Inspiration til risikostyring i staten

Februar 2022

ØKONOMISTYRELSEN

1. Introduktion

ØKONOMISTYRELSEN

Forord

Hvorfor risikostyring?

Risikostyring handler om proaktivt at kunne styre de ude- og indefra kommende faktorer, som kan påvirke realisering af de fastsatte mål. Effektiv risikostyring sikrer, at de væsentligste risici kan håndteres i tide og understøtter dermed langsigtet organisatorisk målopfyldelse.

Læsevejledning

Denne publikation skal inspirere til risikostyring i statslige institutioner ved at skabe kendskab til, hvad risikostyring er, hvorfor det er væsentligt, og hvordan det kan bedrives i praksis. Publikationen er ikke normerende og skal alene ses som inspirationsmateriale.

Publikationen henvender sig først og fremmest til ledere og medarbejdere, som enten skal i gang med eller allerede arbejder med risikostyring.

Publikationen tager udgangspunkt i COSOs[1] helhedsorienterede rammeværk for risikostyring[2], og fokuserer på risikostyring, der favner hele institutionen. Der eksisterer også en række andre rammeværker såsom ISO 31000, herunder den danske standard for risikoledelse[3]. Fælles for rammeværkerne er, at risikostyring ikke handler om at undgå alle risici, men derimod om bevidst at træffe beslutninger, som kan mindske sandsynligheden for og/eller konsekvensen ved, at en risiko indtræffer.

[1] Committee of Sponsoring Organizations (COSO) er en amerikansk organisation, der udvikler rammeværker for intern kontrol og risikostyring.
[2] https://www.coso.org/Documents/Compliance-Risk-Management-Applying-the-COSO-ERM-Framework.pdf
[3] https://www.ds.dk/da/om-standarder/ledelsesstandarder/iso-31000-risikoledelse

Krav til risikostyring i staten

Der stilles alene krav om, at statslige institutioner bedriver risikostyring på udvalgte områder. Det drejer sig om det finansielle område, informationssikkerhed samt ved it-projekter og bygge- og anlægsprojekter.

Bekendtgørelse om statens regnskabsvæsen m.v. stiller krav om, at ministerie-, virksomheds- og regnskabsinstrukser skal indeholde en beskrivelse af hovedelementerne i tilrettelæggelsen af den interne kontrol- og risikostyring i forbindelse med regnskabsaflæggelsen.

Derudover er det et krav, at statslige institutioner følger den internationale sikkerhedsstandard ISO 27001 til styring af informationssikkerhed.

Endelig er det et krav, at statslige it-projekter anvender statens it-projektmodel. It-projekter, hvor de samlede udgifter udgør 15 mio. kr. eller derover, skal risikovurderes af Statens It-råd. For aktstykker om bygge- og anlægsprojekter er det endvidere et krav, at de væsentligste risici beskrives.

Publikationen behandler ikke risikostyring på ovenstående områder. Her henvises til hhv. Digitaliseringsstyrelsens vejledninger til risikostyring inden for informationssikkerhed[1], risikostyring i projekter[2] og statens it-projektmodel[3], Økonomistyrelsens vejledning om intern finansiel kontrol[4] samt Finansministeriets vejledning om bygge- og anlægsaktstykker[5].

[1] https://sikkerdigital.dk/media/6835/vejledning_til_risikostyring-_nden_for_informationssikkerhed_2020.pdf
[2] https://digst.dk/media/18215/11-vejledning-til-risikostyring.pdf
[3] https://digst.dk/media/18236/01-vejledning-til-statens-it-projektmodel-v-11.pdf
[4] https://oes.dk/media/37196/vejledning-om-finansiel-intern-kontrol.pdf
[5] https://oes.dk/media/13324/retningslinjer-for-udformning-af-bygge-og-anlgsaktstykker-ny2docx.pdf

Hvad er en risiko?

Hvad er en risiko og hvad er risikostyring?

En risiko kan defineres som: *"sandsynligheden for, at en begivenhed vil indtræffe og påvirke organisationens målopfyldelse"* (COSO, 2017). En risiko udløses derfor af en årsag, og risikoen medfører en konsekvens. Dette kan illustreres i en årsagsvirkningskæde.

Figur 1: Årsagsvirkningskæde for risici

I denne publikation forstås risici som udgangspunkt som havende negative konsekvenser, mens risici andre steder *både* opfattes som havende negative (skadelige) og positive konsekvenser (muligheder).

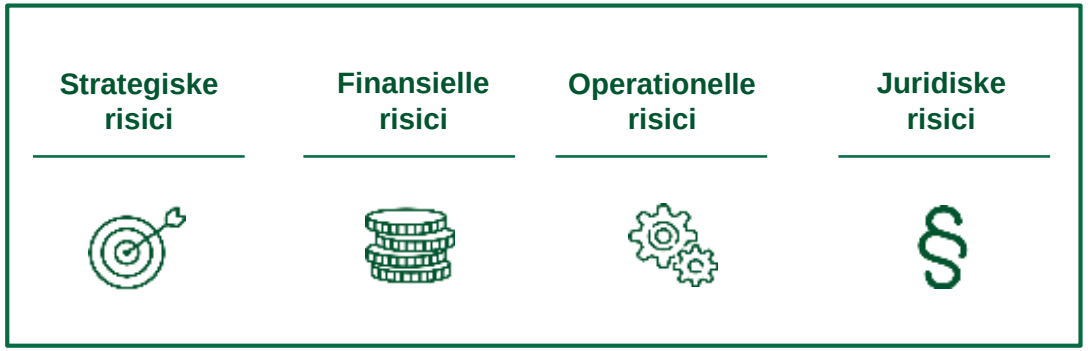
Risikostyring kan defineres som en proces, hvis formål er at identificere og imødegå potentielle risici, der kan påvirke organisationens målopfyldelse. Risikostyring gør det muligt at handle proaktivt og iværksætte mitigerende handlinger, som kan mindske sandsynligheden for og/eller konsekvensen ved, at en risiko indtræffer.

Typer af risici

Risici knytter sig til en institutions mål og opgaver. Det vil derfor variere, hvilke typer af risici der er relevante at arbejde med i de enkelte institutioner. I denne publikation fokuseres på fire generiske typer af risici, som er relevante for driften af en statslig institution: *strategiske*, *finansielle*, *operationelle* og *juridiske risici*. Hver type er nærmere beskrevet på næste side.

De fire typer er ikke udtømmende og kan suppleres med øvrige typer, som vurderes at være relevante i den enkelte institution og/eller opdeles i undertyper. De er ligeledes ikke gensidigt udelukkende og vil ofte være internt forbudne. Eksempelvis kan operationelle fejl føre til aktualisering af en finansiel risiko og omvendt.

Figur 2: Fire generiske typer af risici



Uddybning af de fire generiske risikotyper

Strategiske risici

Strategiske risici er usikkerheder, som truer realisering af strategi og strategiske målsætninger. De vil ofte opstå som følge af eksterne forhold, såsom ændringer i behov hos borgere og brugere, men kan også skyldes ændringer i interne forhold.

Eksempel: Risiko for ikke at indfri mål i institutionens mål- og resultatplan eller risiko for, at initiativer i en given reform ikke kan implementeres inden for de fastsatte rammer.

Finansielle risici

Finansielle risici er forhold, som truer institutionens finansielle processer og systemer, såsom interne og eksterne kontrolsystemer, budgetoverholdelse, likviditet mv. De vil ofte være afhængige af interne processer og systemunderstøttelse.

Eksempel: Risiko for mangelfuld intern finansiel kontrol eller risiko for manglende overholdelse af budgetter.

