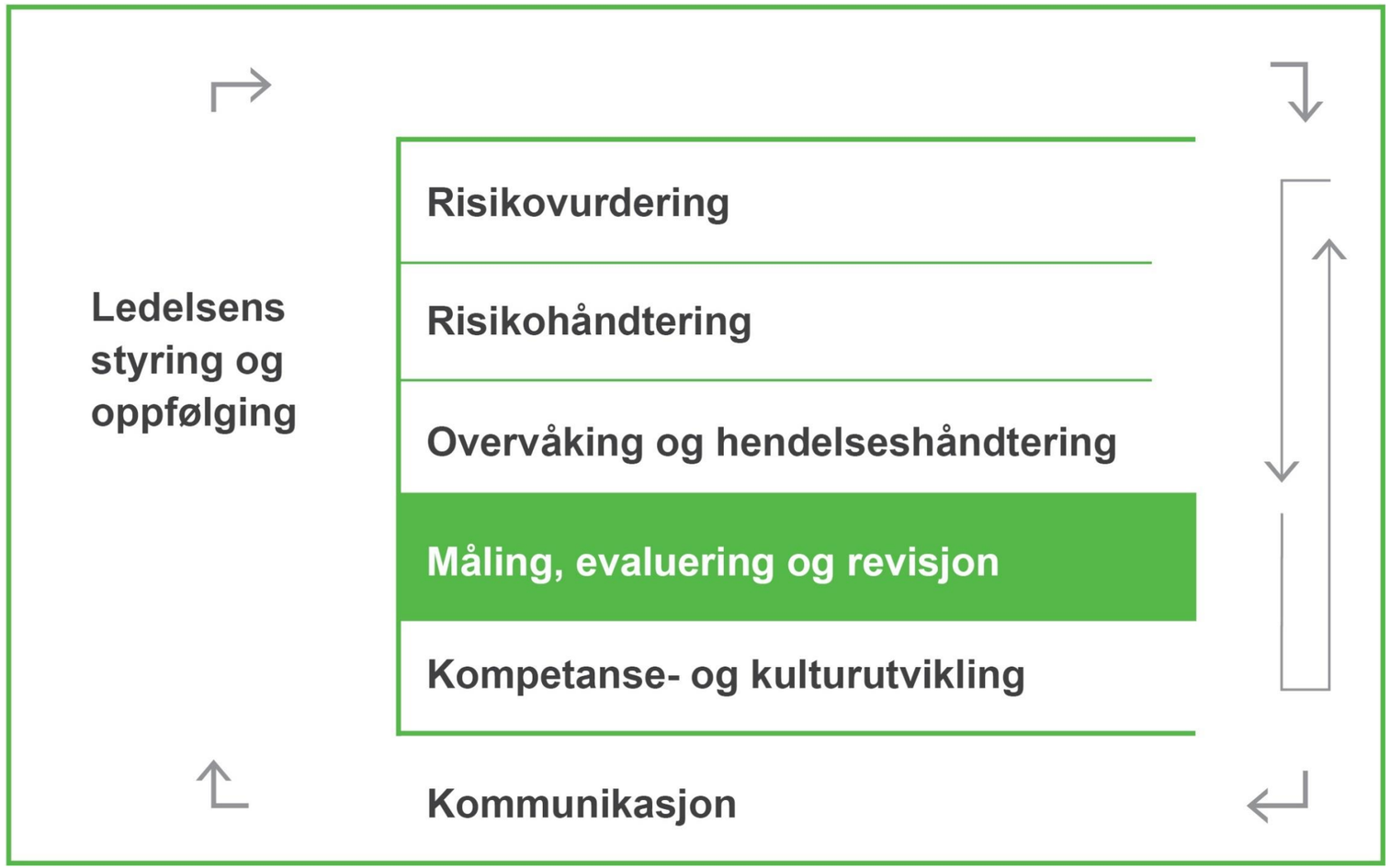
Økt 14
Måling, evaluering og revisjon

—

Innføringskurs

Internkontroll i praksis -
informasjonssikkerhet

Måling, evaluering og revisjon
- «Kontrolløren» i internkontrollen



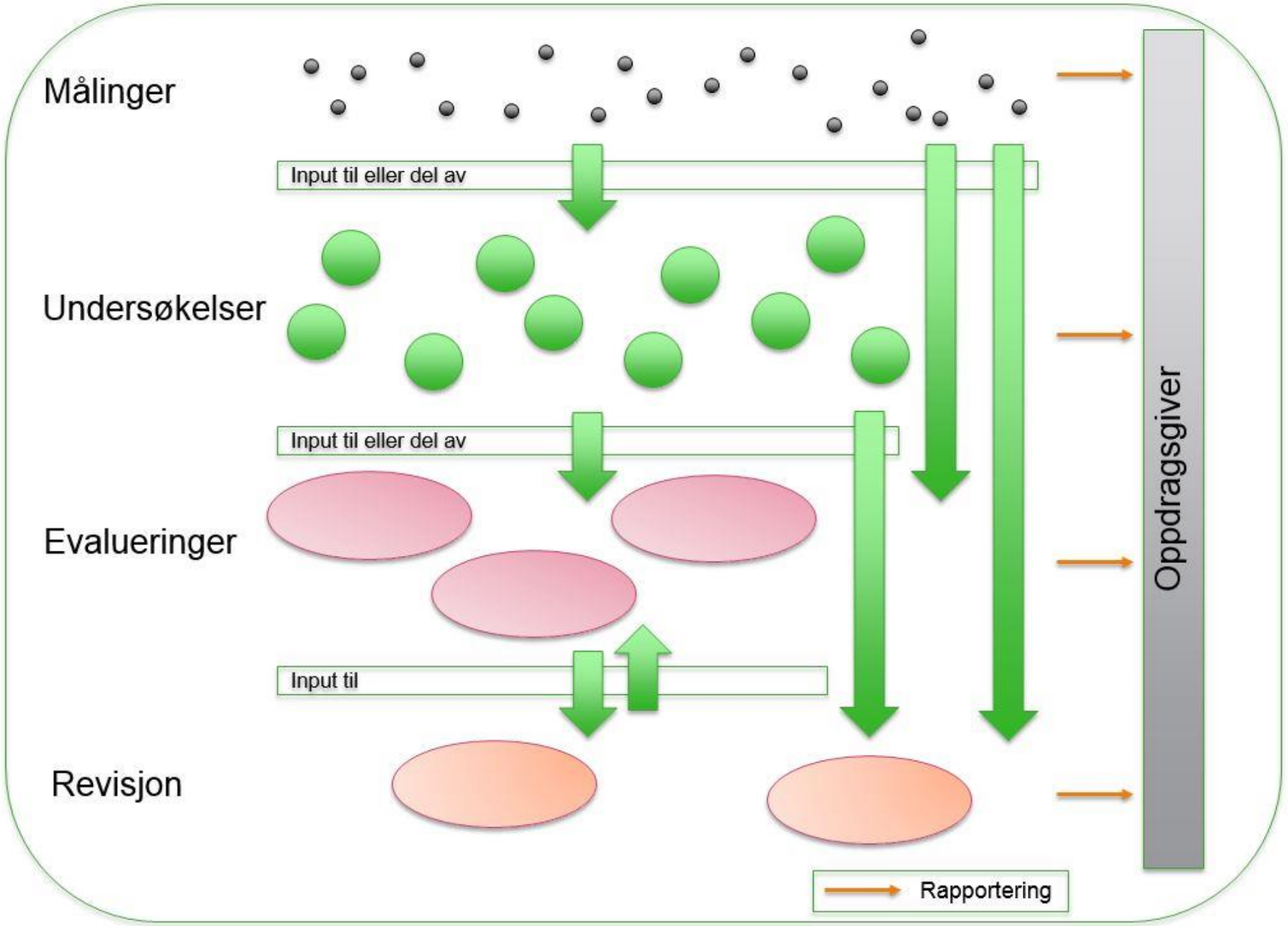
Difi

Begrep og sammenhenger

- Måling
  - Innhenting av data
  - Kan gjøres gjennom ulike teknikker
- Undersøkelser
  - Vurderinger av en tilstand
  - Kvantitative og kvalitative metoder
- Evaluering
  - Systematisk datainnsamling, analyse og vurdering
  - Fellestrekk med, men mer omfattende enn undersøkelser
- Revisjon
  - I vår sammenheng klare fellestrekk med evalueringer
  - Følge anerkjente retningslinjer eller revisjonsstandarder
  - Objektivitet og upartiskhet er svært viktig

Difi

Begrep og sammenhenger



Måling, evaluering og revisjon

SYSTEMATISKE AKTIVITETER

Måling, evaluering og revisjon

Delaktiviteter

- Vurdere status på eget ansvarsområde

- Måle tilstanden på definerte indikatorer
- Gjennomføre evalueringer
- Gjennomføre internrevisjon

Måling, evaluering og revisjon

- Noe er viktig å få gjennomført systematisk hos mange i virksomheten
  - Vurdere status på eget ansvarsområde
- Noe er i hovedsak styrt av behov og beslutninger fra virksomhetsledelsen gjennomgang
  - Måle tilstanden på definerte indikatorer
  - Gjennomføre evalueringer
  - Gjennomføre internrevisjon
- Gjennomføre evalueringer – kan også være:
  - Krav fra departement
  - Regelverkskrav om «systemrevisjoner» e.l.

Difi

Delaktiviteten

Vurdere status på eget ansvarsområde

- Hvem skal gjøre det?
  - ledere som delegerer og skal følge opp gjennom linjen
  - risikoeiere og systemeiere fellessystem
  - tiltaksleverandører
  - ansvarlige for tjenestenivåavtaler eller andre avtaler
  - ansvarlige for egne deler av internkontrollaktivitetene, som f.eks. hendelseshåndteringssystemet og internrevisjon

Delaktiviteten

Vurdere status på eget ansvarsområde

- Statusvurderingen skal omfatte vurderinger av om man selv, egne ansatte og leverandører
  - følger gjeldende lov- og regelverk
  - gjennomfører internkontrollaktivitetene slik man er pålagt
  - etablerer og følger opp vedtatte eller avtalte sikkerhetstiltak
  - etterlever gjeldende sikkerhetstiltak

Vurdere status på eget ansvarsområde

Eksempler - ansvarlige og vurderinger

Ledere som delegerer
Blir pålagte oppgaver faktisk utført av de under meg?

Risikoeiere og systemeier fellessystem
Er kvalitetene på våre foranalyser gode nok?
Blir risikovurderinger og forslag til håndtering fulgt opp?
Blir godkjente forslag til håndtering fulgt opp?
Blir vi informert ved informasjonssikkerhetsbrudd som angår oss?
Har vi tilfredsstillende hedelseshåndtering hos oss?

Tiltaksleverandører
Er avtalte tiltak implementert?
Blir implementerte tiltak gjennomført / fulgt opp som avtalt?
Fungerer tiltakene som forutsatt / avtalt?

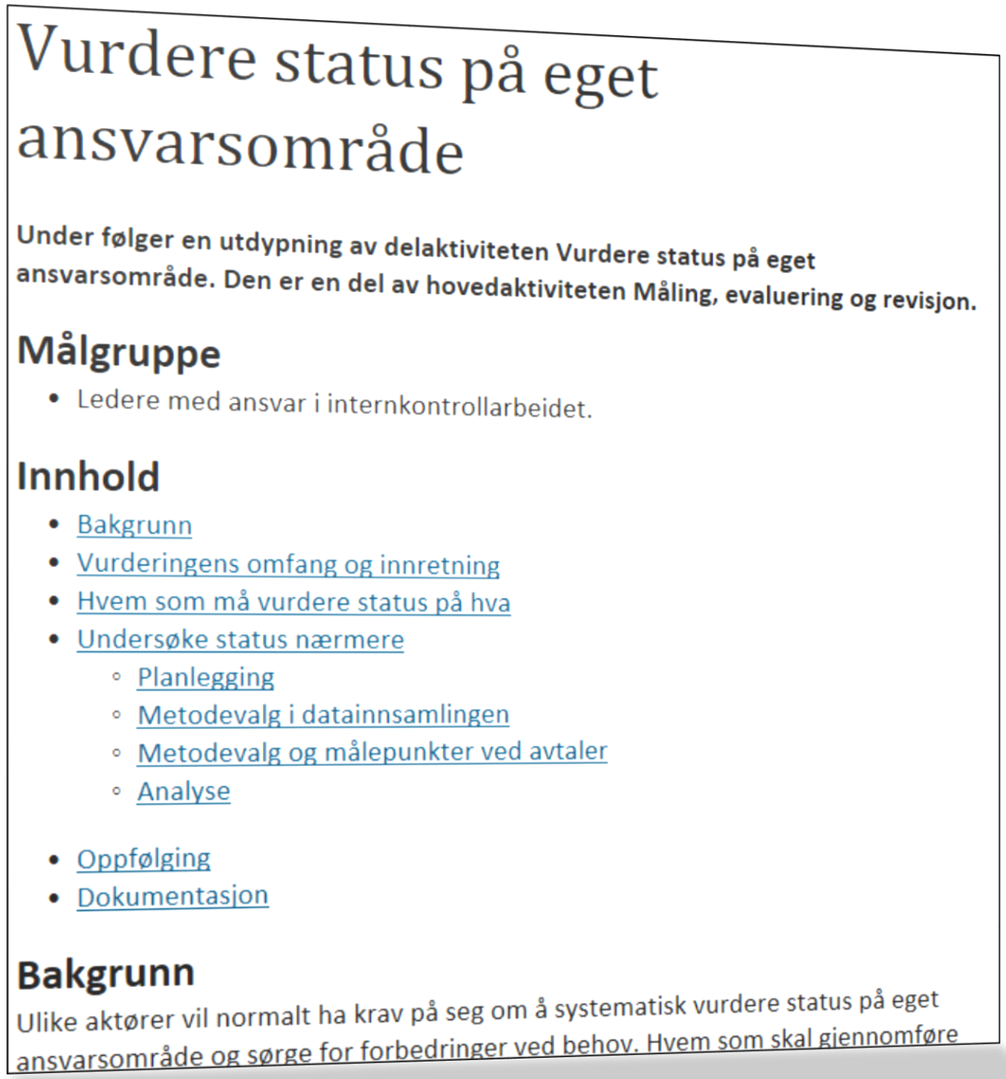
Vurdere status på eget ansvarsområde

Forslag til gjennomføring

- Vurdere egen tillit til at status er tilfredsstillende
  - Lav, moderat, høy
  - Kan være forskjellig for ulike deler av ansvarsområdet
- Gjennomføre undersøkelser ved lav/moderat tillit
  - Enkle kan man gjøre selv
  - Tidkrevende eller metodisk og teknisk kompliserte, kan man engasjere noen til
- Rapportere avvik
  - Dersom det er krav om det
- Forbedre systematisk
  - Slik at ting fungerer og tilliten økes til et tilfredsstillende nivå
- Dokumentere vurdering og undersøkelser
  - Kort notat

Difi

Utdypende veiledning



Vurdere status på eget ansvarsområde

Under følger en utdypning av delaktiviteten Vurdere status på eget ansvarsområde. Den er en del av hovedaktiviteten Måling, evaluering og revisjon.

Målgruppe

- Ledere med ansvar i internkontrollarbeidet.

Innhold

- Bakgrunn
- Vurderingens omfang og innretning
- Hvem som må vurdere status på hva
- Undersøke status nærmere
  - Planlegging
  - Metodevalg i datainnsamlingen
  - Metodevalg og målepunkter ved avtaler
  - Analyse
- Oppfølging
- Dokumentasjon

Bakgrunn

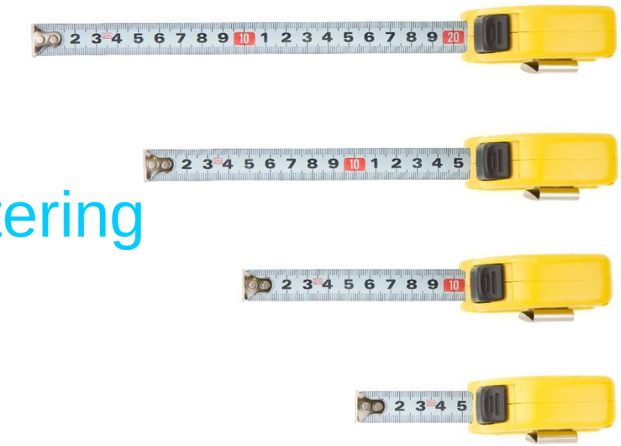
Ulike aktører vil normalt ha krav på seg om å systematisk vurdere status på eget ansvarsområde og sørge for forbedringer ved behov. Hvem som skal gjennomføre

Delaktiviteten

Måle tilstanden på definerte indikatorer

- Gjennomføres dersom virksomhetsledelsen vil følge sikkerhetstilstanden over tid

- Etablere et system
  - med relevante måleindikatorer
  - krav til systematisk måling og rapportering



Måle tilstanden på definerte indikatorer

Eksempler - aktuelle områder og indikatorer

Konfidensialitet
Klager
Innbrudd - fysisk i kontor, arkiv - digitalt generelt, i sosialsystem
Holdning hos ansatte

Integritet
Klager
Innbrudd - fysisk i kontor, arkiv - digitalt generelt, i tilskuddssystem
Holdning hos ansatte

Tilgjengelighet
Nedetid på ulike digitale systemer
Opplevelse av nedetid - hos ansatte - hos eksterne brukere
Opplevelse av hvor lett det er å gjøre jobben med god nok kvalitet

Difi

Delaktiviteten

Gjennomføre evalueringer

- Oftest bestilt av virksomhetsledelsen
  - Kan også gjennomføres / bestilles av risikoeiere og systemeiere fellessystem
- Bakgrunn
  - En overordnet risikovurdering
  - Usikkerhet om viktige deler i internkontrollen fungerer godt nok
  - Krav fra departement
  - Krav i regelverk (f.eks. «sikkerhetsrevisjoner»)
  - m.m.
- Kan utføres av både interne og eksterne fagmiljø
  - Kompetanse, ressurser og behov for uavhengighet påvirker valget

Difi

Eksempel

Etableringsaktiviteten

Analysere status

Delaktiviteten

Gjennomføre internrevisjon

- Bestilt av virksomhetsledelsen

- Formål: få en formell vurdering av
  - om virksomheten følger bestemte krav
  - om kravene er implementert og vedlikeholdt på en formåls- og kostnadseffektiv måte

- Kravene kan være
  - virksomhetens egne retningslinjer
  - kravene i ISO/IEC 27001
  - bestemte lovkrav
  - kombinasjoner

Nødvendig?

- For sertifisering etter ISO/IEC 27001, ja
  - En revisjon må da følge kravene i standardens kapittel 9.2

- For å basere seg på standarden, nei
  - Mer uformelle evalueringer kan da være gode alternativ

Evalueringer og internrevisjon

- Virksomhetsledelsen bør systematisk vurdere behovet
  - og ved behov sørge for gjennomføring
  - Naturlig tema i Virksomhetsledelsens gjennomgang

- Risikoeiere og systemeiere fellessystem
  - Må være oppmerksom på krav om «sikkerhetsrevisjoner» o.l., og følge opp slike på hensiktsmessig måte
  - Med stort ansvarsområde og stor usikkerhet kan ordinære evalueringer være aktuelt for dem også

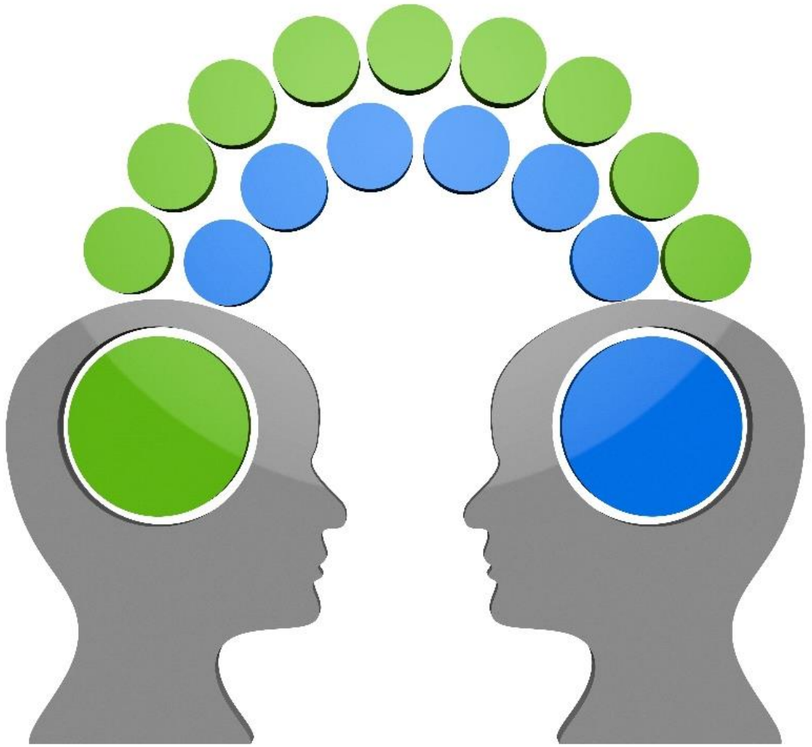
Difi

Måling, evaluering og revisjon

Delaktiviteter

- Vurdere status på eget ansvarsområde

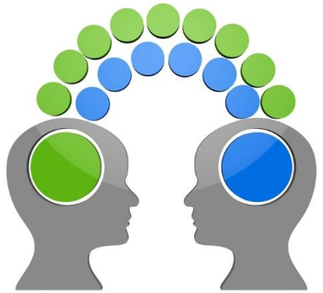
- Måle tilstanden på definerte indikatorer
- Gjennomføre evalueringer
- Gjennomføre internrevisjon



REFLEKSJONSOPPGAVE

Difi

Refleksjonsoppgave 5



1: Velg noen av delaktivitetene under og diskuter i hvilken grad de gjennomføres hos dere i dag – innen informasjonssikkerhet. Bruk vurderingskodene (0 - 4) på side 1 i oppgavearkene.

Måling, evaluering og revisjon

- Vurdere status på eget ansvarsområde
- Måle tilstanden på definerte indikatorer
- Gjennomføre evalueringer
- Gjennomføre internrevisjon

2: Har dere andre områder internt dere kan lære av?

Difi

Difi
Direktoratet for
forvaltning og ikt

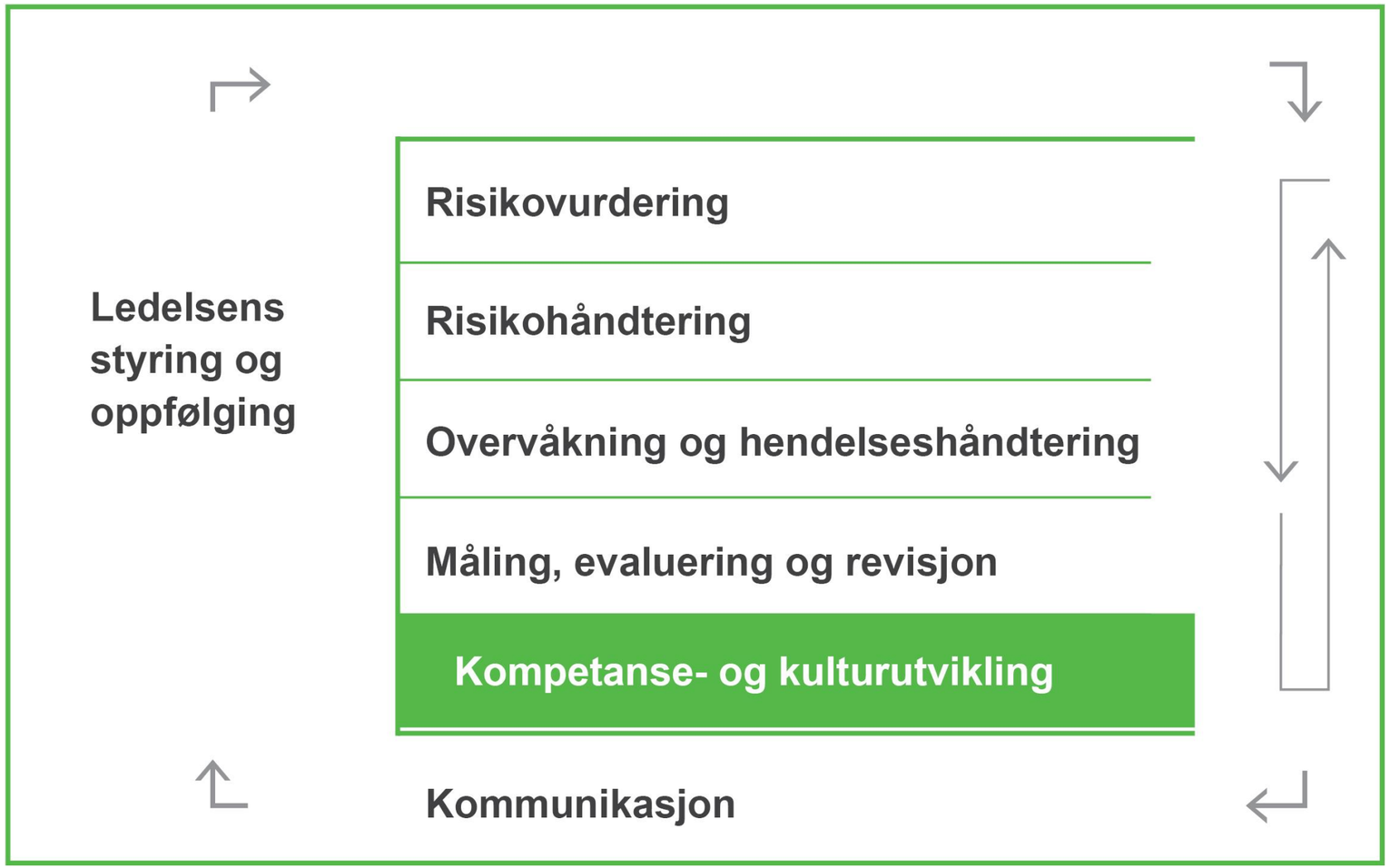
Økt 15
Kompetanse- og kulturutvikling

—

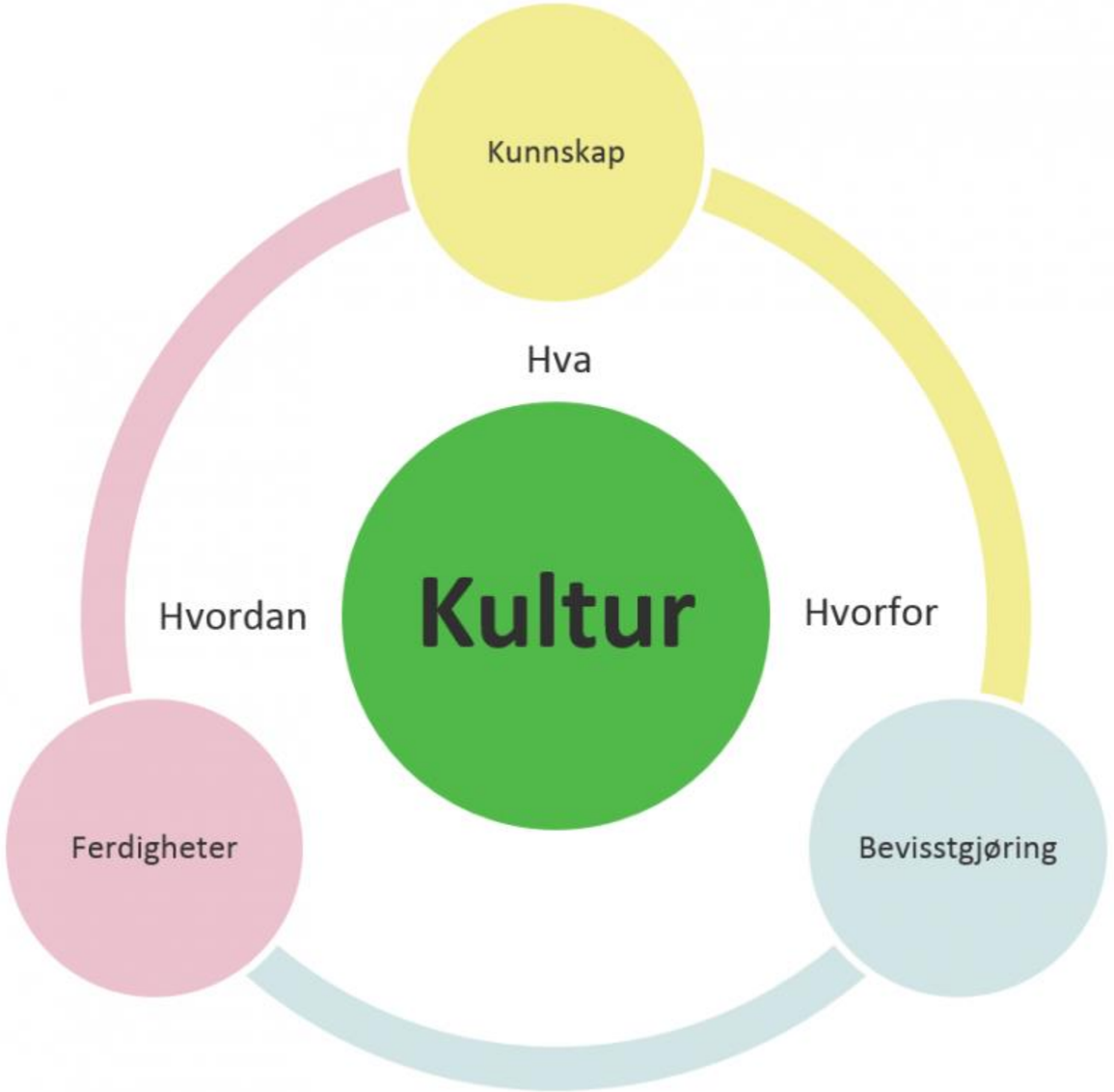
Innføringskurs

Internkontroll i praksis -
informasjonssikkerhet

Kompetanse- og kulturutvikling
- «Læreren» i internkontrollen



Difi


Kunnskap
Hva
Hvordan
Kultur
Hvorfor
Ferdigheter
Bevisstgjøring

Difi

Etableringsaktivitet

Etablering → Grunnopplæring

- Når overordnede styrende dokumenter er ferdige
- Utforme informasjonsmateriell eller kort kurs for ledere

Etableringsaktivitet

Grunnopplæring for ledere

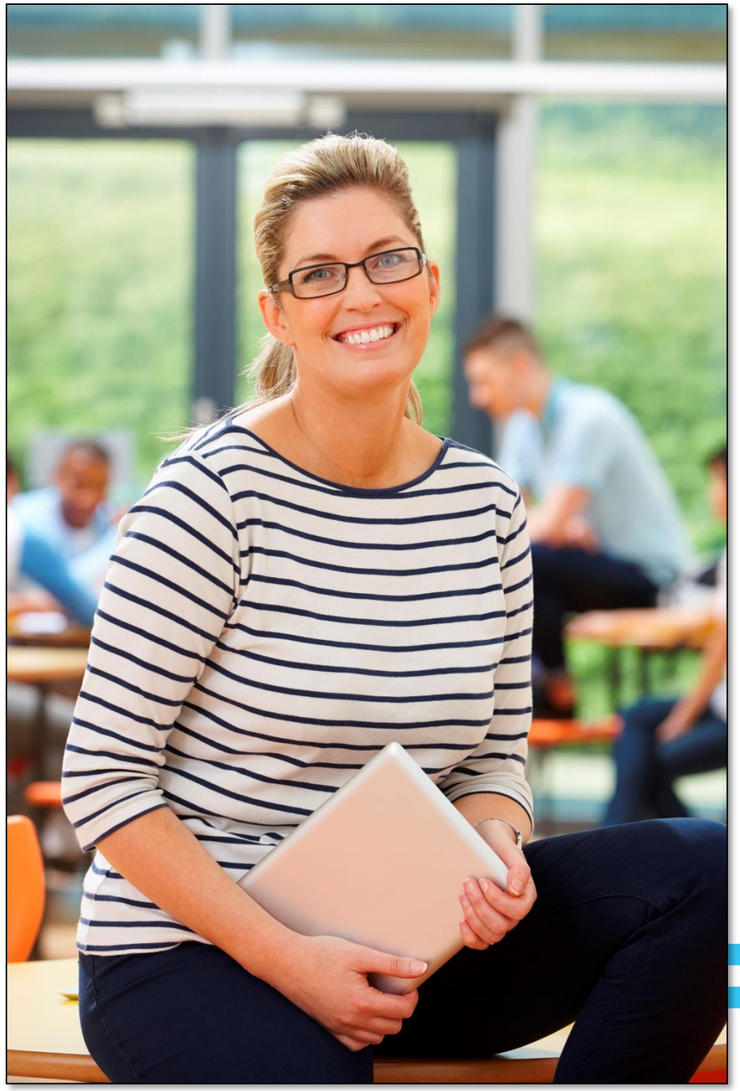
- Hvorfor informasjonssikkerhet og internkontroll er viktig
- Betydningen av innholdet i overordnede styrende dokumenter
- Lederes ansvar og oppgaver
- Hvordan de kan organisere arbeidet lokalt
- Hvor de kan finne utdypende hjelp og støtte til gjennomføring av oppgaver

Difi

Etableringsaktivitet

Annen tilpasset grunnopplæring

- Prosessledere for
  - risikovurdering
  - foreslå håndtering av risikoer
- Håndteringsansvarlige
- Alle ansatte



Difi

Kompetanse- og kulturutvikling

SYSTEMATISKE AKTIVITETER

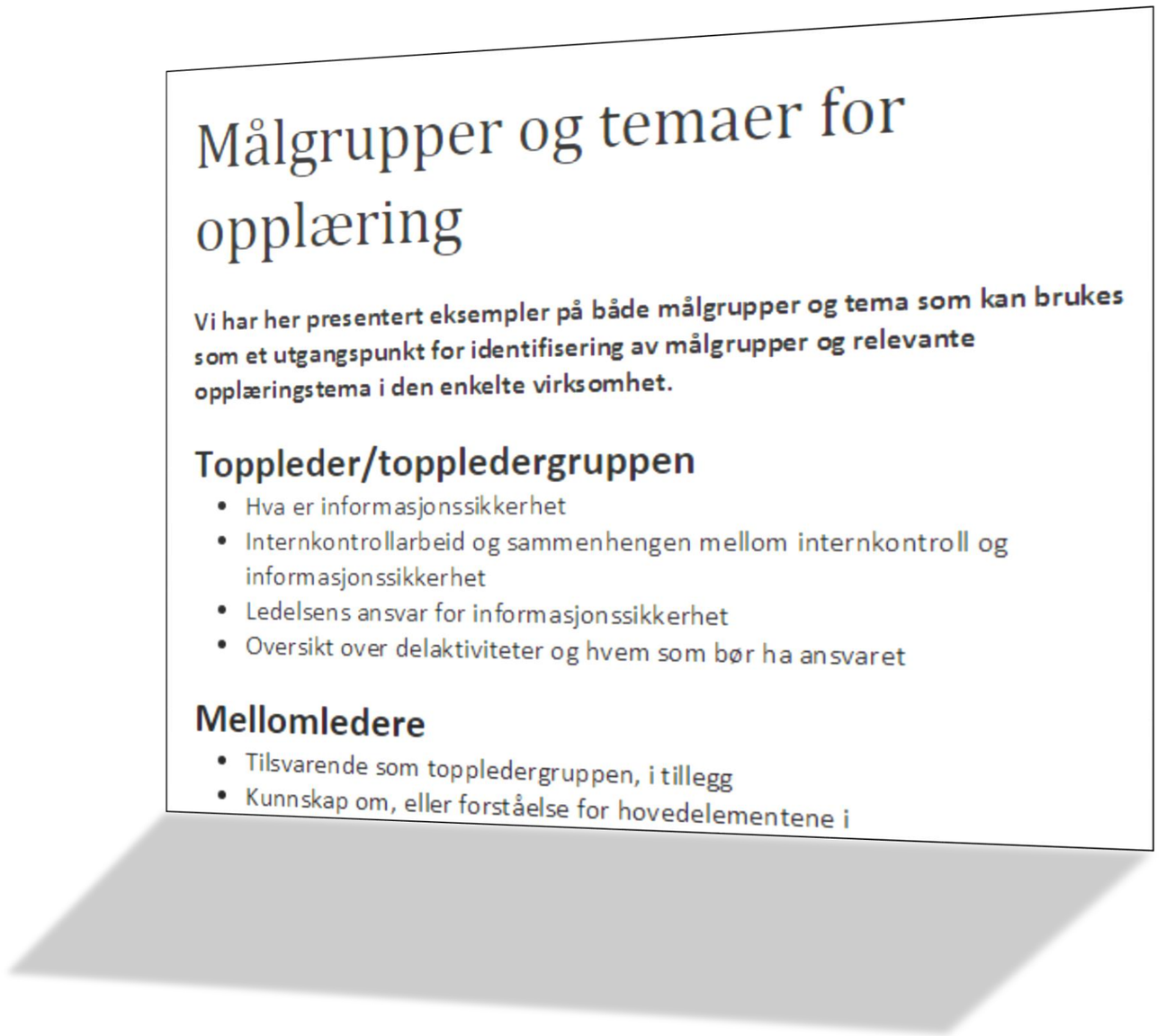
Identifisering av behov

- Kan identifiseres i ulike aktiviteter
  - Risikovurderinger
  - Medarbeidersamtaler
  - Oppfølging av hendelser, avvik og informasjonssikkerhetsbrudd
  - Revisjoner og evalueringer
  - Ledelsens gjennomgang

Følge opp behov

- Planlegge og gjennomføre opplæringstiltak
  - Tilpasse til målgruppen
  - Se tiltak i sammenheng
  - Tilrettelegge for måling av effekten av tiltak
- Variasjon i virkemidler
  - Kurs
  - E-læringskurs
  - Dilemmatrening
  - Foredrag
  - Osv…

Eksempel



Målgrupper og temaer for opplæring

Vi har her presentert eksempler på både målgrupper og tema som kan brukes som et utgangspunkt for identifisering av målgrupper og relevante opplæringstema i den enkelte virksomhet.