Operationelle risici

Operationelle risici er forhold, som truer administrative processer i institutionen. De vil ofte opstå som følge af interne procedurer, menneskelige eller it-systemmæssige fejl, eksterne begivenheder mv.

Eksempel: Risiko for, at sagsbehandlingstid ikke kan overholdes, risiko for cyberangreb og systemnedbrud eller risiko for at (nøgle)medarbejdere siger op.

Juridiske risici

Juridiske risici er forhold, som truer overholdelse af love og regler i institutionen. De vil ofte opstå som følge af regelbrud, forvaltningsretlige brud eller udfordringer med øvrig juridisk compliance i institutionen.

Eksempel: Risiko for ulovlige afgørelser, risiko for manglende lovhjemmel eller risiko for brud på GDPR-reglerne.

ØKONOMISTYRELSEN

2. Organisering og risikokultur

ØKONOMISTYRELSEN

Risikokultur er fundamentet for en effektiv risikostyring

Hvad er risikokultur?

Risikokultur kan defineres som ”*holdninger, adfærd og forståelse for risici, der påvirker ledere og medarbejderes beslutninger og afspejler institutionens mission, vision og kerneværdier*” (COSO, 2017).

Risikokulturen er således afgørende for en institutions evne til at identificere, vurdere og håndtere potentielle risici, og for at kunne bedrive effektiv risikostyring. Samtidigt er risikokulturen definerende for, om der er åbenhed, tillid og gennemsigtighed på tværs af institutionen, hvilket skaber grundlag for vidensdeling.

Når det lykkes, kan kulturen siges at være ”risikobevidst”. En risikobevidst kultur er kendetegnet ved, at ledere og medarbejdere deler viden om og reflekterer over potentielle risici, hvilket gør det muligt at ændre adfærd og handle rettidigt. En risikobevidst kultur øger dermed institutionens parathed over for kritiske hændelser.

Hvad driver en risikokultur?

Risikokulturen drives af interne forhold i institutionen. I figuren nedenfor er oplistet fire forhold, som kan påvirke risikokulturen og er værd at tage stilling til for at lykkes med at skabe en risikobevidst kultur. De fire forhold er: ledelsesforankring, governance, træning og læring, og kommunikation. Dette er uddybet på næste side.

Figur 3: Eksempel på forhold, som driver risikokulturen

Risikokulturen drives af interne forhold

Ledelsesforankring

Risikokultur skabes på flere niveauer i institutionen, men et kontinuerligt ledelsesmæssigt fokus er med til at understøtte, at der skabes en stærk kultur. Det er institutionens øverste ledelse, som sætter retning for institutionens risikostyring. Dette kan bl.a. gøres ved at ledelsen kommunikerer om værdier, ønsket adfærd og forståelse for risikostyring. Ligeledes kan den øverste ledelse efterspørge risikostyring, så det tænkes ind i de enkelte aktiviteter og projekter såvel som i større beslutninger og prioriteringer.

Governance

Governance indebærer, at der etableres en klar organisering af risikostyring i institutionen, som sikrer, at der på alle niveauer er en fælles forståelse for roller og ansvar. Dette kan nedfældes i en fælles, nedskreven risikopolitik, som sætter rammen for arbejdet med risikostyring ved at beskrive den strategiske retning og operationelle principper. Det er vigtigt, at risikopolitikken er integreret med en øvrige styring i institutionen, dvs. stemmer overens med øvrige politikker og retningslinjer, og spiller sammen med processer i institutionens årshjul. Beslutninger om risici bør træffes på rette niveau.

Træning og læring

At uddanne og træne ledere og medarbejdere i institutionens risikostyringsmodel kan sikre kendskab hertil på tværs af institutionen. Ledere og medarbejdere bør kende til organisering, politikker og retningslinjer, så de er bevidst om egne såvel som andres roller og ansvar for risikostyring. Træningen kan ligeledes involvere institutionens værktøjer til risikostyring. Herigennem skabes en fælles referenceramme og sprog for arbejdet med risikostyring.

Træning og læring kan fx ske vha. e-læringskurser og/eller fysiske kurser, som alle ledere og medarbejdere gennemfører. Kurserne kan med fordel indgå i institutionens program for onboarding af nye medarbejdere.

Kommunikation

Kommunikation henviser til, at der så vidt muligt skal være åbenhed om de risici, der identificeres og den læring, der opstår i håndteringen af dem. Det gælder både de tilfælde, hvor risikostyringen skaber værdi, men også de tilfælde, hvor det har været svært at skabe den ønskede værdi. Ved at kommunikere herom opnås dels en indsigt i værdien af risikostyringen, som har indflydelse på ledere og medarbejderes motivation, men også en fælles læring, som kan være med til at øge værdiskabelsen på sigt. Dette kan også bidrage positivt til øget tillid og gennemsigtighed på tværs af institutionen.

ØKONOMISTYRELSEN

Rolle- og ansvarsfordeling i institutionen

De tre forsvarslinjer som udgangspunkt for roller og ansvar

I arbejdet med risikostyring er det vigtigt at tage stilling til roller og ansvar. Beskrivelsen af roller og ansvar kan fx tage udgangspunkt i modellen for de tre forsvarslinjer, men kan også beskrives uden at gøre brug af modellen.

De tre forsvarslinjer beskriver tre uafhængige roller med hver sine opgaver og ansvar for risikostyring og intern kontrol mere generelt. Med udgangspunkt i modellen er det nedenfor beskrevet, hvordan ansvaret for risikostyring kan fordeles.

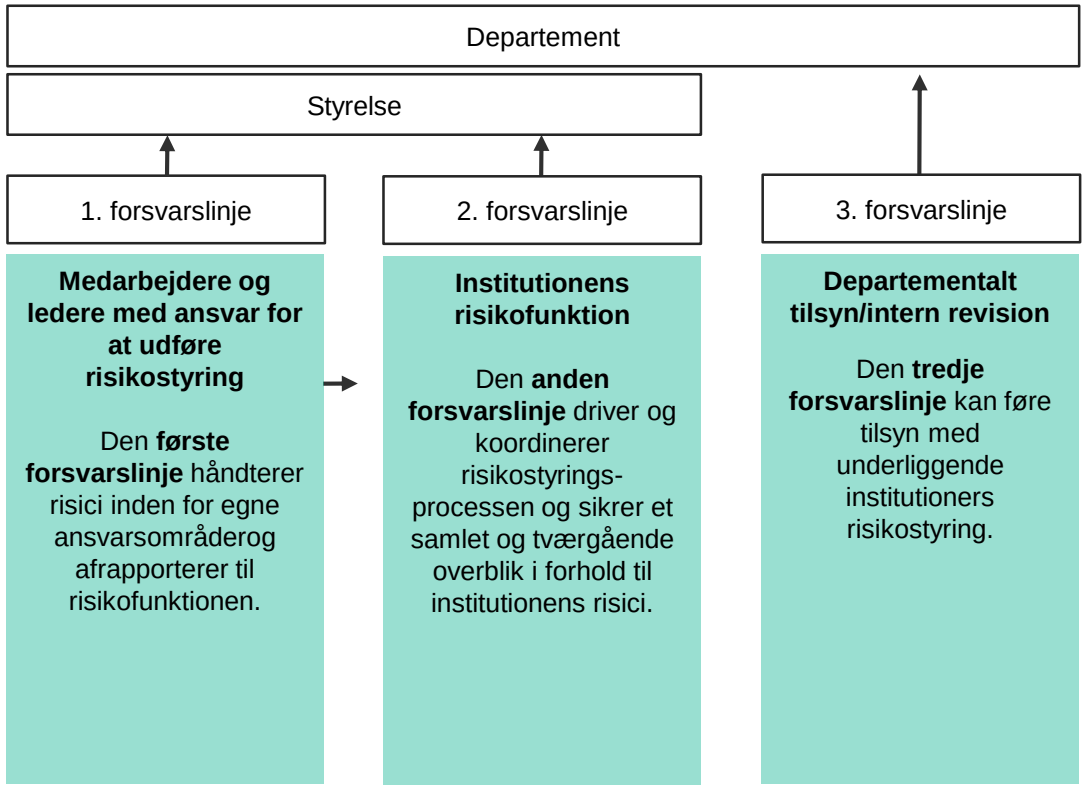
Den øverste ledelse sætter retning for risikostyringen, og har det endelige ansvar for, at risici bliver håndteret.