Toppleder/toppledergruppen

- Hva er informasjonssikkerhet
- Internkontrollarbeid og sammenhengen mellom internkontroll og informasjonssikkerhet
- Ledelsens ansvar for informasjonssikkerhet
- Oversikt over delaktiviteter og hvem som bør ha ansvaret

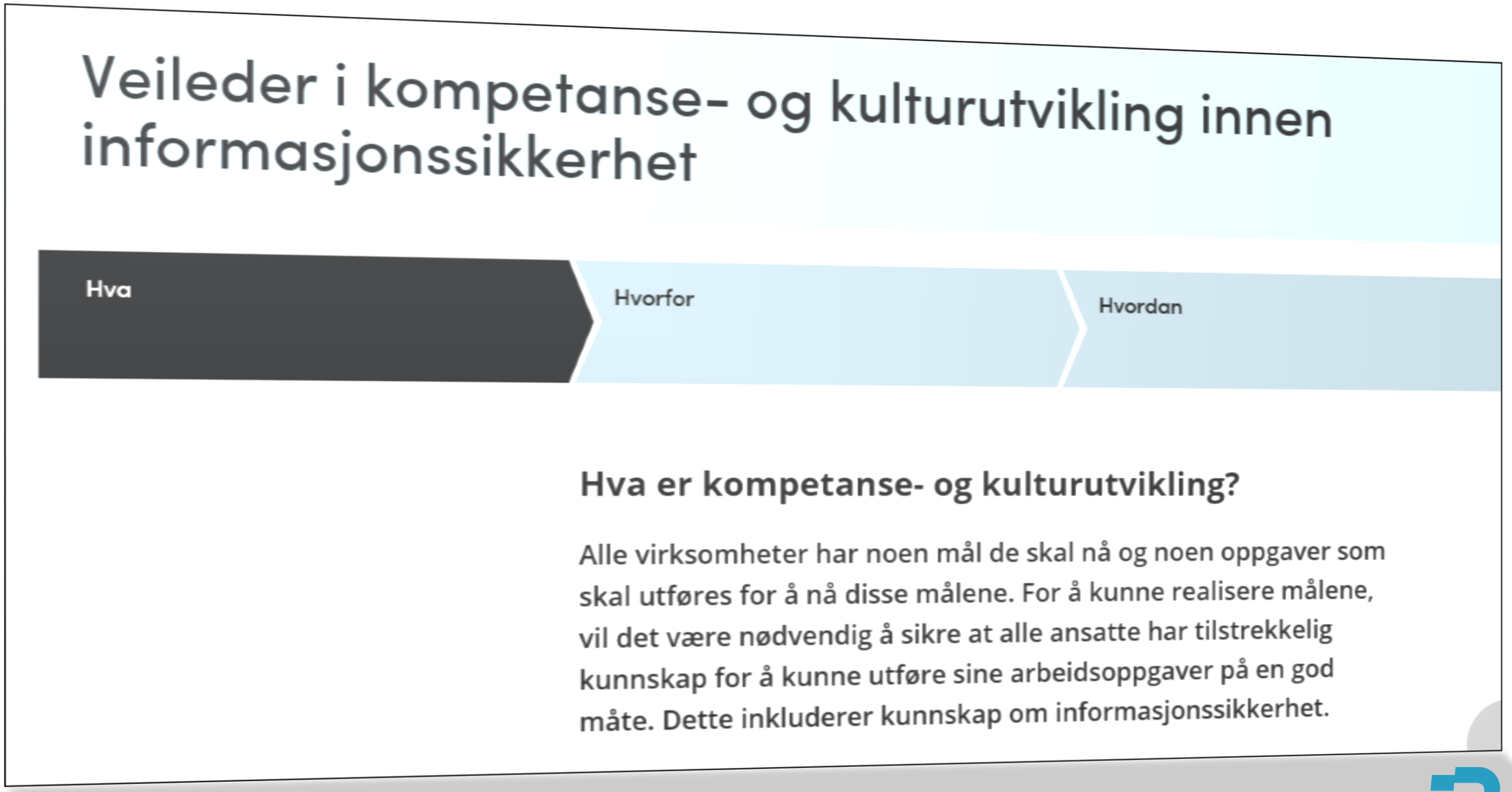
Mellomledere

- Tilsvarende som toppledergruppen, i tillegg
- Kunnskap om, eller forståelse for hovedelementene i

Følge opp sikkerhetskoordinatorer

- Lokal «pådriver» for informasjonssikkerhet
  - Pr. avdeling, eller tilsvarende org.-enhet
  - Typisk: tilleggsfunksjon til ordinær fagstilling
- Samlinger - møteplass
  - Kompetanseheving for sikkerhetskoordinatorene
  - Dele erfaringer og lære av hverandre
- Aktuelle temaer
  - Kompetanse- og kulturutfordringer i virksomheten
  - Sentralstyrte tiltak for kulturendring
  - Innspill og råd til virksomhetsledelsens gjennomgang
  - Innspill og råd rundt fellessikringen

Veileder i kompetanse- og kulturutvikling



Difi

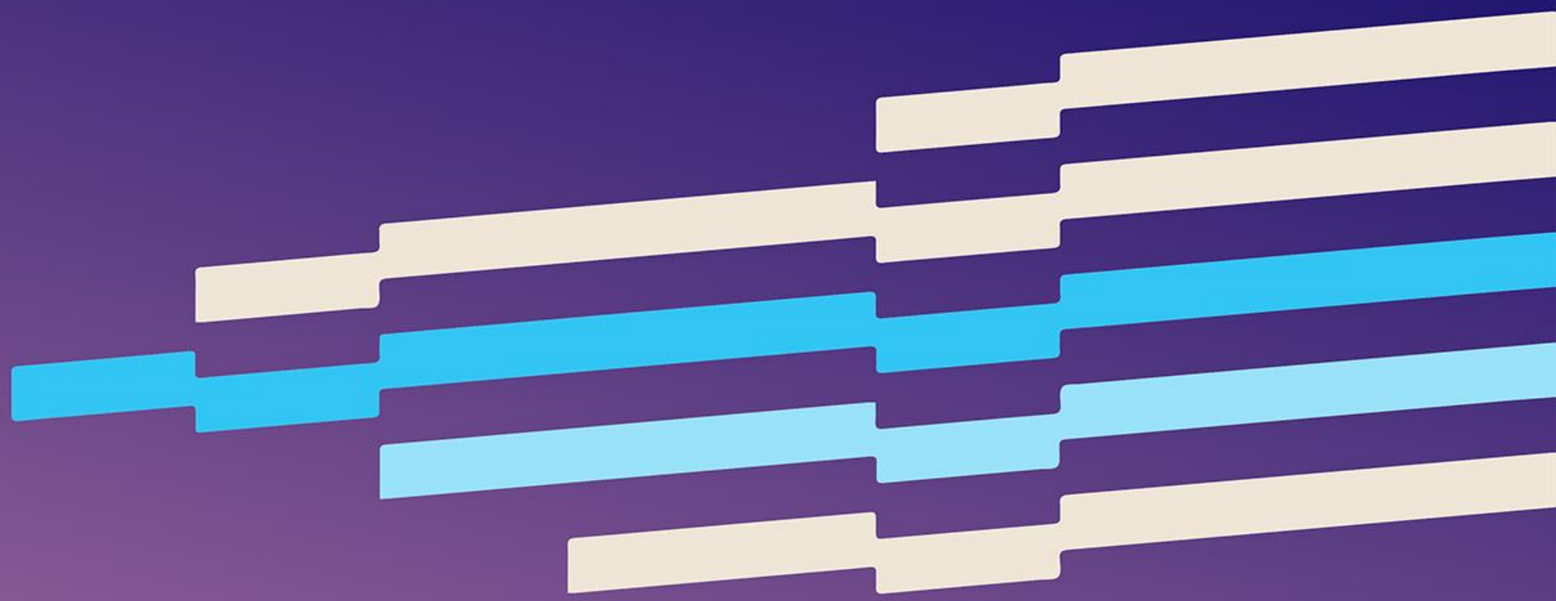
Difi
Direktoratet for forvaltning og ikt

Økt 16
Kommunikasjon

—

Innføringskurs

Internkontroll i praksis - informasjonssikkerhet



Kommunikasjon
- «Limet» i internkontrollen

Difi

Etableringsaktiviteten

Etablere rammeverk for dokumentasjon

- Formål: sikre at
  - man har god orden og struktur på dokumentasjon
  - det er lett å utarbeide nødvendig dokumentasjon
  - nødvendig informasjon er lett tilgjengelig for de som har behov for den

- Ikke gjør rammeverket mer omfattende enn nødvendig

Difi

Rammeverk for dokumentasjon

- kan blant annet
  - utdype formål og bruksområde for de ulike dokumentasjonstypene
  - vise til relevante maler
  - klargjøre generelle arkiverings- og publiseringskrav
  - klargjøre forvaltningsansvar og -prosedyrer for rammeverket

Etablering av rammeverk

- Bruk det man har dersom det er bra
  - Tydeliggjør hva som eventuelt mangler for informasjonssikkerhet
  - Juster det man har ut fra det

- Ved store mangler eller store svakheter i det man har
  - Oppnevn en arbeidsgruppe for å etablere et rammeverk
  - Alle internkontrollområder bør være representert
  - Viktig å sikre god forankring i virksomheten forøvrig

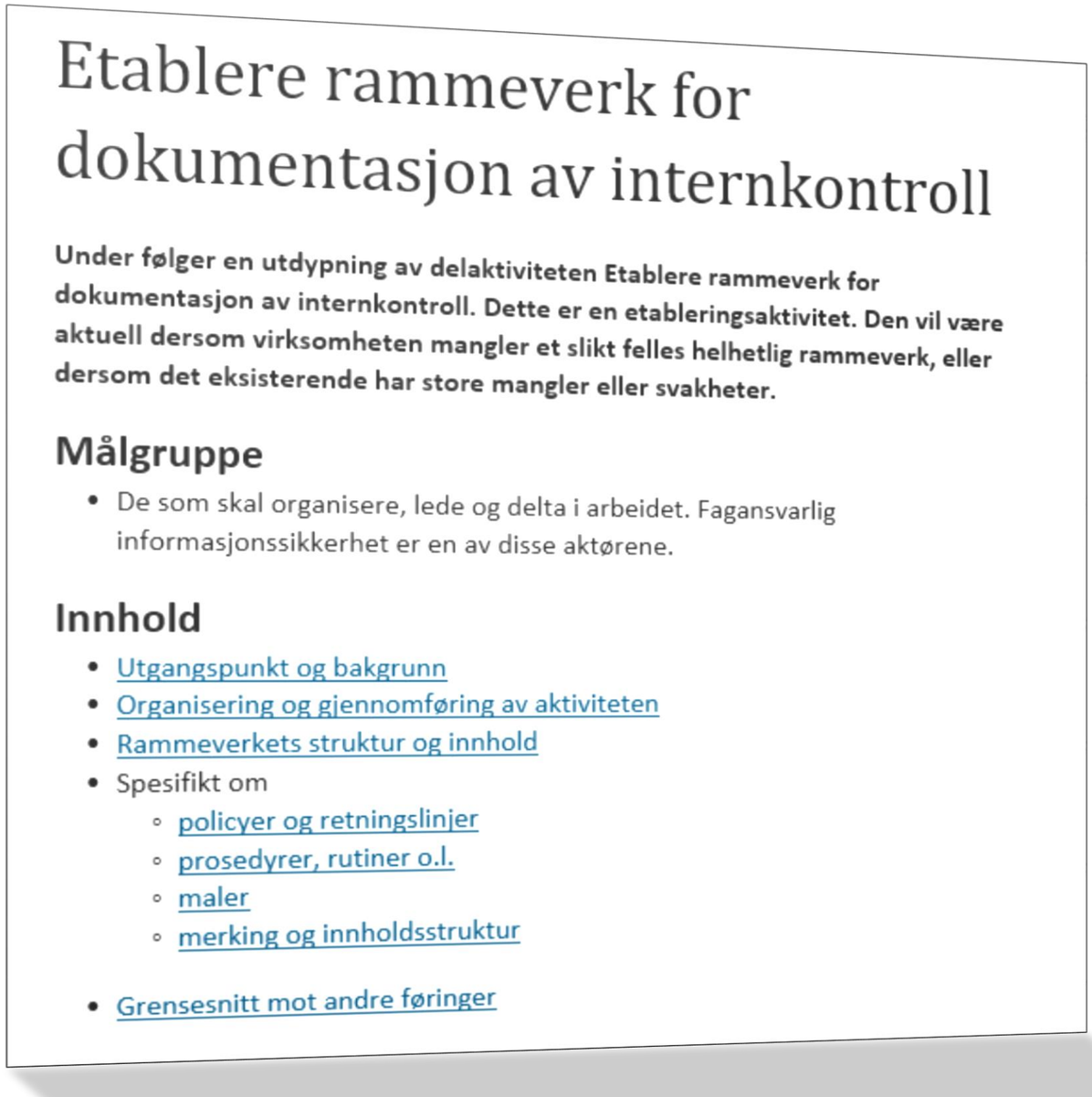
Difi

Eksempel:
Rammeverk for dokumentasjon

	Nivå	Dokumentasjonstype	Ansvar	Hovedinnhold
Eksternt	Styrende	Lover, forskrifter, tildelingsbrev o.l.	Myndigheter og overordnet departement	HVA skal gjøres
Internt	Overordnet styrende	Policyer og retningslinjer	Virksomhets-ledelsen	HVA skal gjøres av HVEM
Internt	Operasjonelt styrende (Gjennomførende)	Krav, instrukser, prosedyrer, rutiner og dokumentasjon av andre typer tiltak	Ledere på ulike nivå ut fra ansvarsområde	HVORDAN og NÅR skal noe gjøres
Internt	Kontrollerende	Logger, referat, rapporter, notat o.l. om utførte oppgaver, risikovurderinger, andre vurderinger, revisjoner, beslutninger mv.	Utførere (alle ansatte ut fra ansvar)	HVA er utført eller besluttet iht. ovennevnte

Difi

Utdypende veiledning



Etablere rammeverk for dokumentasjon av internkontroll

Under følger en utdypning av delaktiviteten Etablere rammeverk for dokumentasjon av internkontroll. Dette er en etableringsaktivitet. Den vil være aktuell dersom virksomheten mangler et slikt felles helhetlig rammeverk, eller dersom det eksisterende har store mangler eller svakheter.

Målgruppe

- De som skal organisere, lede og delta i arbeidet. Fagansvarlig informasjonssikkerhet er en av disse aktørene.

Innhold

- Utgangspunkt og bakgrunn
- Organisering og gjennomføring av aktiviteten
- Rammeverkets struktur og innhold
- Spesifikt om
  - policyer og retningslinjer
  - prosedyrer, rutiner o.l.
  - maler
  - merking og innholdsstruktur
- Grensesnitt mot andre føringer

Kommunikasjon

SYSTEMATISKE AKTIVITETER

Difi

Kommunikasjon – delaktiviteter

- Formidle nye føringer
- Dokumentere gjennomførte internkontrollaktiviteter
- Dokumentere etterlevelse av sikkerhetstiltak
- Statusrapporter som grunnlag for risikovurderinger
- Saksnotat til virksomhetsledelsens gjennomgang
- Kommunikasjon mellom delaktiviteter og aktører
- Ekstern kommunikasjon

Difi

Kommunikasjon – delaktiviteter

- Formidle nye føringer
- Dokumentere gjennomførte internkontrollaktiviteter
- Dokumentere etterlevelse av sikkerhetstiltak
- Statusrapporter som grunnlag for risikovurderinger
- Saksnotat til virksomhetsledelsens gjennomgang
- Kommunikasjon mellom delaktiviteter og aktører
- Ekstern kommunikasjon

Difi

Dokumentere gjennomførte internkontrollaktiviteter

- Bør som hovedregel skje skriftlig
- Unngå vesentlig merarbeid ved å:
  - Bruke gode maler
  - Ha fokus på å dokumentere det viktigste
  - Integrere dokumentasjonsarbeidet i de ordinære arkivering- og journalføringsrutiner
- Sikrer virksomhetens «hukommelse»:
  - Hva er gjort?
  - Hvilke beslutninger er tatt?
  - Hva var bakgrunnen for beslutningene?