1. forsvarslinje er ledere og medarbejdere, som styrer risici relateret til egen opgavevaretagelse.

2. forsvarslinje er risikofunktionen, som driver institutionens risikostyring, sparrer med ledere og medarbejdere om risikostyringen, og rapporterer til den øverste ledelse.

3. forsvarslinje er det departementale tilsyn, som fører tilsyn med underliggende institutioner, og kan vælge herunder at føre tilsyn med den interne risikostyring.

De tre forsvarslinjers roller og ansvar i forhold til risikostyring



Rolle- og ansvarsfordeling i institutionen

Uddybning af ledelsens rolle og ansvaret for de tre forsvarslinjer

Fordelingen af roller og ansvar skal tilpasses den enkelte institution. Uddybningerne nedenfor er eksempler på, hvordan de kan fordeles.

Den øverste ledelses rolle og ansvar

Den øverste ledelse har det endelige ansvar for institutionens risici. Ledelsen sætter den strategiske retning for risikostyringen og fastlægger risikoappetitten, dvs. hvad institutionen vil risikere for at nå sine mål.

Ledelsen bør sikre, at der er politikker og retningslinjer for institutionens risikostyring, herunder at der er en klar rolle- og ansvarsfordeling, og at ledere og medarbejdere på alle niveauer bliver gjort bekendt med disse.

1. forsvarslinje

Ledere og medarbejdere i 1. forsvarslinje identificerer risici relateret til egne opgaver og sikrer, at de bliver håndteret. Ansvaret kan fordeles mellem en risikoejer og en risikoansvarlig.

Risikoejeren har ansvar for risikoen, og for at der følges op på håndteringen heraf. En risikoejer kan eje flere risici og kan fx være en kontorchef eller et direktionsmedlem. Den risikoansvarlige har det operationelle ansvar for at håndtere risikoen, og vil typisk være en medarbejder med reference til risikoejeren.

2. forsvarslinje

Risikofunktionen driver og koordinerer risikostyringsprocessen. Det kan fx indebære udformning af en risikopolitik på vegne af den øverste ledelse, at facilitere aktiviteter i årshjulet for risikostyring[1] og at sparre med de risikoansvarlige.

Risikofunktionen kan være en særskilt enhed eller være forankret i en relevant stabsfunktion afhængigt af institutionens organisering samt risikofunktionens opgaver. Risikofunktionen kan udgøres af én eller flere personer.

3. forsvarslinje

Det departementale tilsyn eller intern revision kan føre tilsyn med risikostyringen i underliggende institutioner. Tilsynet kan fx tage udgangspunkt i et overblik over væsentlige risici på ministerområdet.

Det departementale tilsyn eller intern revision kan være organiseret forskelligt på tværs af ministerier, og den konkrete rolle- og ansvarsfordeling samt enhedens opgaver vil derfor variere på tværs.

[1] Se årshjul for risikostyring på s. 25

3. Risikostyringsproces

ØKONOMISTYRELSEN

Risikostyring kan anskues som en proces i fire trin

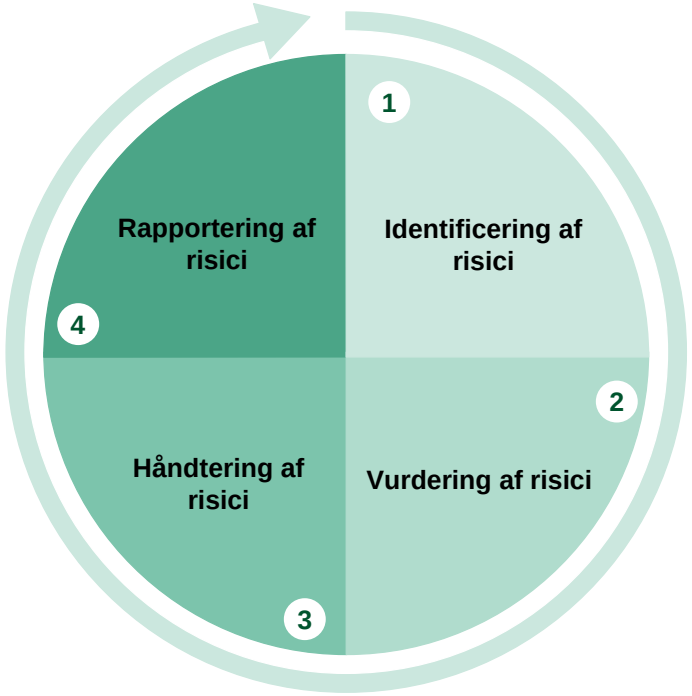
Risikostyringsprocessens fire trin

Risikostyring er en kontinuerlig proces, som kan inddeles i en række gentagne trin. Processen skal ikke opfattes som et årshjul, men som en løbende proces, der finder sted, når der sker ændringer i risikobilledet. Risikostyringsprocessen skal derfor være integreret med den øvrige styring af institutionen.

Denne publikation beskriver risikostyring som en proces i fire trin:

1. Identifikation af risici
2. Vurdering af risici
3. Håndtering af risici
4. Rapportering af risici

Hvert trin udfoldes på de følgende sider.



Trin 1: Identificering af risici

1

Hvad indebærer risikoidentifikation?

Risikoidentifikation handler om at finde, genkende og beskrive risici, der potentielt kan forhindre institutionen i at nå sine mål.

En god og præcis risikoidentifikation kan være en forudsætning for, at den videre risikostyringsproces forløber hensigtsmæssigt. Det er derfor vigtigt at være åben over for mulige risici i identifikationsprocessen og senere frasortere de risici, som ikke er tilstrækkeligt væsentlige. Det kan være en omfattende proces, som også stiller krav om efterfølgende prioritering.

Der kan være mange forskellige kilder til risici, og det vil variere, hvad der driver risici i de enkelte institutioner. Risici kan være drevet af interne forhold, fx ressourcer og kompetencer, eller ændringer i omgivelserne såsom politiske forhold, der fx medfører stigning i antallet af en given type sager.

Når risici skal identificeres, kan det være en god idé at inddrage både ledere og medarbejdere fra relevante enheder. Udover at de besidder den nødvendige viden til at kunne identificere risici, kan inddragelse bidrage til en følelse af ansvar og ejerskab til risici, som er afgørende for at drive en effektiv risikostyringsproces, hvor risikoejere og risikoansvarlige løfter deres ansvar. Endelig er inddragelse med til at øge risikobevidsthed og forståelse for risikostyringsprocessen i institutionen.

Hvordan identificeres risici?

Som beskrevet indledningsvist, er en risiko en hændelse, som kan opstå som følge af en eller flere årsager, og som, hvis den indtræffer, vil føre til en eller flere konsekvenser. Dette er illustreret nedenfor. I identifikation af risici skal der være blik for såvel årsagerne som selve hændelsen og de potentielle konsekvenser heraf. Ikke mindst fordi konsekvenser kan have en potentielt forstærkende effekt og føre til nye risici.