Dokumentere etterlevelse av tiltak

- Når tiltakene stiller krav om det
- Risikobasert og klart forankret i behov
- Bør legges opp på en måte som ikke oppleves unødvendig eller vesentlig hemmende for annet arbeid

Statusrapporter som grunnlag for risikovurderinger

- Bakgrunn og støtte for gjennomføring av risikovurderinger
- Bør utarbeides minst en gang årlig
  - utarbeides av fagansvarlig informasjonssikkerhet
  - tidspunkt tilpasset når vurderingene oftest gjøres
  - tilgjengelig for risikoeiere
- Innhold tilpasset behov, for eksempel:
  - Tidligere registrerte sikkerhetshendelser
  - Trender i trussel- og risikobildet
  - Trender i interne revisjoner, evalueringer, undersøkelser, målinger
  - Sårbarhetsnivå/tiltaksstyrke på felles tiltaksområder
  - Oversikt over felles tiltaksleverandører, fellessikring og mulig tilleggssikring

Difi

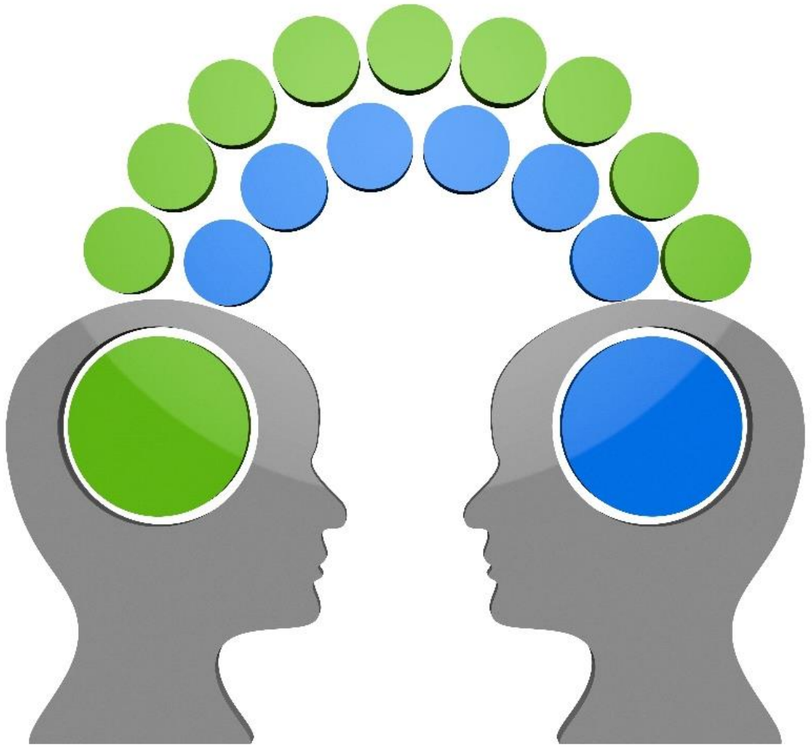
Saksnotat til virksomhetsledelsens gjennomgang

- Virkemiddel for en effektiv virksomhetsledelsens gjennomgang
- Utarbeides av fagansvarlig informasjonssikkerhet
- Tydelige og begrunnede anbefalinger
- Innhold tilpasset virksomhetens behov og situasjon, og hva som vil være tema i virksomhetsledelsens gjennomgang.

Kommunikasjon – delaktiviteter

- Formidle nye føringer
- Dokumentere gjennomførte internkontrollaktiviteter
- Dokumentere etterlevelse av tiltak
- Statusrapporter som grunnlag for risikovurderinger
- Saksnotat til virksomhetsledelsens gjennomgang
- Kommunikasjon mellom delaktiviteter og aktører
- Ekstern kommunikasjon

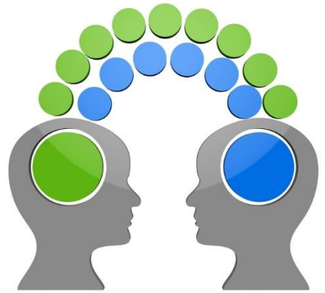
Difi



REFLEKSJONSOPPGAVE

Difi

Refleksjonsoppgave 6



1: Velg noen av delaktivitetene under og diskuter i hvilken grad de gjennomføres hos dere i dag – innen informasjonssikkerhet. Bruk vurderingskodene.

Kompetanse- og kulturutvikling

- Identifisere og følge opp behov for kompetanse- og kulturutvikling
- Følge opp lokale sikkerhetskoordinatorer

Kommunikasjon

- Statusrapporter som grunnlag for risikovurderinger
- Saksnotat til virksomhetsledelsens gjennomgang

2: Har dere andre områder internt dere kan lære av?

Difi

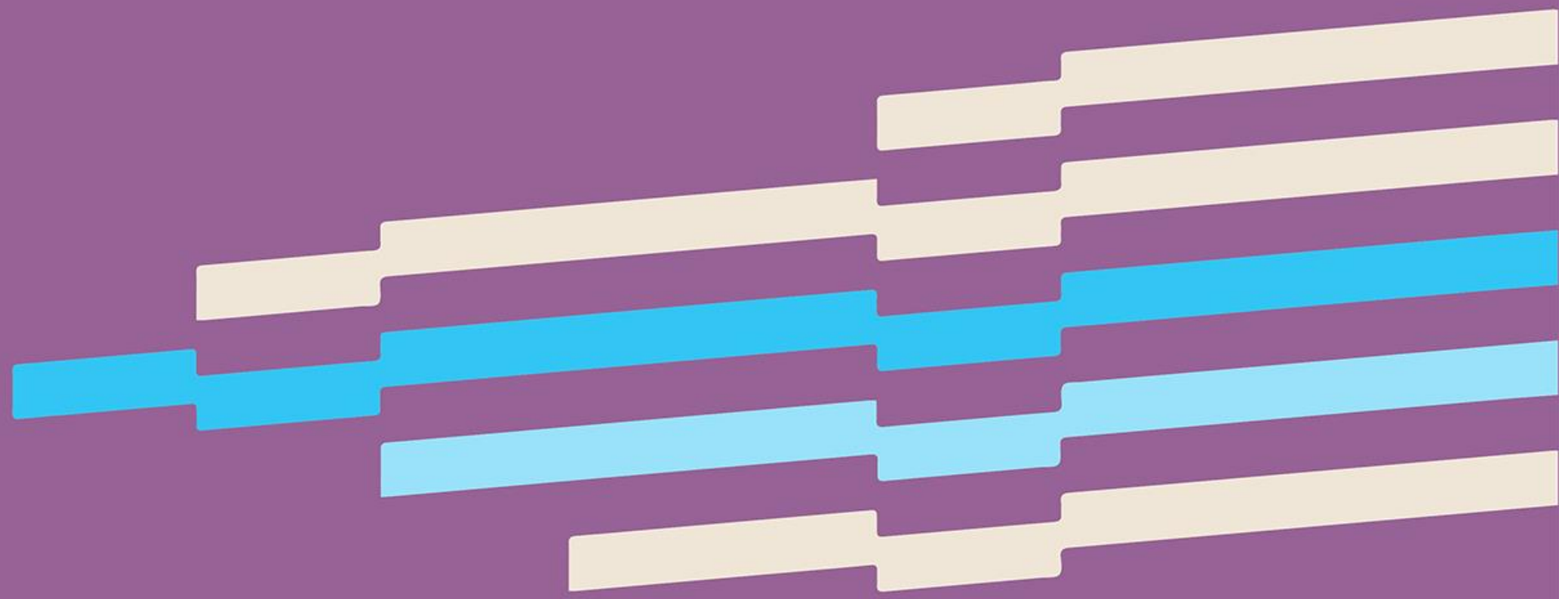
Difi
Direktoratet for
forvaltning og ikt

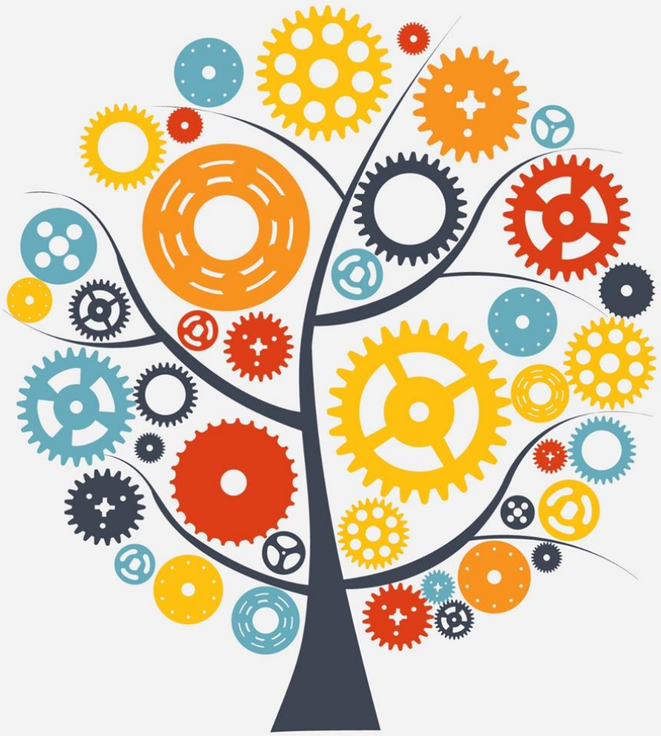
Økt 17
Etableringsaktiviteter

—

Innføringskurs

Internkontroll i praksis -
informasjonssikkerhet





Ledelsens styring og oppfølging

- Risikovurdering
- Risikohåndtering
- Overvåkning og hendelseshåndtering
- Måling, evaluering og revisjon
- Kompetanse- og kulturutvikling

Kommunikasjon

Difi

Hvor er dere?

Er det bra nok?

Difi

Hvordan dere kan jobbe

Gradvis oppbygging

Etablering

Systematisk

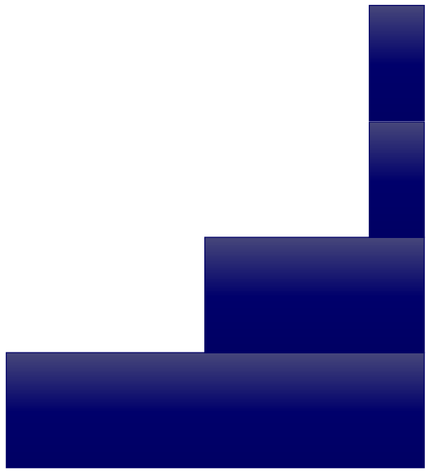
År

n

3

2

1



Eksempel på arbeidsmengde

Gradvis oppbygging

Etablering

Systematisk

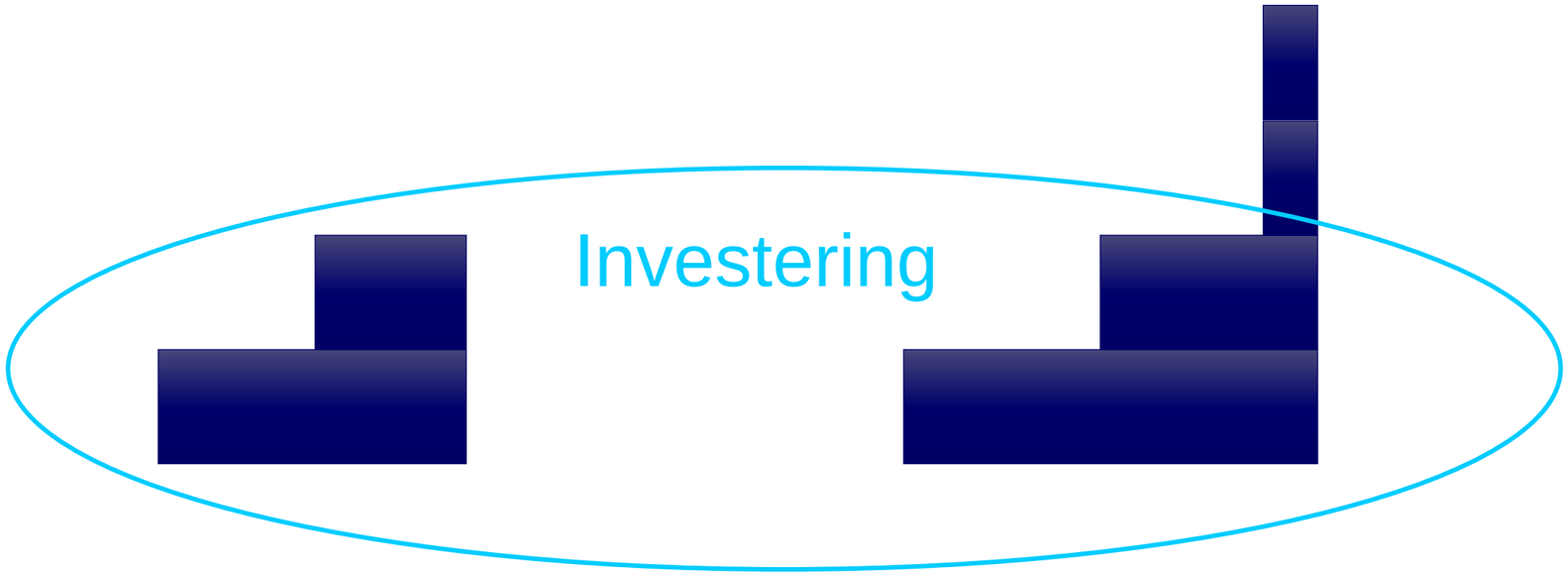
År

n

3

2

1



Difi

Start

Difis anbefaling:

1. Analyse av status
   - Med Difis mal
2. Plan for etablering | forbedring
3. Ledelsens føringer for aktivitetene
   - Hvordan skal ting fungere hos oss?
   - → Styrende dokumenter

Ledelsesforankring

- Husk! Dette er ledelsens verktøy for å ha styring og kontroll
  - En virksomhet kan ikke ha et «styringssystem» på siden, forankret noe annet sted
- Topplederbeslutning: gjennomføre analyse av status
- Topplederbeslutning: plan for etablering | forbedring
  - eller å være fornøyd med det dere har

Difi

1

- **Analysere** status
- **Planlegge** etablering/forbedring
- Gjennomføre andre **etableringsaktiviteter**

Gjennomføre aktivitetene systematisk

2

Internkontroll-aktiviteter

Sikkerhetstiltak

3

Tilleggssikring

Fellessikring

- Instrukser og rutiner
- Avtaler
- Retningslinje for fysisk sikkerhet
- Tilgangsstyring IT-systemer
- Sikkerhetskopiering og gjenoppretting
- Osv.

Difi

Oversikt over alle

ETABLERINGSAKTIVITETENE

Etableringsaktiviteter

- Avklare behov og lage en plan
  - Analysere status
  - Planlegge etablering/forbedring
- Få på plass det viktigste
  - Utforme/forbedre overordnede styrende dokumenter
  - Få på plass nøkkelpersoner og aktivere sikkerhetsorganisasjonen
  - Utforme og gjennomføre grunnopplæring
  - Etablere system for hendelses- og avvikshåndtering
- Skape en god plattform
  - Etablere fellessikring og synliggjøre tilleggssikring
  - Etablere rammeverk for dokumentasjon
- Lage et godt grunnlag for sentrale aktiviteter
  - Felles analyse av eksterne krav
  - Identifisere typiske oppgave- og informasjonstyper

Difi

Analysere status

Støttedokument

Anbefalte delaktiviteter og dokumentasjon

Støttedokument

Dette er en samlet oversikt over de delaktiviteter og den dokumentasjon Difi anbefaler for internkontroll på informasjonssikkerhetsområdet. Oversikten er en punktvis versjon laget for å gi støtte under aktivitetene *Analysere status* og *Planlegge etablering/forbedring.* Strukturen følger hovedaktivitetene i Difis forklaringsmodell (jf. under). Det har ingen betydning for analyse og senere plan om virksomheten har valgt eller velger en annen struktur på sitt internkontrollarbeid.

Innhold

Innledning 2

1 Ledelsens styring og oppfølging 3

1.1 Virksomhetsledelsens gjennomgang 3

1.2 Delegere og følge opp gjennom linjen 3

1.3 Sikre finansielle rammer for internkontroll- og sikkerhetsarbeidet 4

Difi

Analyseskjema

Analyse av status

Referanse: Difis veiledningsmateriell «Internkontroll i praksis - informasjonssikkerhet»

Om analysen

Virksomhetsnavn:		**Dato ferdig:**	
Leder av og deltakere i analysearbeidet:			

Vurderingskoder

Kodene benyttes i analyseskjemaet under.

I hvilken grad gjennomfører vi de systematiske aktivitetene og lager anbefalte dokumenter? (eller)
I hvilken grad har vi gjennomført etableringsaktivitetene og laget anbefalte dokumenter?

0	Ikke i det hele tatt, eller i liten grad
1	Noe samsvar i praksis eller i formaliserte krav, men behov for store forbedringer
2	En god del samsvar i praksis eller i formaliserte krav, men behov for en del justeringer og forbedringer
3	Tilstrekkelig samsvar i praksis, men mangler noe i formalisering/dokumentasjon
4	Tilstrekkelig samsvar i praksis og god formalisering/dokumentasjon. Ingen forbedring er nødvendig.