Figur 4: Årsagsvirkningskæde for risici

En hændelse kan eksempelvis være, at der sker fejl i udbetaling af tilskud, hvilket kan give anledning til en revisionsbemærkning. En årsag til hændelsen kan være manglende kompetencer eller kvalitetssikring, og konsekvensen kan bl.a. være påvirkning af berørte borgeres økonomi. De samme årsager – manglende kompetencer eller kvalitetssikring – kunne også give anledning til en forkert forvaltningsmæssig afgørelse, som ligeledes kan påvirke borgere eller virksomheder negativt.

Formålet med at se på en risiko ud fra en årsagsvirkningskæde er at identificere tiltag, som kan mindske sandsynligheden og/eller konsekvensen ved hændelsen. Dette udfoldes nærmere i trin 3.

Trin 1: Identificering af risici

1

Eksempler på tilgange til at identificere risici

Identificering af risici kan fx ske gennem interviews eller workshops med relevante ledere og medarbejdere. I dette afsnit beskrives eksempler på tre tilgange til identifikation af risici, som også kan danne grundlag for interviews og workshops. De forskellige tilgange kan kombineres for bedst muligt at sikre, at de væsentligste risici identificeres.

Risikobilledet er i konstant forandring, og det er vanskeligt at identificere alle risici på én gang. Processen for risikoidentifikationen kan derfor gentages minimum én gang årligt og ved alle større ændringer. Ideelt set indtænkes risikoarbejdet i alt løbende arbejde.

Den generiske tilgang fokuserer på at identificere risici ud fra et eksisterende kendskab til risici, fx risici der tidligere er opstået eller typiske risici relateret til en konkret opgave- eller projekttype.

Dette kan gøres ved at anvende ”tjeklister” over kendte risici, der tidligere er identificeret og vurdere, om de fortsat er relevante, fx ved en årlig risikovurdering af institutionens risici. Det kan også være i forbindelse med nye opgaver eller projekter, hvor ”tjeklister” over kendte risici på det givne område gennemses. Det kan være effektivt at tage udgangspunkt i kendte risici frem for at starte fra bunden, men det kan kræve kritisk sans i forhold til, om de enkelte risici er relevante.

Den målbaserede tilgang fokuserer på at identificere risici med udgangspunkt i institutionens strategiske mål. Enhver begivenhed, der kan forhindre, at et mål nås, kan identificeres som en risiko.

Dette kan fx gøres ved at tage udgangspunkt i strategiske mål i institutionens mål- og resultatplan eller rammekontrakt, eller i mål fastsat på afdelings- eller kontorniveau omkring det som er strategisk vigtigst at lykkedes med. Med udgangspunkt i målet stilles spørgsmålet *”hvad kan gå galt, som gør, at vi ikke når vores mål?”* dvs. hændelser, der medfører den konsekvens, at målet ikke nås.

Den procesbaserede tilgang fokuserer på at identificere risici ved at skabe overblik over alle aktiviteter i en proces, og derigennem kunne se, hvornår i processen risici opstår.

Dette kan gøres ved at kortlægge en given proces end-to-end, dvs. kortlægge samtlige aktiviteter i processen. Det kan fx være en finansiel proces for udbetaling af støtte og tilskud. Med udgangspunkt i delprocesser og aktiviteter stilles spørgsmålet *”hvad kan gå galt, som gør, at der sker fejl”*. Fejlene kan være af forskellig karakter og relateret til såvel strategiske som finansielle, operationelle eller juridiske risici.

Trin 1: Identificering af risici

1

Værktøj til identificering af risici

De identificerede risici kan oplistes i en risikolog. Risikologgen giver overblik over risici i de enkelte enheder, og fungerer som afrapportering til risikofunktionen.

Nedenfor er et eksempel på et udsnit af risikologgen[1], hvor nogle af de kolonner, der er relevante at udfylde under dette trin, fremgår. I loggen tildeles hver risiko et unikt nummer/ID. Risikoen beskrives kort, men tilstrækkeligt fyldestgørende til, at den er forståelig for personer i andre dele af institutionen. For at sikre at det er tydeligt, hvem der har ansvar for at følge op på risikoen, angives den ansvarlige enhed, og risikoen tildeles risikoen en risikoejer og risikoansvarlig.

Tabel 1: Eksempel på risikolog

ID	Beskrivelse af risiko	Risikotype	Ansvarlig enhed	Risikoejer	Risiko-ansvarlig
1	[Indsæt]	Strategisk/finansiel/ operationel/juridisk	[indsæt]	[indsæt]	[indsæt]
2	[Indsæt]	Strategisk/finansiel/ operationel/juridisk	[indsæt]	[indsæt]	[indsæt]
3	[Indsæt]	Strategisk/finansiel/ operationel/juridisk	[indsæt]	[indsæt]	[indsæt]
…					

[1] Risikologgen kan hentes på Økonomistyrelsens hjemmeside.

Hvem kan have ansvaret for at identificere risici?

Inden risici bliver identificeret, kan der med fordel gøres overvejelser om roller og ansvar knyttet til opgaven. Typisk vil den øverste ledelse sætte retning for processen, fx ved at fastlægge, hvilke overordnede typer af risici der fokuseres på. Processen vil dog oftest involvere en større del af institutionen, hvor både ledere og medarbejdere på flere niveauer bidrager.

Selve processen kan med fordel være drevet af en koordinator eller en koordinerende enhed, fx en risikofunktion, som på vegne af den øverste ledelse sikrer, at de væsentligste risici bliver identificeret. Da det kræver en vis indsigt i et opgaveområde at kunne identificere de væsentligste risici, kan selve identifikationen som regel bedst foretages af de ledere og medarbejdere, der sidder med området til dagligt. De vil både være placeret i 1. og 2. forsvarslinje, fx både i fagkontorer og stabsfunktioner.

Trin 2: Vurdering af risici

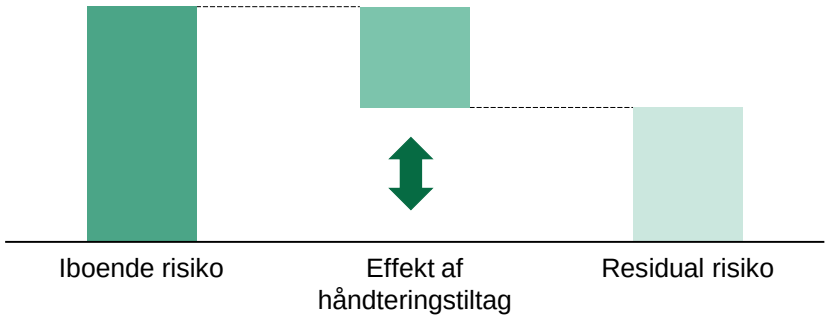
Hvad indebærer risikovurdering?

Risikovurdering handler om at analysere og vurdere de identificerede risici. Det er både den iboende og den residuale risiko, der vurderes.

Den iboende risiko er den risiko, der vurderes at være, når risikoen identificeres, dvs. *før* der iværksættes tiltag til håndtering. Vurderingen af den iboende risiko er afgørende for efterfølgende at kunne håndtere risikoen mest effektivt. *Den residuale risiko* er den risiko, der vurderes at være tilbage, dvs. *efter* der er iværksat tiltag til håndtering af risikoen.

Risikoappetitten er den samlede værdi, som institutionen er villig til at risikere for at nå sine mål. Risikoappetitten fastlægger således på et strategisk niveau, hvornår der bør og ikke bør løbes en risiko. De tiltag, der iværksættes for at mindske risikoen, skal derfor bringe den residuale risiko på niveau med eller under risikoappetitten. Se figuren nedenfor.

Figur 5: Illustration af iboende og residual risiko



Det er den øverste ledelse, der fastlægger risikoappetitten. Den er typisk kvalitativt fastlagt, fx som *lav*, *mellem* eller *høj*, og kan variere mellem typer af risici. Institutionen kan eksempelvis have en lavere risikoappetit for finansielle risici end for strategiske risici. Dermed fungerer risikoappetitten som en rettesnor for risikovurderingen.

Mens risikoappetitten sætter en øvre grænse for, hvad institutionen på et strategisk niveau er villig til at risikere, er risikotolerancen et operationelt og ofte kvantitativt mål for variation i performance i forhold til specifikke risici. *Risikotolerance* er det acceptable niveau af variation, som institutionen er villig til at acceptere for at realisere sine mål. Eksempler på de to begreber fremgår af figuren nedenfor.

Figur 6: Eksempler på risikoappetit og -tolerance

Risikoappetit	Risikotolerance
Mellem risikoappetit ift. manglende målopfyldelse i mål- og resultatplan	Min. 75 pct. af målene i mål- og resultatplanen skal være helt eller delvist opfyldt.
Lav risikoappetit ift. manglende overholdelse af love og regler	Alle love og regler skal overholdes.
Lav risikoappetit ift. fejl i sagsbehandlingen	Min. 95 pct. af alle sager skal afgøres korrekt.

Trin 2: Vurdering af risici

Hvordan vurderes risici?

En risiko vurderes ud fra en kombination af sandsynligheden for og konsekvensen ved, at risikoen indtræffer. Tilsammen giver det en risikoscore, som indikerer, hvor væsentlig risikoen er.

Risikoens *sandsynlighed* og *konsekvens* vurderes på en valgt skala fra fx 1 til 3 eller fra 1 til 5, som her anvendes som eksempel. Sandsynligheds- og konsekvensskalaer kan ligeledes anvendes til at definerer de enkelte trin nærmere og dermed hjælper med at sikre en objektiv vurdering af risikoen. Dette uddybes på næste side.

Vurderingen af risikoens sandsynlighed og konsekvens indtastes i risikologgen[1], som vist i udsnittet nedenfor. Herefter ganges værdien af hhv. risikoens sandsynlighed og konsekvens sammen for at få den samlede risikoscore. På en skala fra 1-5 vil den laveste risikoscore være 1 og den højeste 25.

Tabel 2: Eksempel på risikolog

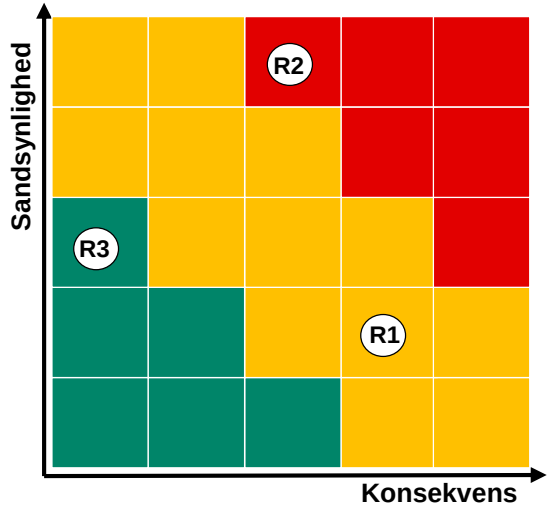
ID	Beskrivelse af risiko	Sandsynlighed	Konsekvens	Risikoscore
1	[Indsæt]	2	5	10
2	[Indsæt]	5	4	20
3	[Indsæt]	3	2	6
…				

[1] Risikologgen kan hentes på Økonomistyrelsens hjemmeside.

Risici fra risikologgen kan plottes ind i en risikomatrice eller et heatmap, som viser, hvordan risiciene placerer sig relativt til hinanden. For at visualisere hvor alvorlige risiciene er kan matricens områder farves, ligesom risikoappetit og -tolerance kan indtegnes. Det vil sige, at det bliver muligt at se, hvis en given risiko ligger over den fastsatte risikoappetit. I praksis bør risikomatricen tilpasses til det enkelte ministerium eller institution.

Nedenfor et eksempel på en risikomatrice, hvor de tre risici fra risikologen er indsat.

Figur 7: Eksempel på risikomatrice



Trin 2: Vurdering af risici

Sandsynlighedsskala

For at sikre en objektiv vurdering af risikoens sandsynlighed og konsekvens på den valgte skala, og muliggøre sammenligning af risici på tværs af enheder i institutionen, kan der med fordel anvendes sandsynligheds- og konsekvensskalaer.

Formålet med en sandsynlighedsskala er at kunne vurdere, hvor sandsynligt det er, at risikoen indtræffer. Nedenfor er vist et eksempel på en sandsynlighedsskala med en beskrivelse af hvert trin samt en angivelse af en procent. Der er forskellige præferencer i anvendelsen af sandsynlighedsskalaer, herunder om beskrivelser, procenter eller lignende fungerer bedst.

Tabel 3: Eksempel på sandsynlighedsskala

Trin	Sandsynlighed
1. Sjælden eller usandsynlig	< 1 pct.
2. Vil næppe forekomme	1 - 10 pct.
3. Er mulig	10 - 30 pct.
4. Må forventes at forekomme	30 - 75 pct.
5. Vil helt sikkert forekomme	Over 75 pct.

Konsekvensskala

Formålet med en konsekvensskala er at vurdere virkningen af, at risikoen indtræffer. Konsekvensskalaen kan opdeles i dimensioner, som er relevante for den enkelte institution. Dimensionerne kan fx være økonomisk tab for styrelsen, omdømme og politiske konsekvenser, realisering af projekter og opgaver og strategiske målsætninger. Dette kan tilpasses til det enkelte ministerium eller institution afhængigt af, hvad der vurderes mest væsentligt at styre på.

Nedenfor ses et eksempel på hvordan en konsekvensskalaen kan bygges op.

Tabel 4: Eksempel på konsekvensskala[1]

Trin	Dimension 1	Dimension 2	Dimension 3	Dimension 4
1. Uvæsentlig				
2. Mindre				
3. Nogen				
4. Stor				
5. Uacceptabel				

[1] På Økonomistyrelsens hjemmeside kan der ses eksempler på en konsekvensskala fra Landbrugsstyrelsen og Miljøstyrelsen.

Trin 2: Vurdering af risici

Hvordan prioriteres risici?

Prioritering af risici kan bidrage til at en mere informeret beslutningstagning, hvor ressourcerne prioriteres til de risici, der er mest kritiske for institutionen. Prioriteringen af risici bør altid ske ud fra institutionens risikoappetit.

Det kan være nyttigt at gøre brug af prioriteringskriterier, der kan bruges til at vurdere og prioritere risici. Det giver en helhedsforståelse for risikoen og dens omfang. Nedenfor ses et eksempel på fire prioriteringskriterier, som, foruden risikoappetitten, kan anvendes som retningslinje for prioritering.

Figur 8: Eksempel på prioriteringskriterier

- **Kompleksiteten** af risici. Hvad er omfanget af risikoen og hvordan påvirker risikoen institutionen.
- **Hastigheden** på hvor hurtig risikoen udvikler sig eller hvor risikoen rammer institutionen
- **Udholdenhed** i institutionen. Hvor lang tid vil risikoen kunne have en effekt på institutionen.
- **Gendannelse** i institutionen. Hvor hurtig vil institutionen komme sig, hvis en hændelse indtræffer.