Behov for endring

A	Aktiviteten bør gjennomføres fullt ut
B	Deler av aktiviteten bør gjennomføres
C	Aktiviteten og anbefalt dokumentasjon bør formaliseres i retningslinje eller lignende
D	Informasjonsbehov
E	Opplæringsbehov
F	Behov for mer systematisk etterspørring/oppfølging av status gjennom linjen
G	Andre behov (spesifiser)

Prioritet (P) = 1-4, Indikerer foreløpig anbefalt rekkefølge i en kommende plan

Resurssbehov (R) = L/M/H; Lav = Bør dekkes kurant innenfor egne rammer og eksisterende ansvar; Moderat = Ikke svært omfattende, men kan kreve spesiell avklaring på ulike ledernivå; Høy = Må trolig prioriteres spesielt av virksomhetsledelsen

Difi

Tette gapet

Plan for etablering | forbedring

- Felles plan for hele virksomheten
  - alle eller deler av etableringsaktivitetene
  - det som er nødvendig for å få de systematiske aktivitetene i gang i hele virksomheten
  - ansvar og frister
  - status og fremdrift (for rapportering)

Styrende dokumenter

- Policy for informasjonssikkerhet
- Retningslinjer
  - Roller og ansvar i internkontroll- og sikkerhetsarbeidet
  - Forstå, vurdere og håndtere risiko
  - Vurdere behov for risikovurderinger

Nøkkelpersoner + organisasjon

- Ressurser til å dekke rollene det er behov for
- Peke ut | tilsette
  - **Fagansvarlig informasjonssikkerhet**
  - Tiltaksleverandører
  - Prosessledere for risikovurderinger
  - Lokale sikkerhetskoordinatorer
  - Arbeidsgrupper for etableringsfasen
  - Osv
- Aktivering av roller bør inngå i planen for etablering | forbedring

Grunnopplæring

- Ledere – eksempler på innhold:
  - Hvorfor informasjonssikkerhet og internkontroll er viktig
  - Ledernes ansvar og oppgaver i aktivitetene
  - Hvordan de bør organisere arbeidet lokalt

- Annen tilpasset opplæring – eksempler på målgruppe:
  - Prosessledere for risikovurderinger
  - Håndteringsansvarlige
  - Alle ansatte

Hendelses- og avvikshåndtering

- Identifisere og håndtere hendelser så effektivt som mulig
- Etablere system for hendelses- og avvikshåndtering
  - Registrering og oppfølging
  - Kategoriseringsfunksjoner
  - Rapporteringsmuligheter
- Læring og forbedring

Etablere fellessikring

Fase 1
- Minimumsnivå: kjente behov + god praksis

Fase 2
- Risikovurdering + risikohåndtering av 2-4 pilotområder

Fase 3
- Velge: Fellesikring || Tilleggssikring

Fase 4
- Høring i virksomheten: sideeffekter - kostnader

Fase 5
- Beslutning

Fase 6
- Iverksettelse

Difi

Behov for dokumentasjon av sikkerhetstiltak

- Risikoeier
  - Oversikt
  - «Overordnede tiltak»
  - Hva inngår i fellessikringen?
  - Hva er tilgjengelig tilleggssikring?
  - Tiltaksstyrke
- Tiltaksleverandør
  - Oversikt
  - «Detaljtiltak»
  - Ref. til tiltaksbanker
  - Ref. til detaljer i regelverk
  - Detaljer om implementering
  - Tekniske detaljer

Difi

Behov for dokumentasjon av sikkerhetstiltak

- Risikoeiere ⇔ Tiltaksleverandører
  - God kommunikasjon
  - Risikoeiere må forstå tiltak og helheten av tiltak
    - uten å kjenne alle tekniske detaljer
  - Detaljer må være tilgjengelig ved behov
    - f.eks. ifbm. vurdering av spesifikke risikoer

Rammeverk for dokumentasjon

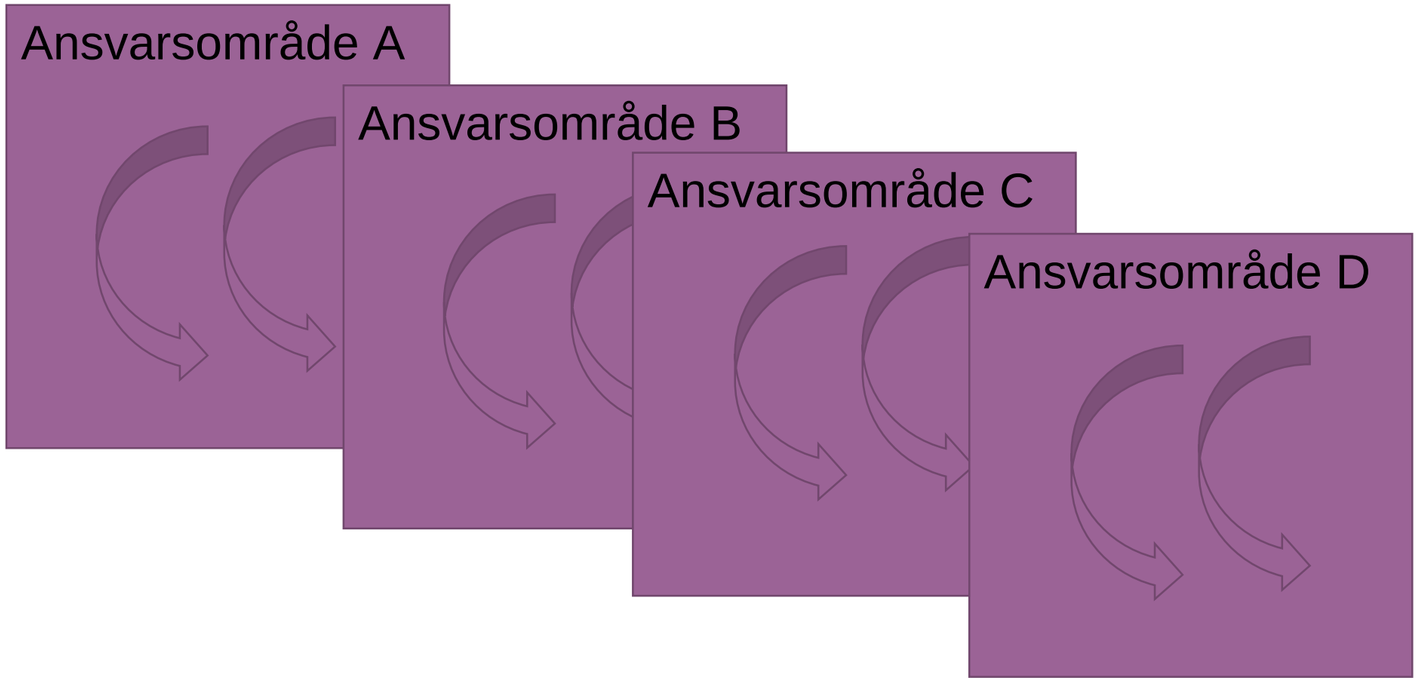
- Struktur og oversikt
- Nødvendig dokumentasjon tilgjengelig for de som har behov for den
- Lett å utarbeide dokumentasjon

Felles identifisering og analyse

Arbeidsoppgaver

Informasjonstyper

Eksterne krav



Difi

Etableringsaktiviteter

- Avklare behov og lage en plan
  - Analysere status
  - Planlegge etablering/forbedring
- Få på plass det viktigste
  - Utforme/forbedre overordnede styrende dokumenter
  - Få på plass nøkkelpersoner og aktivere sikkerhetsorganisasjonen
  - Utforme og gjennomføre grunnopplæring
  - Etablere system for hendelses- og avvikshåndtering
- Skape en god plattform
  - Etablere fellessikring og synliggjøre tilleggssikring
  - Etablere rammeverk for dokumentasjon
- Lage et godt grunnlag for sentrale aktiviteter
  - Felles analyse av eksterne krav
  - Identifisere typiske oppgave- og informasjonstyper

Difi

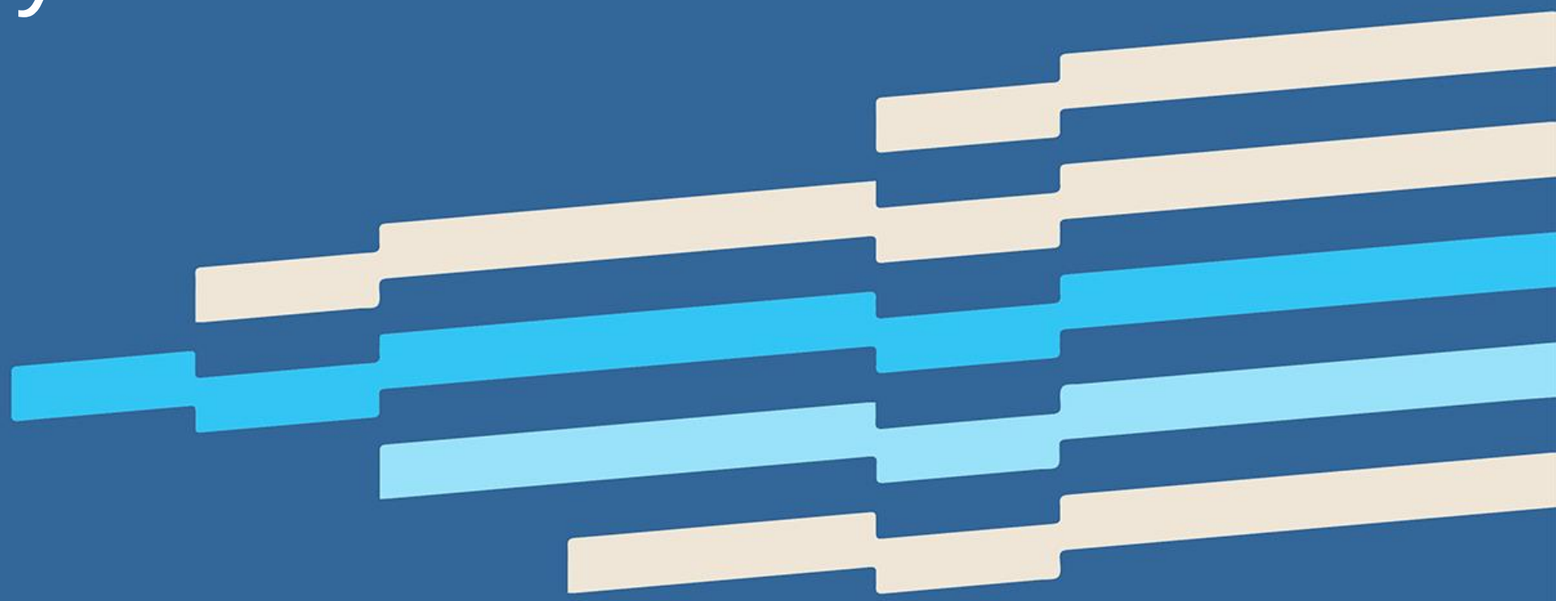
Difi
Direktoratet for
forvaltning og ikt

Økt 18
Overordnede styrende dokumenter

—

Innføringskurs

Internkontroll i praksis -
informasjonssikkerhet



Overordnede styrende dokumenter

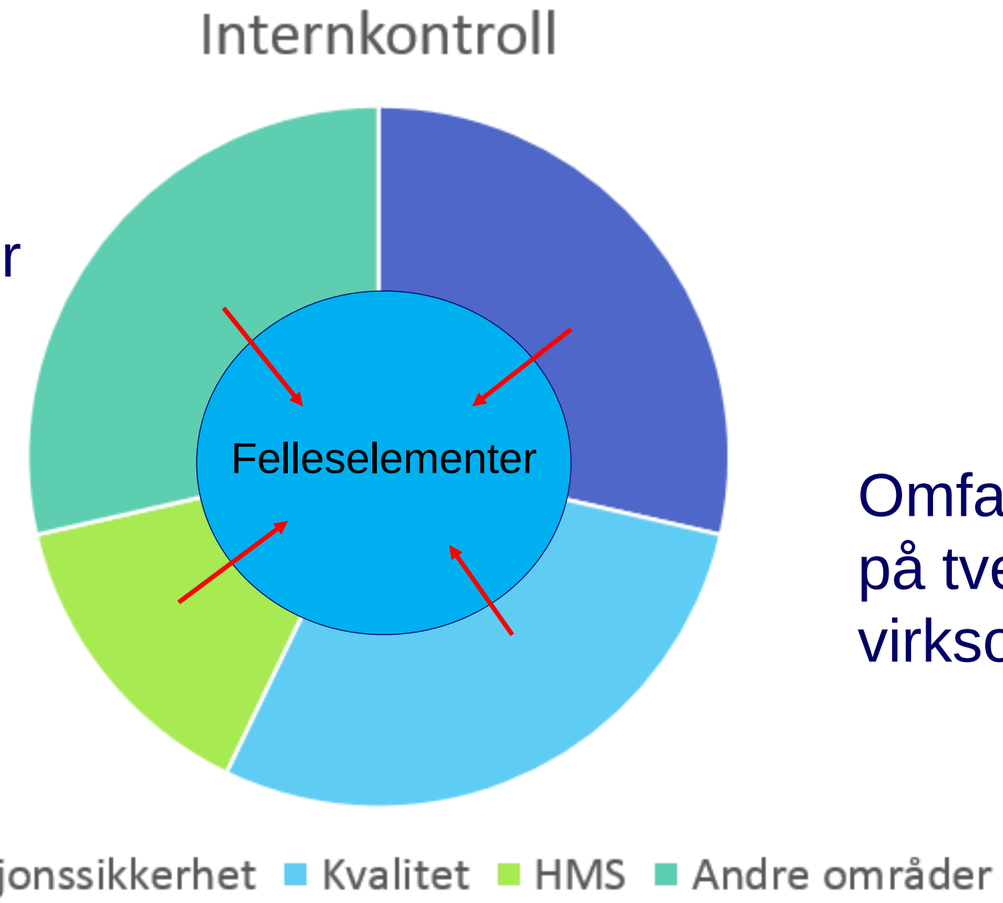
- Er fundamentet i internkontrollen
- Klargjør hvem som skal gjøre hva, og gir føringer for arbeidet
- Er en forutsetning for at de systematiske aktivitetene i internkontrollen skal bli gjennomført i tilstrekkelig omfang og på riktig måte

Overordnede styrende dokument

- Inneholder virksomhetsledelsens føringer for internkontrollarbeidet
- Må som minimum dekke området informasjonssikkerhet
- Flere dokumenter kan med fordel utformes som fellesdokumenter for flere internkontrollområder

Helhetlig internkontroll

Områdespesifikke deler



Omfang av integrering på tvers må tilpasses virksomheten

Difi

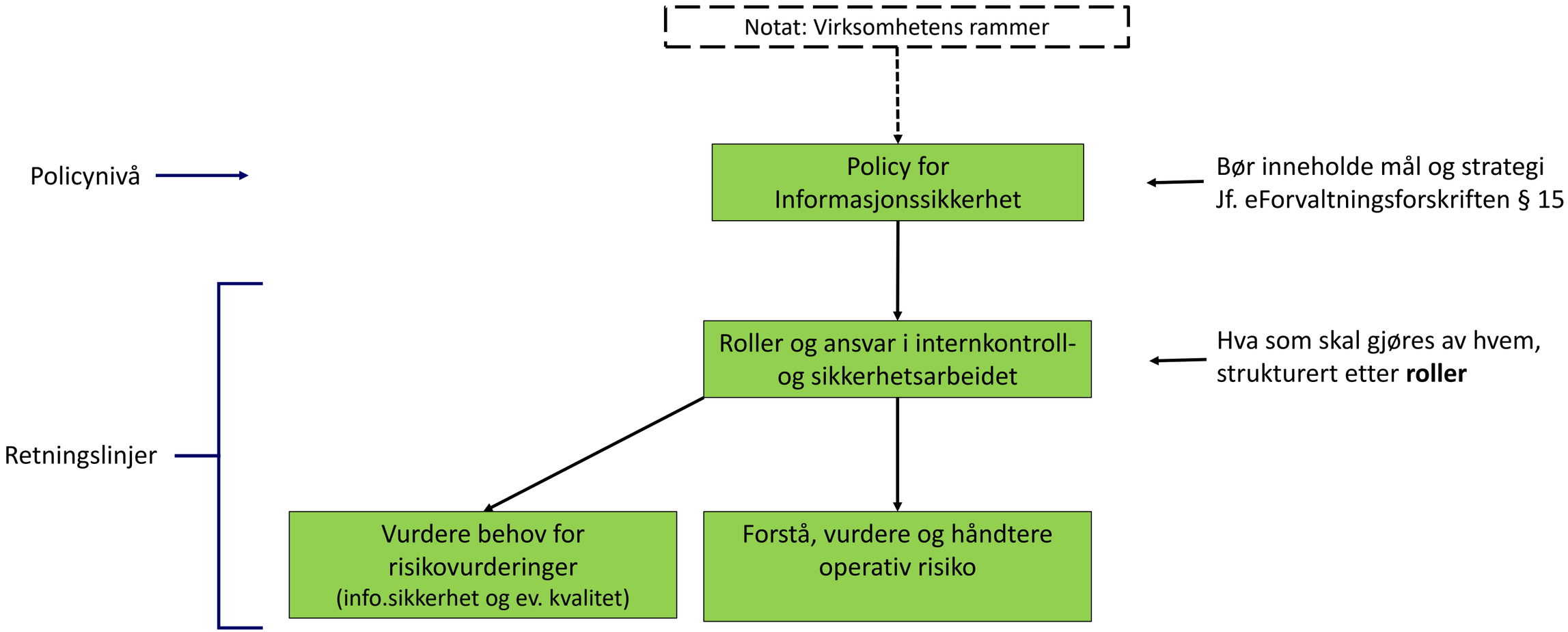
Difis anbefaling:
Overordnede styrende dokumenter

1. En kort overordnet policy for informasjonssikkerhet
2. En retningslinje om roller og ansvar i internkontroll- og sikkerhetsarbeidet
3. En retningslinje om å forstå, vurdere og håndtere operative risikoer
4. En retningslinje om å systematisk vurdere behov for risikovurderinger