Hvem kan have ansvaret for at vurdere risici?

Vurderingen af risici tager som nævnt udgangspunkt i institutionens risikoappetit, som fastlægges af den øverste ledelse. Med udgangspunkt heri kan de identificerede risici vurderes.

Vurderingen involverer ligesom identifikationen af risici ledere og medarbejdere på flere niveauer i institutionen. De ledere og medarbejdere, som har identificeret risici på eget opgaveområde, vil typisk også være mest kvalificeret til at vurdere risici.

Den valgte koordinator eller koordinerende enhed, fx en risikofunktion, kan med fordel udfordre vurderingerne, så der sikres ensartede vurderinger på tværs af institutionen. Vurderingen af alle risici kan efterfølgende indtastes i en risikolog eller tilsvarende oversigt, så der er et samlet overblik over de risici, der arbejdes med.

Trin 3: Håndtering af risici

3

Hvad indebærer risikohåndtering?

Risikohåndtering handler om at finde ud af, hvilke strategier der bedst håndterer de identificerede risici og nedbringer risikoen. Som beskrevet under forrige trin, er målet at nedbringe risikoen, så den residuale risiko er på niveau med eller under risikoappetitten.

Hvordan håndteres risici?

Der findes forskellige strategier til risikohåndtering og det afhænger af vurderingen af den enkelte risiko, hvilken strategi der er relevant. I denne publikation præsenteres fire strategier: 1) accept af risiko, 2) undgå risiko, 3) reducere risiko, eller 4) overføre/dele risiko.

Hvis risikoen vurderes at have en lav sandsynlighed og konsekvens, kan en passende strategi være at *acceptere* risikoen. Hvis risikoen omvendt har en høj sandsynlighed og konsekvens, kan det være nødvendigt at *undgå*, *reducere* eller *overføre* risikoen.

Et eksempel kan være risiko for fejl i sagsbehandling af en ny type af sager med stor politisk bevågenhed. Sandsynligheden kan fx vurderes at være høj, hvis kun få medarbejdere har de fornødne kompetencer. Samtidigt kan konsekvensen vurderes at være høj, da det både kan få økonomisk og politisk betydning. For at reducere risikoen kan der fx afholdes et internt kursus i lovgrundlaget, indføres sidemandsoplæring eller lignende tiltag.

Figur 9: Strategier til risikohåndtering

At **acceptere** risikoen betyder, at risikoen overvåges, men at der ikke iværksættes mitigerende handlinger. Strategien anvendes typisk, hvis det vurderes, at der er meget begrænset mulighed for at reducere den residuale risiko til det ønskede niveau, eller hvis omkostninger ved at håndtere risikoen ikke står mål med det forventede udbytte.

At **undgå** risikoen betyder, at den årsagsgivende aktivitet stoppes med henblik på at eliminere risikoen. Strategien vil ikke altid være mulig at anvende i praksis.

At **reducere** risikoen betyder, at der iværksættes handlinger, der enten kan mindske sandsynligheden for eller konsekvensen ved, at risikoen indtræffer. Der kan også iværksættes handlinger, som har til hensigt at holde risikoen under kontrol. En risiko reduceres oftest, hvis risikoen er over institutionens risikoappetit

At **overføre eller dele** risikoen betyder, at risikoen bæres af flere aktører. Det kan fx være ved at udlicitere til eller betale en tredjepart for at bære hele eller dele af risikoen.

Trin 3: Håndtering af risici

Hvordan håndteres risici? (fortsat)

Det er vigtigt at have for øje, at risikobilledet løbende udvikler sig som følge af ændringer i interne forhold eller i omgivelserne. Den valgte strategi til håndtering af risici og de handlinger, der evt. er iværksat, kan derfor løbende genbesøges for at sikre, at håndteringen er effektiv. Kadence og tidspunkt for opfølgning vil afhænge af vurderingen af væsentligheden af den enkelte risiko.

Håndteringen af hver risiko angives i risikologgen[1]. Det angives, hvordan risikoen bliver håndteret, herunder hvilke evt. mitigerende handlinger eller handleplaner, der er iværksat.

Tabel 5: Eksempel på risikolog

ID	Beskrivelse af risiko	Strategi	Mitigerende handlinger
1	[Indsæt]	Accepter/undgå/reducer/overfør	[indsæt]
2	[Indsæt]	Accepter/undgå/reducer/overfør	[indsæt]
3	[Indsæt]	Accepter/undgå/reducer/overfør	[indsæt]
…			

Udover ovenstående information bør det også fremgå, hvornår handlingerne er iværksat, og hvornår der planmæssigt følges op på håndteringen af risikoen.

[1] Risikologgen kan hentes på Økonomistyrelsens hjemmeside.

Hvem kan have ansvaret for at håndtere risici?

Når risici er identificeret og vurderet, bør der tages stilling til, hvordan ansvaret for at håndtere risici skal fordeles.

For hver risiko kan der angives en risikoejer og en risikoansvarlig, som har ansvaret for den enkelte risiko, herunder at beslutte og iværksætte strategier og handlinger for håndtering af risikoen. Dette sikrer, at der en tydelig ansvarsplacering for håndtering af hver risiko. Typisk vil risikoejeren være den kontorchef, der har det primære ansvar for området, mens den risikoansvarlige vil være en medarbejder, der refererer til vedkommende.

Den valgte koordinator eller koordinerende enhed kan indgå i forbindelse med håndteringen ved at følge op på, om de iværksatte handlinger udføres og genbesøges løbende.

Trin 4: Rapportering af risici

4

Hvad indebærer risikorapportering?

Risikorapportering har til formål at skabe et grundlag for prioritering og beslutningstagning, og gør det muligt for den øverste ledelse at følge op på håndteringen af risici. Det er derfor vigtigt, at rapporteringen er fyldestgørende og opdateret, så den skaber værdi som værktøj for ledelsen.

For at skabe mest muligt værdi bør risikorapporteringen alene fokusere på de væsentligste risici for den pågældende målgruppe, fx kontorchefen for en given enhed eller den øverste ledelse. De væsentligste risici vil være de mest kritiske risici og de risici, der snarest skal følges op på. Det kan fx være i revisionsbemærkninger fra Rigsrevisionen med snarlig frist.

Det er op til det enkelte ministerium og institution at vurdere, hvilke risikorapporteringer, der er meningsfulde. Det vil ofte være hensigtsmæssigt med rapporteringer til:

Kontorchefer (1. forsvarslinje)

Den øverste ledelse

Risikofunktionen (2. forsvarslinje)

Intern revision/ tilsynsenhed/ departement (3. forsvarslinje)

Det er ikke nødvendigt at rapportere på alt. Nedenfor ses nogle eksempler på, hvad der kan indgå i en risikorapportering.

Figur 10: Eksempler på emner i en risikorapportering

Hvordan ser **risikobilledet i fremtiden** ud? Risikobilledet kan vises som en kvantitative visualisering af de risici, der har en residual score over risikoappetitten. Risikobilledet kan også vise en beskrivelse og indledende vurdering af potentielle risici eller risikoområder.

Hvad er der sket med **risikoen siden sidst**? Det kan vises som en kvantitativ opgørelse over, om der er flere eller færre kritiske risici, siden sidst. Der kan ligeledes laves et opgørelse over, hvilke mitigerende handlinger der er taget i brug for at begrænse effekten.

Hvordan går det med **medarbejdere og risikokulturen**? Der kan gives en status på potentielle initiativer med fokus på områder som ledelsesforankring, træning og læring, kommunikation om risikostyring og evaluering af kompetencer.

Efterleves egen **risikopolitik**? En gang om året kan der gives status på efterlevelsen af risikopolitikken i institutionen og en vurdering af, hvor institutionen ligger på modenhedstrappen.

Trin 4: Rapportering af risici

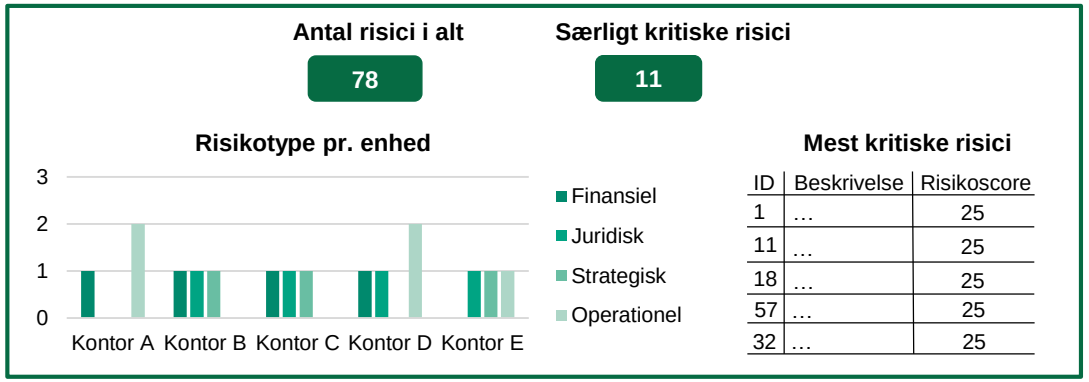
4

Hvordan rapporteres risici?

Risikorapporteringen er baseret på data fra institutionens risikolog, som viser det samlede billede af risici på tværs af institutionen. Risikologgen kan eksempelvis være en Excel baseret løsning eller en database, som udvalgte ledere og medarbejdere kan tilgå og opdatere løbende.

Data fra risikologgen kan med fordel indgå i den løbende ledelsesinformation og være visualiseret i et Dashboard, som skaber overblik over væsentligste risici og udviklingen heri. Dette kan fx gøres ved hjælp af en Excel baseret løsning eller vha. integration til MS Power BI/Statens BI. Nedenfor ses et eksempel på ledelsesinformation om risikostyring fra et Dashbord[1].

Figur 11: Eksempel på Dashboard til ledelsesrapportering



[1] Risikologgen inkl. visualisering i Excel kan hentes på Økonomistyrelsens hjemmeside.

Hvem kan have ansvaret for at rapportere risici?

Når risici skal rapporteres, bør der tages stilling til de interne processer for rapportering. Der kan dels gøres overvejelser om, hvem der har ansvar for at rapportere risici, men også hvem der modtager rapporteringerne, hvad indholdet skal være og hvor ofte, der skal rapporteres. Det kan fx være overvejelser om, hvilke risici der forelægges den øverste ledelse i institutionen eller departementet. For at skabe mest mulig værdi bør rapporteringen ske med en kadence, der gør det muligt at følge udviklingen løbende og handle proaktivt.

Det kan være den valgte koordinator eller koordinerende enhed, fx en risikofunktion, der indsamler informationer fra relevante enheder og sikrer, at risici bliver rapporteret videre til de valgte modtagere.

4. Årshjul og drift af koncept

ØKONOMISTYRELSEN

Årshjul for risikostyring

Hvordan kan årshjulet for risikostyring se ud?

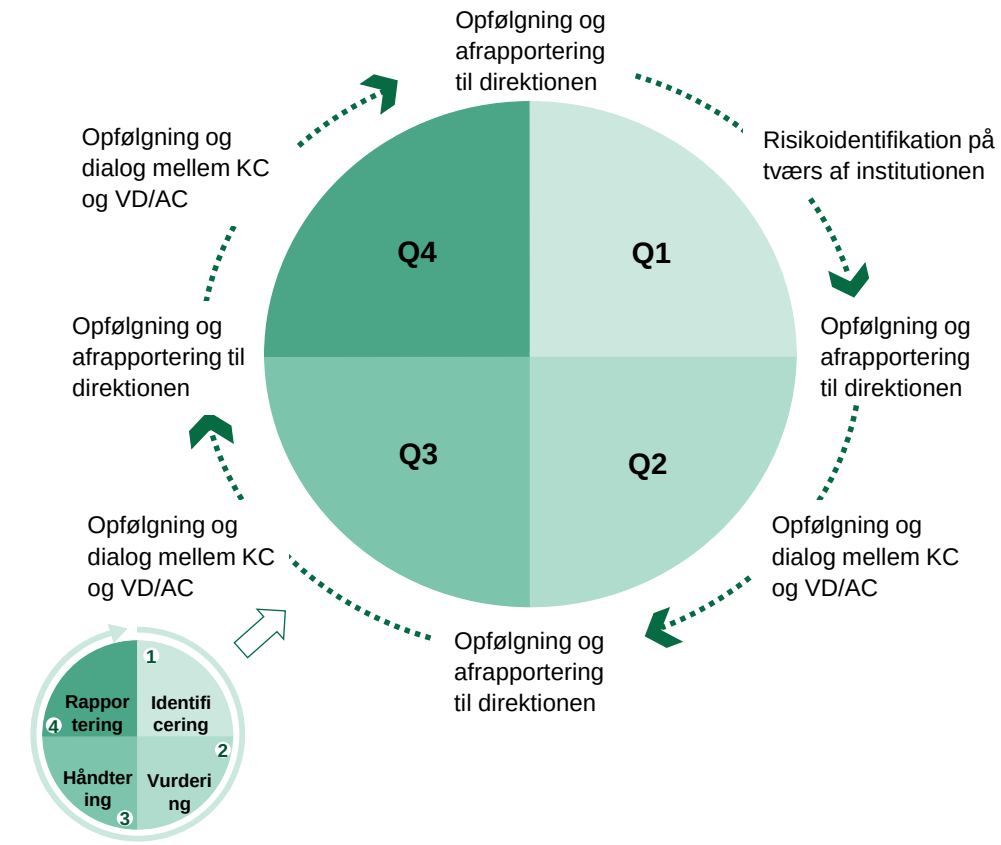
Et sammentænkt årshjul kan bidrage til at tydeliggøre de interne afhængigheder, der er mellem risikostyringsaktiviteter og administrative processer for strategi, økonomi og HR. Årshjul kan bruges til at understøtte en effektiv styringsmodel, skabe gennemsigtighed og begrænse kompleksiteten i institutioner.

Risikostyring er en løbende proces, der giver institutionen mulighed for at blive opmærksom og være foran nye risici. Årshjulet for risikostyring kan ses som en struktureret tidslinje for risikostyringsaktiviteter.

Til højre ses et eksempel på et årshjul for risikostyring. I eksemplet påbegyndes processen for risikoidentifikation og risikovurdering i starten af året, og herefter følges der løbende op på risikobilledet. Det kan være nyttigt, at de væsentlige risici med en fast kadence afrapporteres til den øverste ledelse, fx månedligt eller kvartalsvist. Ligeledes kan det være en fordel, at kontorchefer/fagchefer og vicedirektører/afdelingschefer med en fast kadence mødes og drøfter de væsentligste risici.

Sideløbende med rapporteringen gentages risikostyringsprocessen, som ikke nødvendigvis skal følges i en bestemt rækkefølge. I den forbindelse er det vigtigt at have fokus på løbende ændringsstyring, dvs. at institutionen skal være åben over for, at der kan opstå nye risici, eller at identificerede risici ændrer sig.