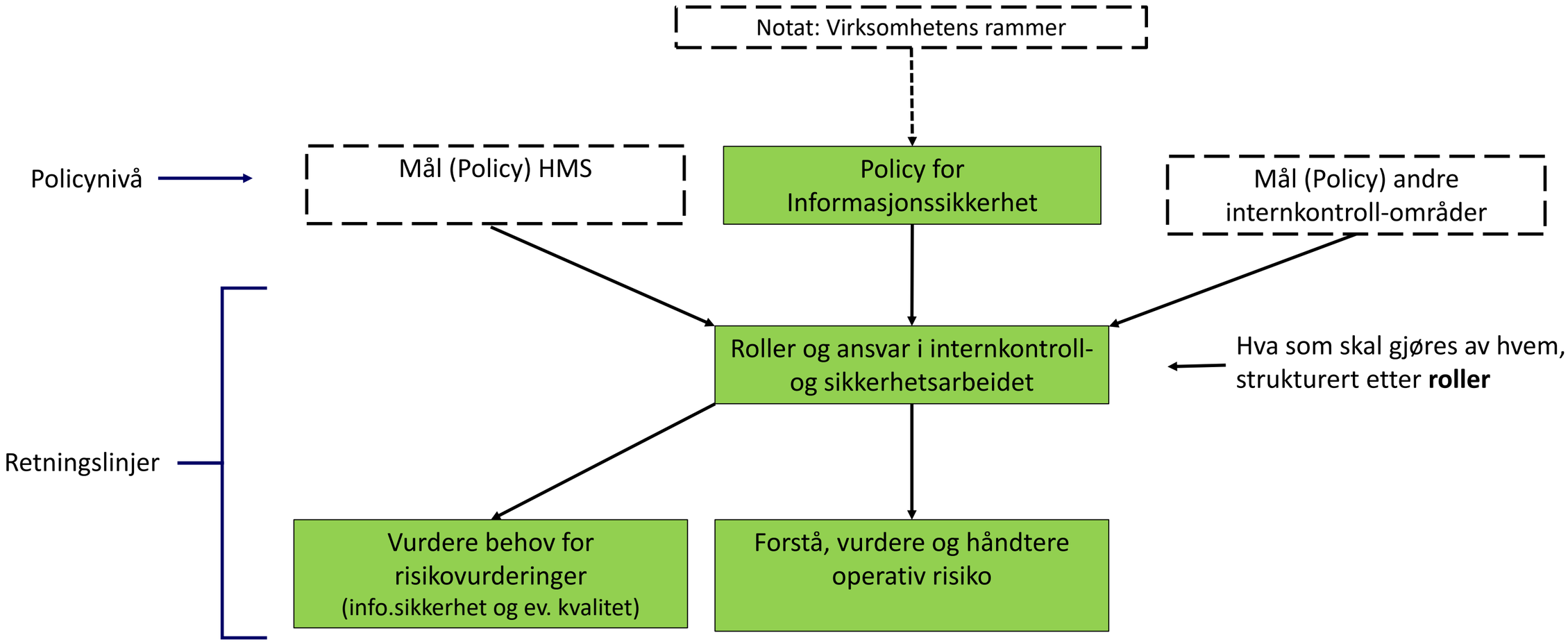
+ Et lite grunnarbeid først (notat)
+ Eventuelt en eller flere utdypende veiledninger av nr. 2
    - Eksempelvis: Veiledning: Aktiviteter og ansvar - internkontroll informasjonssikkerhet

Difi

Difis anbefaling:
Overordnede styrende dokumenter



Difis anbefaling:
Overordnede styrende dokumenter



Utforme overordnede styrende dokumenter

Organisering

- Bred men effektiv involvering i utformingen
  - Gjennomgående: God involvering på de riktige tingene og en effektiv prosess
    - Dokumentene er eid av virksomhetsledelsen – de må involveres med forankring og styringssignal underveis i utformingen
    - En rekke føringer trenger bred forankring og involvering ute i virksomheten
    - Må sikre nødvendig samordning med andre internkontrollområder
- Etabler flere arbeidsgrupper med ulikt fokus
  - Lokal forankring, diskusjoner og bearbeiding må sikres på hensiktsmessig måte for ulike tema og dokumenter
- Bør være god støtte i eksempler fra Difi
  - Kan velge andre navn på dokumentene

Difi

GRUNNARBEID – KLARGJØRE SENTRALE RAMMER

Grunnarbeid - klargjøre sentrale rammer

- Identifisere og lage en enkel oversikt over sentrale rammer som kan påvirke innholdet i dokumentene
- Mye kan være identifisert allerede, men ofte være spredd i ulike dokumenter
- Samle og sammenstille hovedmoment fra ulike interne kilder
  - I et notat

Notat etter grunnarbeidet

Eksempel på innhold

- Virksomhetens visjon, formål og primære oppgaver
- Interessenter og interesser i informasjonsbehandlingen som skjer i og under ansvaret til virksomheten
- Eventuelle relevante føringer fra overordnet departement eller enhet
- Sentrale lover, forskrifter og avtaler som påvirker informasjonsbehandling i virksomheten
- Andre internkontrollområder i virksomheten med lignende dokumenter og aktiviteter
- Eksisterende organisering og fordeling av ansvar og myndighet innen både informasjonssikkerhet og på andre områder
- Andre vesentlige rammevilkår og forhold, eksempelvis:
  - Tidligere valg om bruk av ekstern databehandler
  - Trender rundt trusler og sårbarheter

Difi

POLICY FOR INFORMASJONSSIKKERHET

Difi

Policy for informasjonssikkerhet

- Skal kommunisere de viktigste føringene fra toppledelsen
- Nå bredt ut i virksomheten
- Danne grunnlaget for mer detaljerte retningslinjer
- Være et sentralt referansepunkt

- Offentlig dokument
- Kan være interessant for mange

- Bør være overordnet, tydelig og førende, og samtidig ikke for lang

Policy for informasjonssikkerhet

Difis anbefalte innhold

- Omfang
  - Hvilke områder policyen gjeler for
    - Normalt hele virksomheten
- Formål med virksomhetens informasjonsbehandling og informasjonssikkerhet
- Mål for informasjonssikkerhet
- Strategi for informasjonssikkerhet
  - Organisering
  - Krav til internkontroll- og sikkerhetsarbeidet
  - Krav til ansatte (overordnet)

Utgangspunkt i Difis eksempel

- Følgende må være svært virksomhetsspesifikt
  - Formålet med vår informasjonsbehandling og informasjonssikkerhet

- Følgende er ofte svært likt for offentlige virksomheter
  - Omfang
  - Mål for informasjonssikkerhet
  - Strategi for informasjonssikkerhet
    - Organisering
    - Krav til internkontroll og sikkerhetsarbeidet
    - Krav til ansatte

- Sentrale deler bør uansett diskuteres, forstås og forankres bredt i virksomheten

Difi

Foreslått tilnærming

- Involver representanter fra flere deler av virksomheten
- Hovedvekt
  - Formål med virksomhetens informasjonsbehandling og informasjonssikkerhet
    - Finn gode, inspirerende og relevante formuleringer
    - gode «one-linere» eller «two-linere» som de ansatte kjenner seg igjen i og som gir forståelse for hvorfor informasjonssikkerhet er viktig for «oss»
- Diskutere og forankre
  - Formål med og struktur på policydokumentet
  - Hva målene betyr og reell nytte av eventuell endring
  - Hva strategidelene betyr og reelt behov for endring
    - Merk at kravene i eksempelet er kjernen i de systematiske aktivitetene – og dermed grunnlaget for øvrige retningslinjer

Difi

Utgangspunkt i Difis eksempel

- Se Difis eksempel:

  Policy for informasjonssikkerhet

Retningslinje:

ROLLER OG ANSVAR I INTERNKONTROLL- OG SIKKERHETSARBEIDET

Difi

Retningslinje:
Roller og ansvar i internkontroll- og sikkerhetsarbeidet

- Viktig å ha klare og lett tilgjengelige føringer for hvem som har hvilke roller
  - Gjelder alle internkontroll- og sikkerhetsområder
- De fleste virksomheter har samme / lignende roller på tvers av internkontrollområder
  - Dette bør derfor være en felles retningslinje
    - Men man kan dekke informasjonssikkerhet først og utvide etterhvert

Retningslinje:
Roller og ansvar i internkontroll- og sikkerhetsarbeidet

- Ikke for omfattende og kompleks
- Klargjøre sentrale roller
- Konkrete oppgaver og ansvar for de enkelte aktørene kan stå andre steder, f.eks.:
  - Utdypende veiledninger
    - for alle internkontrollområder og/eller for spesifikke områder som informasjonssikkerhet
    - samlet eller delt opp i hensiktsmessige deler
  - Stillings- eller funksjonsinstrukser
- Viktig å forstå rollebegrep i ulikt regelverk
  - Det er roller som skal dekkes, og ikke stillinger som skal fylles

Difi

Innhold i Difis eksempel

- Grunnleggende prinsipp
  - ansvarsprinsippet, likhetsprinsippet, nærhetsprinsippet, samvirkeprinsippet
- Linjen som hovedføring og krav til
  - toppleder / direktøren
  - ledere på alle nivå
  - ledere på operativt nivå (risikoeiere)
- Ansvar og krav til
  - Systemeiere fellessystem
  - Tiltaksleverandører
  - Alle ansatte
  - Spesialfunksjoner
  - Faste fora

Foreslått tilnærming

- Utgangspunkt
  - Se over grunnarbeidet/notatet om virksomhetens rammer
    - Eksisterende organisering
    - Eventuelle lov- og forskriftskrav
    - Eksisterende tilsvarende retningslinjer på andre områder
  - Ta deretter utgangspunkt i Difis eksempel

- Diskusjon og vurderinger
  - Er de grunnleggende prinsippene hensiktsmessige?
  - Er rollebegrepene nyttige og klargjørende?
  - Hva har vi?
  - Hva fungerer godt / mindre godt?
  - Hva trenger vi?
  - Hva bør endres/tydeliggjøres?
    - Fra det vi har og/eller fra Difis eksempler

Utgangspunkt i Difis eksempel

- Se Difis eksempel:
  - Retningslinje: Roller og ansvar i internkontroll- og sikkerhetsarbeidet

Retningslinje:

FORSTÅ, VURDERE OG HÅNDTERE OPERATIV RISIKO

Difi

Retningslinje:
Forstå, vurdere og håndtere operativ risiko

- Internkontroll (styring og kontroll) krever rimelig felles forståelse i virksomheten av
  - hva risiko er
  - hvordan risiko skal uttrykkes
  - hvordan risikoer på ulikt nivå skal estimeres og forstås
  - hvordan risikoer skal håndteres
  - hvilke kriterier som gjelder for å akseptere risiko
- Difis eksempel kan danne utgangspunkt
- Innholdet må gjøres til «virksomhetens eget».
- Sentrale deler bør bli
  - godt forankret underveis hos toppledelsen og ut i virksomheten
  - akseptert/bearbeidet gjennom bred og god involvering

Difi

Retningslinje: Forstå, vurdere og håndtere operativ risiko

Innhold i Difis eksempel

- Risikoforståelse
  - med henvisning til Vedlegg A: Risikoforståelse - sentrale begrep og sammenhenger
- Gjennomføre risikovurderinger og risikohåndtering
  - Hovedprosessen og gjennomføring av den
    - Bl.a. hvilke vedlegg o.l. man skal følge og støtte seg til underveis
- Førende prinsipper for risikohåndtering
- Førende prinsipper for risikoaksept
  - Med henvisning til hva prinsippene medfører - Vedlegg B: Kriterier for å akseptere risiko
- Forenklinger i risikoarbeidet- som skal benyttes hos oss
  - Konsekvenskategorier
  - Nivåer som måleenhet
  - Normering av nivåene for konsekvens, sannsynlighet og risiko
- Kommunisere risiko – hvordan det skal gjøres hos oss
  - Risikobeskrivelse, risikostørrelse og hvordan uttrykke risiko
- Viktige vedlegg

Difi

Innhold i Difis eksempel

- Viktige vedlegg
  - Vedlegg A: Risikoforståelse - sentrale begrep og sammenhenger
  - Vedlegg B: Kriterier for å akseptere risiko
  - Vedlegg C: Normerende beskrivelser av risikonivå
  - Vedlegg D: Normerende beskrivelser av konsekvensnivå
  - Vedlegg E: Normerende beskrivelser av sannsynlighetsnivå
  - Vedlegg F: Fremgangsmåte for å estimere nivå på konsekvens, sannsynlighet og risiko
  - Vedlegg G: Støtte ved estimat av sannsynlighetsnivå

Retningslinje: Forstå, vurdere og håndtere operativ risiko

Foreslått tilnærming

- Ta utgangspunkt i Difis eksempel og evt.
  - egne lignende dokument innen informasjonssikkerhet
  - tilsvarende fra andre internkontrollområder
- Ta stilling til relevansen av og innretning på Difis foreslåtte struktur, tema og beskrivelser
- Ut fra behov / antatt nytte
  - Aksepter
  - Juster
  - Slett
  - Legg til
  - Omstrukturer
- Forankre eller videreutvikle ulike deler og vedlegg hos toppledelsen og/eller med bred representasjon fra virksomheten
  - Vær kritisk involverende til hvem som bør og må bør involveres i hva

Difi

Prinsipper – del 1

- 4. Førende prinsipper for risikohåndteringen
  - Ressursinnsats og fokus
    - Eksempel: Ressursinnsatsen på å finne alternative arbeidsmåter og risikoreduserende tiltak skal stå i forhold til risikoens størrelse
  - Unngå risikoen
    - Eksempel: Alternative arbeidsmåter som gjør at man kan unngå risikoen, skal vurderes og eventuelt velges ut fra hensiktsmessighet, risikostørrelse og kostnad
  - Valg av risikoreduserende tiltak
    - Eksempel: Aktuelle risikoreduserende tiltak skal vurderes opp mot nytte (risikoreduserende effekt), negative sideeffekter og kostnader for øvrig
    - Eksempel: Benytt ALARP på liv og helse og nytte/kost på andre områder
  - Nye tiltak i eksisterende oppgaver og system
    - Vurder behov for midlertidige strakstiltak eller stopp i nåværende praksis
  - Tiltak i nye oppgaver og system
    - Nye arbeidsoppgaver og system skal som hovedregel ikke startes eller tas i bruk før valgte tiltak er implementert

Difi

Prinsipper – del 2

- 5. Førende prinsipper for risikoaksept
  - Størrelsen på aksepterte risikoer skal stå i et rimelig forhold til viktigheten og nytten av oppgaven/tjenesten som skaper risikoen.
  - Aksept av risikoer skal bare kunne skje når risikoen er lav eller etter at det er gjennomført en risikohåndtering i henhold til kapittel 4 Førende prinsipper for risikohåndteringen
  - Aksept av risikoer skal skje på et ledernivå som står i forhold til risikoens størrelse.
- De to prinsippkapitlene
  - Er gode diskusjonsgrunnlag for toppledelsen
  - Gir føringer for «Kriterier for å akseptere risiko»
    - Jf. vedlegg B i Difis eksempel på retningslinjen

Difi

Retningslinjen:
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.

(fortsetter)

Difi

Retningslinjen:
Forstå, vurdere og håndtere operativ risiko

Vedlegg B: Kriterier for å akseptere risiko

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.

Difi

Retningslinjen:
Forstå, vurdere og håndtere operativ risiko

Vedlegg C: Normerende beskrivelser av risikonivå

Risikomatrisen under viser hvilke kombinasjoner av konsekvensnivå og tilhørende sannsynlighetsnivå som skal gi hvilke risikonivå hos oss.

Dersom noe har ubetydelig konsekvens eller ubetydelig sannsynlighet vil risikoen hos oss alltid være ubetydelig. Vi anser ikke dette som noen risiko.

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				

Retningslinjen:
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

Difi

Retningslinjen:
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	

Difi

Sammenheng

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.

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				

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

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	

Utgangspunkt i Difis eksempel

- Se Difis eksempel:
  - Retningslinje: Forstå, vurdere og håndtere operativ risiko

Gir føringer og støtte i gjennomføring av «Få oversikt og prioritere» under hovedaktiviteten «Risikovurdering»

Retningslinje

VURDERE BEHOV FOR RISIKOVURDERINGER

Difi

Retningslinje: Vurdere behov for risikovurderinger

Innhold i Difis eksempel

2.1 Foranalyse av eget ansvarsområde

2.2 Gruppere og dele opp (ansvarsområdet)

- Ut fra kompleksitet og andre forhold

2.3 Avdekke usikkerhet for hvert delområde

- Bruk støttespørsmålene i denne retningslinjens vedlegg A
- Suppler med andre spørsmål selv ved behov
- Vurder underveis og konkluder på
  - Antatt høyeste risikonivå
    - Med støtte i den gjennomførte foranalysen
  - Nivå på egen usikkerhet - stor, moderat eller lav - mht. om risikoene kan aksepteres som de er
    - Jf. akseptkriteriene (vedlegg B) i retningslinjen Forstå, vurdere og håndtere operativ risiko
- Ved stor variasjon i usikkerheten
  - Foreta en ny oppdeling og gjenta 2.3 for de nye delen

2.4 Ta beslutning på hvert delområde ut fra beslutningskriterier som kombinerer

- antatt høyeste risikonivå
- nivå på egen usikkerhet om risikoene kan aksepteres som de er
- Jf. denne retningslinjens vedlegg B

Difi

Retningslinje: Vurdere behov for risikovurderinger

Innhold i Difis eksempel

Vedlegg B: Beslutningskriterier

Velg prioriteringsgruppe for området ut fra

- Høyeste konsekvensnivå fra spørsmål 1
- Nivå på usikkerhet fra spørsmål 10

Usikkerhet om risikoene kan aksepteres					
Nivå usikkerhet		**Prioritetsgruppe for risikovurderinger**			
	Høy	5	4	2	1
	Moderat	0	5	3	2
	Lav	0	0	6	6
		Lav	**Moderat**	**Høy**	**Svært høy**
		Konsekvensnivå			

(Man bør i arbeidet med retningslinjen systematisk vurdere innholdet i matrisen over og tabellen under, slik at man forstår hva de medfører, og kan vurdere om dette er hensiktsmessig for virksomheten. Begge kan justeres ut fra virksomhetens behov.)

Difi

Retningslinje: Vurdere behov for risikovurderinger

Innhold i Difis eksempel

(Vedlegg B fors.)