Figur 12: Eksempel på årshjul for risikostyring



Løbende risikostyringsproces

Rammeværk for risikostyring

Hvordan kan et rammeværk for risikostyring se ud?

Risikostyringen er mest effektiv, når den er helhedsorienteret, dvs. går på tværs af institutionen og omfatter alle de områder, hvor institutionen kan være udsat for væsentlige risici. Det kan være en fordel, hvis risikostyringen er integreret med den eksisterende styringsmodel og interne processer i institutionen.

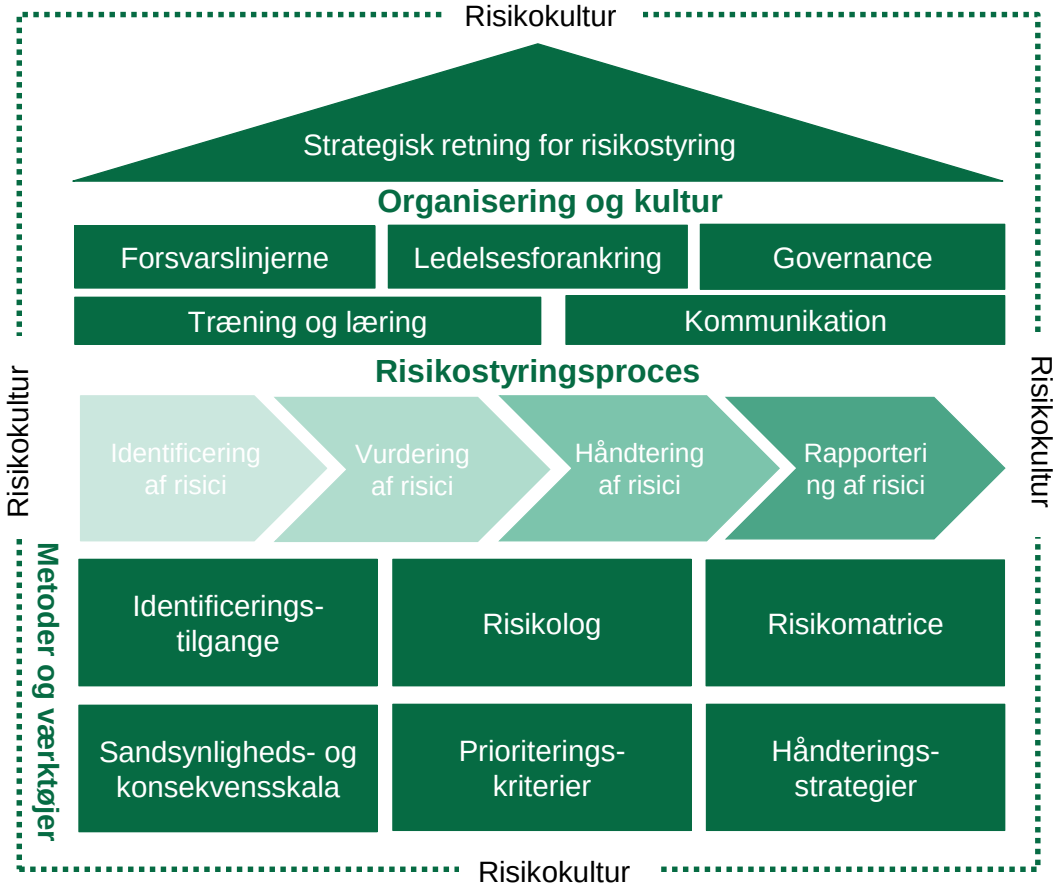
Risikostyringen kan være er baseret på et koncept, som skaber en fælles ramme på tværs af institutionen. Konceptet bør indeholde retningslinjer og politikker for, hvordan institutionen konkret arbejder med risikostyring, herunder proces, rolle- og ansvarsfordeling mv. For at skabe mest mulig værdi bør risikostyringskonceptet være forankret hos den øverste ledelse og være kendt på flest mulige niveauer i institutionen.

Den øverste ledelse sætter den strategiske retning for risikostyringen ved fx at kommunikere om ønsket adfærd og forståelse for risikostyring. Risikofunktionen og de ansvarlige kan efterfølgende udarbejde et koncept for risikostyring.

Figuren til højre illustrerer et eksempel på et risikostyringskoncept.

Risikostyringsprocessen igangsættes som en integreret del af den øvrige styring af institutionen, hvor værktøjer og metoder kan benyttes til at skabe en helhedsorienteret risikostyring.

Figur 13: Eksempel på rammeværk for risikostyring

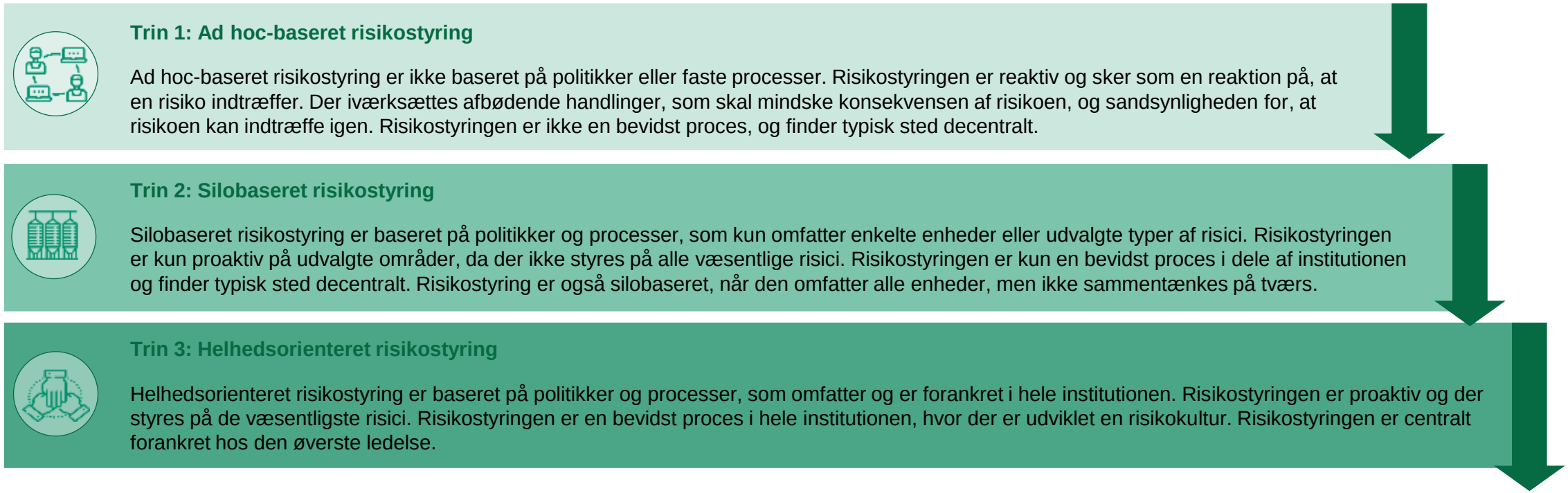


Modenhedstrappe for risikostyring

Hvordan kan en modenhedstrappe for risikostyring se ud?

Nedenfor ses eksempler på tre forskellige modenhedstrin for risikostyring. Formålet er, at forbedre risikostyringen løbende og arbejde henimod en så helhedsorienteret risikostyring som muligt. Den optimale risikostyring i en institution vil dog afhænge af ambitionsniveauet for institutionen.

Figur 14: Eksempel på rammeværk for risikostyring



ØKONOMISTYRELSEN

ØKONOMISTYRELSEN