Planlegg risikovurderinger iht. tabellen under

Prioritets-gruppe	Beslutning
0	• Det er **ikke behov** for å gjennomføre nye eller oppdaterte risikovurderinger
1 - 2	• Ny/oppdatert risikovurdering skal gjennomføres **uten ugrunnet opphold** • Prioritering skal skje etter prioritetsgruppe • Nye arbeidsoppgaver skal ikke startes og nye system skal ikke tas i bruk før ny eller oppdatert risikovurdering er gjennomført og fulgt opp • Det skal straks vurderes om det er behov for eventuelle midlertidige ekstratiltak eller stopp i gjennomføring av oppgaver og bruk av IKT-system og annet utstyr.
3 - 5	• Ny/oppdatert risikovurdering skal gjennomføres **innen rimelig tid** • Prioritering skal skje etter prioritetsgruppe og ut fra kunnskapsstyrken[5] på tidligere vurderinger • Nye arbeidsoppgaver kan startes og nye system kan tas i bruk dersom de etableres innen virksomhetens fellessikring og oppgaven som skal løses er svært viktig for å nå virksomhetens overordnede mål
6	• Ny/oppdatert risikovurdering skal **gjennomføres med intervall på maks 3 år, dersom ikke ny kunnskap tilsier gjennomføring tidligere** • Omfanget skal tilpasses kunnskapsstyrken[4] på tidligere vurderinger • Nye arbeidsoppgaver kan startes og nye system kan tas i bruk dersom de etableres innen virksomhetens fellessikring og oppgaven som skal løses er svært viktig for å nå virksomhetens overordnede mål

Difi

Retningslinjen

Vurdere behov for risikovurderinger

- Er en forenklet overordnet risikovurdering
- Gjør at man kan få oversikt over
  - hvor man er mest usikker på tilstanden innen eget ansvarsområde og hvor høye risikoene der kan være
  - hvor man bør få gjennomført grundigere risikovurderinger
    - umiddelbart
    - på sikt etter en plan
  - hvor man ikke behøver å bruke ressurser på nye eller oppdaterte risikovurderinger

Retningslinjen

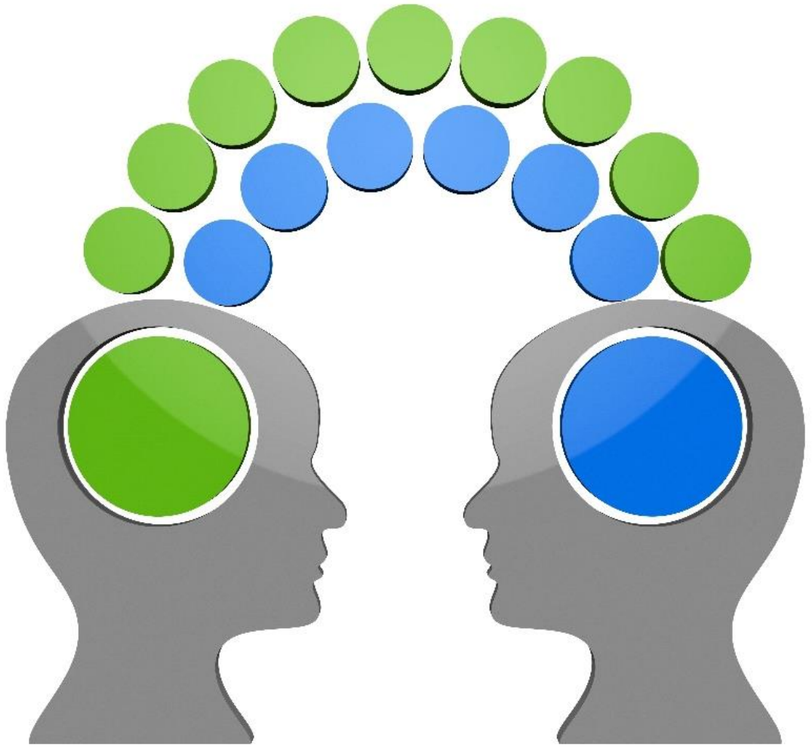
Vurdere behov for risikovurderinger

- Inngår i delaktiviteten «Få oversikt og prioritere»
  - Under hovedaktiviteten «Risikovurdering»
  - Dokumentasjonsstøtte i Difis mal nr 4 under delaktiviteten «Få oversikt og prioritere»
    - [MAL] Behov og plan for risikovurderinger-Få oversikt og prioritere

Utgangspunkt i Difis eksempel

- Se Difis eksempel:

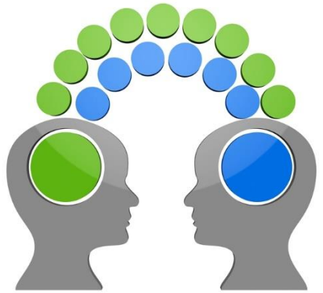
Retningslinje: Vurdere behov for risikovurderinger



REFLEKSJONSOPPGAVE

Difi

Refleksjonsoppgave 7



Diskuter hvor deres virksomhet er i forhold til Difis anbefalinger rundt innhold og innretning i de ulike overordnede styrende dokumentene. Velg noen fra listen under, og grader på følgende skala:

0 = Mangler

1 = Lite samsvar

2 = Noe samsvar

3 = Godt samsvar

Overordnede styrende dokumenter

- En kort overordnet policy for informasjonssikkerhet
- En retningslinje om roller og ansvar i internkontroll- og sikkerhetsarbeidet
  - som stiller krav til hvilke systematiske internkontrollaktiviteter som skal gjennomføres rundt om i virksomheten og hvem som skal gjøre dem
- En retningslinje om å forstå, vurdere og håndtere operativ risiko
- En retningslinje om å systematisk vurdere behov for risikovurderinger

Difi

Difi
Direktoratet for
forvaltning og ikt

Økt 19
Analysere status og Planlegge etablering/forbedring

—

Innføringskurs

Internkontroll i praksis - informasjonssikkerhet

Etableringsaktiviteten

Analysere status

- Utgangspunkt:
  - Har vi god nok oversikt og systematikk?
  - Er omfang og kvalitet på det vi har godt nok?
  - Kjenner vi risikoene godt nok?

- Status i virksomheten bør vurderes opp mot en anbefalt referanse
  - Difis veiledningsmateriell «Internkontroll i praksis – informasjonssikkerhet»
- Må også omfatte kvalitative vurderinger
  - Eksisterende overordnede styrende dokumenter i virksomheten - opp mot Difis eksempler
  - Det vi faktisk gjør i dag – opp mot Difis anbefalinger

Difi

Etableringsaktiviteten:

Analysere status

- Aktuelle dokumenter
  - Støtteark fra Difi
  - Utfylt analyseskjema
  - Et beslutningsnotat

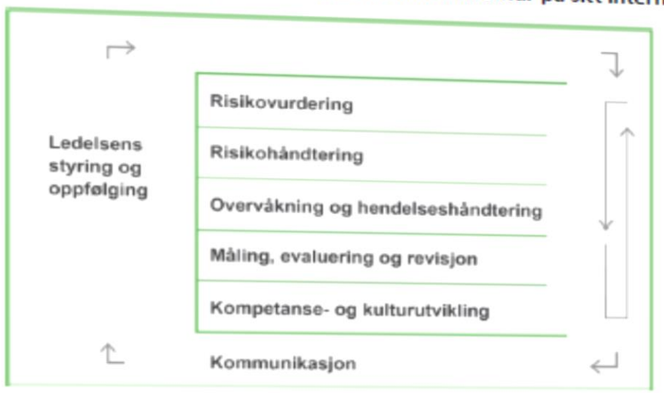
- Støtteark og analyseskjema er tilgjengelig fra «Maler og eksempler»
  - i Difis veiledningsmateriell

Støtteark fra Difi

Anbefalte delaktiviteter og dokumentasjon

Støttedokument

Dette er en samlet oversikt over de delaktiviteter og den dokumentasjon Difi anbefaler for internkontroll på informasjonssikkerhetsområdet. Oversikten er en punktvis versjon laget for å gi støtte under aktivitetene *Analysere status* og *Planlegge etablering/forbedring*. Strukturen følger hovedaktivitetene i Difis forklaringsmodell (jf. under). Det har ingen betydning for analyse og senere plan om virksomheten har valgt eller velger en annen struktur på sitt internkontrollarbeid.



Innhold

Innledning 2

1 Ledelsens styring og oppfølging 3

1.1 Virksomhetsledelsens gjennomgang 3

1.2 Delegere og følge opp gjennom linjen 3

1.3 Sikre finansielle rammer for internkontroll- og sikkerhetsarbeidet 4

1.4 Kommunisere viktighet 4

1.5 Håndtere problemstillinger løftet gjennom linjen 4

1.6 Beredskap og krisehåndtering 4

2 Risikovurdering 5

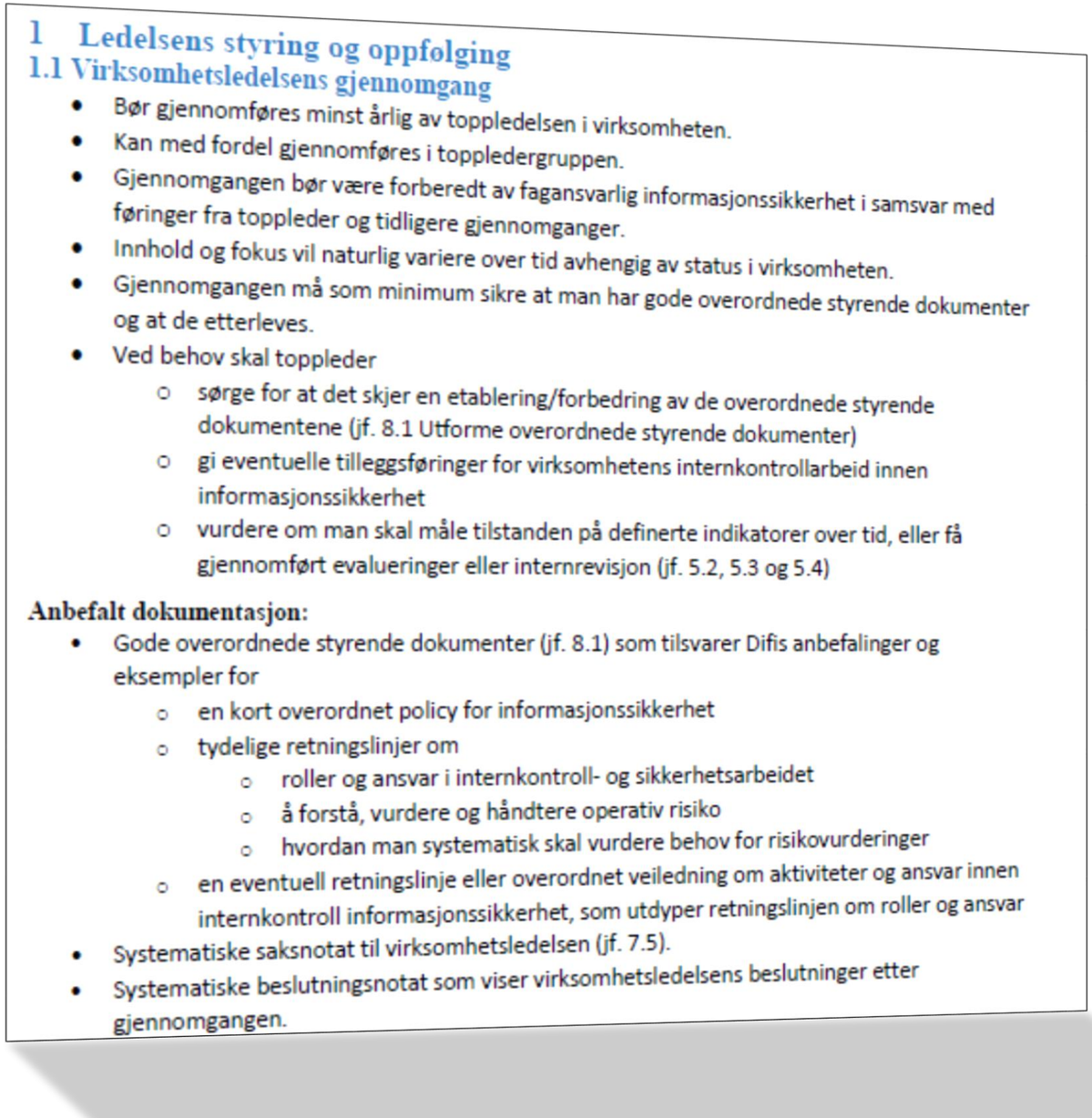
2.1 Få oversikt og prioritere 5

2.2 Analysere eksterne krav 6

2.3 Planlegge risikovurdering 6

Difi

Støtteark fra Difi
(forts.)



1 Ledelsens styring og oppfølging

1.1 Virksomhetsledelsens gjennomgang

- Bør gjennomføres minst årlig av toppledelsen i virksomheten.
- Kan med fordel gjennomføres i toppledergruppen.
- Gjennomgangen bør være forberedt av fagansvarlig informasjonssikkerhet i samsvar med føringer fra topplеder og tidligere gjennomganger.
- Innhold og fokus vil naturlig variere over tid avhengig av status i virksomheten.
- Gjennomgangen må som minimum sikre at man har gode overordnede styrende dokumenter og at de etterleves.
- Ved behov skal topplеder
    - sørge for at det skjer en etablering/forbedring av de overordnede styrende dokumentene (jf. 8.1 Utforme overordnede styrende dokumenter)
    - gi eventuelle tilleggsføringer for virksomhetens internkontrollarbeid innen informasjonssikkerhet
    - vurdere om man skal måle tilstanden på definerte indikatorer over tid, eller få gjennomført evalueringer eller internrevisjon (jf. 5.2, 5.3 og 5.4)

Anbefalt dokumentasjon:

- Gode overordnede styrende dokumenter (jf. 8.1) som tilsvarer Difis anbefalinger og eksempler for
    - en kort overordnet policy for informasjonssikkerhet
    - tydelige retningslinjer om
        - roller og ansvar i internkontroll- og sikkerhetsarbeidet
        - å forstå, vurdere og håndtere operativ risiko
        - hvordan man systematisk skal vurdere behov for risikovurderinger
    - en eventuell retningslinje eller overordnet veiledning om aktiviteter og ansvar innen internkontroll informasjonssikkerhet, som utdyper retningslinjen om roller og ansvar
- Systematiske saksnotat til virksomhetsledelsen (jf. 7.5).
- Systematiske beslutningsnotat som viser virksomhetsledelsens beslutninger etter gjennomgangen.

Difi

Analyseskjema

Analyse av status

Referanse: Difis veiledningsmateriell «Internkontroll i praksis - informasjonssikkerhet»

Om analysen

Virksomhetsnavn:		**Dato ferdig:**	
Leder av og deltakere i analysearbeidet:			

Vurderingskoder

Kodene benyttes i analyseskjemaet under.

I hvilken grad gjennomfører vi de systematiske aktivitetene og lager anbefalte dokumenter? (eller)
I hvilken grad har vi gjennomført etableringsaktivitetene og laget anbefalte dokumenter?

0	Ikke i det hele tatt, eller i liten grad
1	Noe samsvar i praksis eller i formaliserte krav, men behov for store forbedringer
2	En god del samsvar i praksis eller i formaliserte krav, men behov for en del justeringer og forbedringer
3	Tilstrekkelig samsvar i praksis, men mangler noe i formalisering/dokumentasjon
4	Tilstrekkelig samsvar i praksis og god formalisering/dokumentasjon. Ingen forbedring er nødvendig.

Behov for endring

A	Aktiviteten bør gjennomføres fullt ut
B	Deler av aktiviteten bør gjennomføres
C	Aktiviteten og anbefalt dokumentasjon bør formaliseres i retningslinje eller lignende
D	Informasjonsbehov
E	Opplæringsbehov
F	Behov for mer systematisk etterspørring/oppfølging av status gjennom linjen
G	Andre behov (spesifiser)

Prioritet (P) = 1-4, Indikerer foreløpig anbefalt rekkefølge i en kommende plan

Resurssbehov (R) = L/M/H; Lav = Bør dekkes kurant innenfor egne rammer og eksisterende ansvar; Moderat = Ikke svært omfattende, men kan kreve spesiell avklaring på ulike ledernivå; Høy = Må trolig prioriteres spesielt av virksomhetsledelsen

Difi

Analyseskjema
(forts.)

Analyse av status

Referanse: Difis veiledningsmateriell «Internkontroll i praksis - informasjonssikkerhet»

Råd for analysen og utfylling av skjemaet

- Hver av delaktivitetene under er konkretisert i støttedokumentet *Anbefalte delaktiviteter og dokumentasjon*. Bruk støttedokumentet som referanse både under utfylling og lesing av skjemaet under.

- Skriv inn relevante vurderingskoder (tall og bokstaver) i aktuelle kolonner til høyre for hver delaktivitet. Bruk kodeforklaringene på side 1 som veiledning. Skriv ikke i grå felt i analyseskjemaet. De anses ikke relevante i analysen.

- Benytt raden under hvert aktivitetsnavn til utfyllende kommentarer om det som er valgt i kolonnene til høyre. Det anbefales å bruke kommentarfeltet for alle delaktiviteter. Det gir nyttig bakgrunn og forståelse for valgte koder.

- Ved vesentlige avvik mellom status og Difis anbefalinger, kan det også være nyttig å legge inn korte kommentarer som kobler Difis anbefalinger til lignende aktiviteter virksomheten gjør på andre internkontrollområder enn informasjonssikkerhet. Det gir nyttig oversikt over sammenhenger mellom internkontrollområder og muligheter for læring og samordning.

- Dersom man mener man ikke har behov for å følge Difis anbefalinger, og ikke eller i liten grad ser behov for endringer selv om avviket mellom status og Difis anbefalinger er vesentlig, bør dette kommenteres spesielt i aktuelle kommentarfelt.

- Oppsummer resultatet fra analysen i et eget beslutningsnotat til ledelsen. Se da etter trender i vurderingskolonnene (ved å lese de vertikalt) og kommenter trendene. Se også etter konkrete områder/aktiviteter med vesentlige avvik og forbedringsbehov. Grupper gjerne oppsummeringen av de på hovedaktivitetsnivå. Benytt kommentarfeltene som støtte. Ta også med noe overordnet om prioritet og ressursbehov (jf. de to siste kolonnene). Avslutt med en begrunnet anbefaling om virksomheten bør legge en plan for etablering/forbedring av internkontroll på informasjons-sikkerhetsområdet basert på Difis anbefalinger og resultatet fra analysen, alternativt at dette ikke er nødvendig.

Difi

Analyseskjema
(forts.)

Systematiske aktiviteter	I hvilken grad gjennomføres dette?					Behov for endring (kan merke flere)							Prioritet Ress.beh	
	0	1	2	3	4	A	B	C	D	E	F	G	P	R
1 Ledelsens styring og oppfølging														
1.1 Virksomhetsledelsens gjennomgang														
Kommentarfelt....														
1.2 Delegere og følge opp gjennom linjen														
Kommentarfelt....														
1.3 Sikre finansielle rammer for internkontroll- og sikkerhetsarbeidet														
1.4 Kommunisere viktighet														
1.5 Håndtere problemstillinger løftet gjennom linjen														
1.6 Krise- og beredskapshåndtering														

Difi

Beslutningsnotat

- Til virksomhetsledelsen
- Oppsummerer analysen
- Anbefalinger med hensyn til
  - om man bør lage en plan for videre etablerings-/forbedringsarbeid
  - spesielle forhold ved planen / videre arbeid
  - hvem som bør involveres
  - overordnet estimat av omfang og tidsperspektiv
  - ..?

Etableringsaktiviteten

PLANLEGGE ETABLERING/FORBEDRING

Plan for etablering/forbedring

- Lages dersom virksomhetsledelsen beslutter det
  - etter fremlagt analyse av status
- Gjennomføringen er ofte et langsiktig arbeid
  - Planen kan være overordnet på lang sikt og detaljeres for ulike perioder underveis

Plan for etablering/forbedring

- Innhold
  - Gjennomføring av etableringsaktiviteter
    - helt eller delvis
  - Ulike tiltak rundt systematiske aktiviteter
    - Informasjon
    - Opplæring
    - De første «rundene» i gjennomføringen i ulike organisatoriske enheter
      - Spesielt fasiliteringer og støtte under «Få oversikt og prioritere», «Gjennomføre risikovurderinger» og «Foreslå håndtering av risikoer»
    - Mer systematisk etterspørring/oppfølging gjennom linjen av om det man skal gjøre er gjort
    - Annet..?

Difi

Plan for etablering/forbedring

- En ordinær prosjektplan med
  - hva som skal gjøres
  - ansvar og frister
  - status og fremdrift for rapportering

- Planen bør forankres og følges opp
  - i den ordinære virksomhetsplanleggingen
  - i virksomhetsledelsens gjennomgang innen informasjonssikkerhet

Internkontroll informasjonssikkerhet
Hvor er dere?

Er det bra nok?

Det handler om å
nå mål og resultatkrav, være effektive
etterleve lover og regler, ha pålitelig rapportering

Difis anbefaling:

- Analyse av status
  - med Difis mal
- Plan for etablering/forbedring

Difi

GRUPPEOPPGAVE

Difi

Gruppeoppgave 2

Analysere status ved hjelp av

- *Anbefalte delaktiviteter og dokumentasjon - Støttedokument*
- *Analyse av status - Analyseskjema*

Velg noen delaktiviteter. Diskuter status, og fyll ut skjemaet med

- i hvilken grad gjennomføres dette hos dere
- behov for endringer
- eventuelle kommentarer

Fordel delaktivitetene mellom virksomhetene på gruppen, slik at dere får vurdert noen delaktiviteter for hver virksomhet.

Difi

Difi
Direktoratet for
forvaltning og ikt

Økt 20
Oppsummering og avslutning

—

Innføringskurs

Internkontroll i praksis -
informasjonssikkerhet

Ledelsens styring og oppfølging
- «Hjernen» i internkontrollen

Difi

Risikovurdering
- «Hjertet» i internkontrollen

Difi

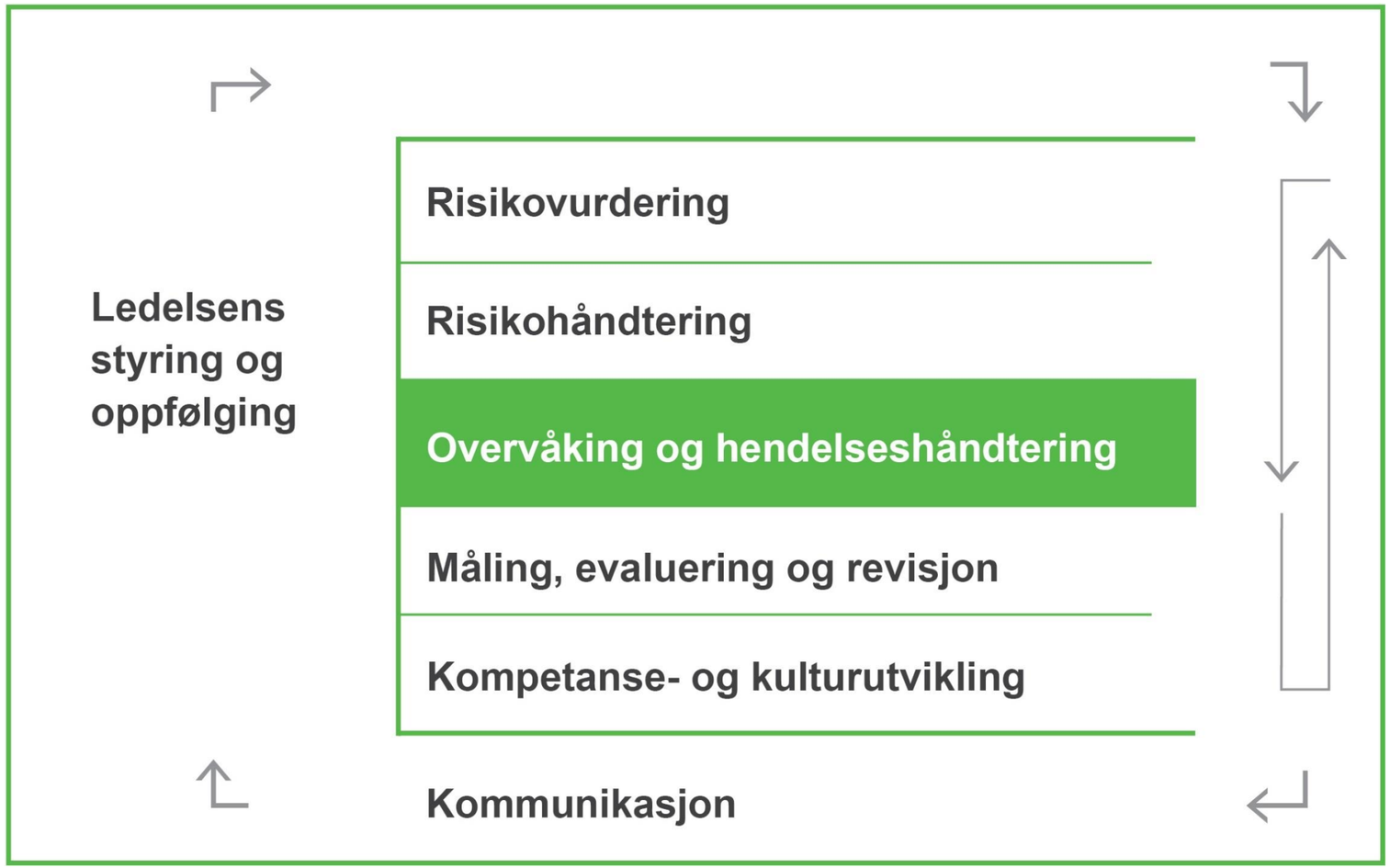
Risikohåndtering
- «Hendene» i internkontrollen

Ledelsens styring og oppfølging

- Risikovurdering
- **Risikohåndtering**
- Overvåking og hendelseshåndtering
- Måling, evaluering og revisjon
- Kompetanse- og kulturutvikling

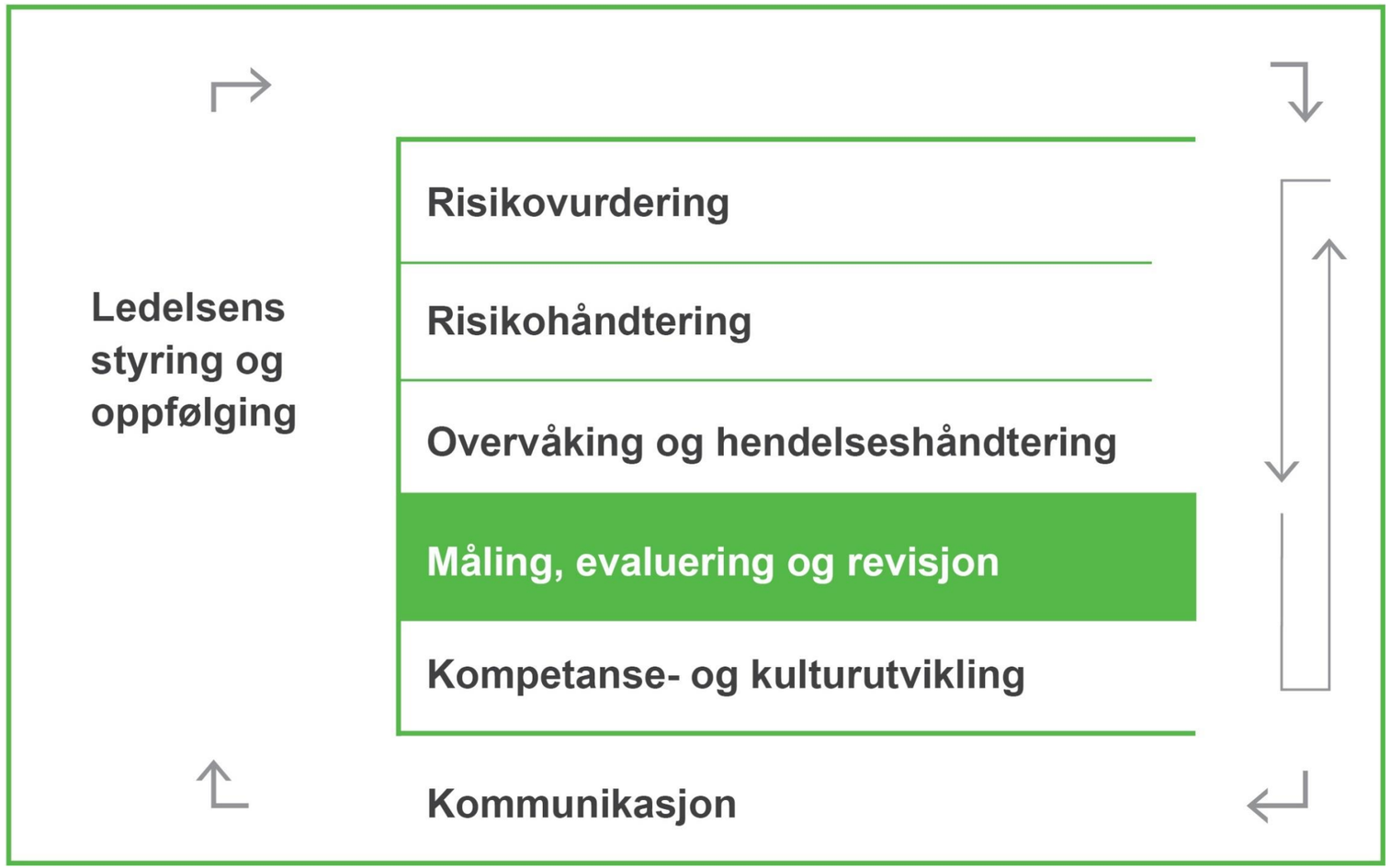
Kommunikasjon

Overvåking og hendelseshåndtering
- «Vakta» i internkontrollen



Difi

Måling, evaluering og revisjon
- «Kontrolløren» i internkontrollen

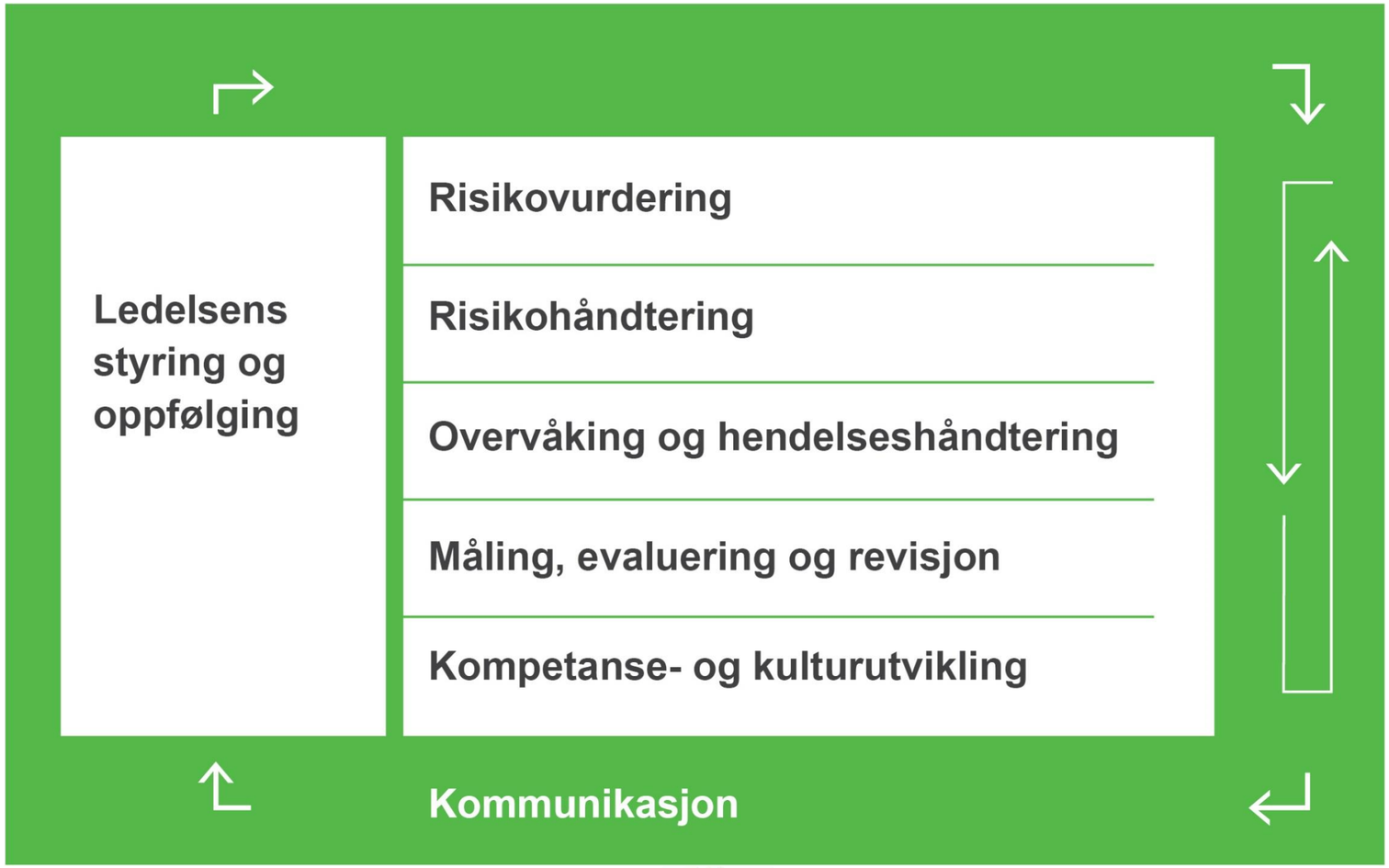


Difi

Kompetanse- og kulturutvikling
- «Læreren» i internkontrollen

Difi

Kommunikasjon
- «Limet» i internkontrollen



Difi

Internkontroll i praksis - informasjonssikkerhet

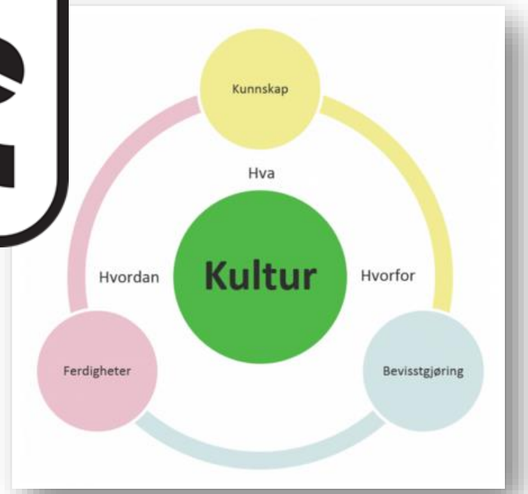
Ledelsens styring og oppfølging

- Risikovurdering
- Risikohåndtering
- Overvåking og hendelseshåndtering
- Måling, evaluering og revisjon
- Kompetanse- og kulturutvikling

Kommunikasjon

Difi

- Har dere et godt grunnlag for arbeidet med internkontroll informasjonssikkerhet?



Internkontroll i praksis - informasjonssikkerhet

Dette er betaversjon 7.0 av et veiledningsmateriell Difi utarbeider i samarbeid med brukerne. Veiledningsmateriellet er utviklet iterativt, og publisert i en serie betaversjoner frem mot ferdigstillelse i løpet av 2015. Dette er siste planlagte betaversjon. Materiellet er ikke ferdig eller endelig godkjent fra Difi før betabetegnelsen fjernes. Innholdet bør likevel være nyttig for mange allerede nå. Alle som ønsker det kan bidra med kommentarer eller delta i referansegruppe.

Difi

Aktuelle arbeidsseminar

Internkontroll i praksis - informasjonssikkerhet

- 20. november: Utforme overordnede styrende dokumenter
- 21. november: Fellessikring og tilleggssikring
- 22. november: Få oversikt og prioritere før risikovurderinger

Takk for nå!

internkontroll.infosikkerhet.difi.no

infosikkerhet@difi.no

Difi