ØKONOMISTYRELSEN

# Vejledning om risikostyring i staten

Maj 2007

## Indholdsfortegnelse

# 1. Forord

Denne vejledning er en praktisk guide til, hvordan statslige institutioner kan introducere risikostyring eller udbygge deres nuværende risikostyring. Der fokuseres på risikostyring med særligt sigte på materielle skader. Vejledningen er udarbejdet i samarbejde med Deloitte.

### Baggrund

Vejledningen skal ses på baggrund af omkostningsreformen og fokus på at sikre et mere styringsrelevant beslutningsgrundlag. I "Omkostningsprincipper for statens selvforsikring" (januar 2006) anbefaler Finansministeriet øget fokus på risikostyring, herunder en vejledning, og i beretning 5/03 om statens selvforsikringsordning anbefaler Rigsrevisionen, at staten registrerer skader og derigennem sikrer et overblik over omfanget heraf.

### Formål

Vejledningen skal hjælpe institutionerne med at gå fra reaktiv og ad hoc-præget til mere proaktiv risikostyring. Ikke alle institutioner har brug for et komplekst risikostyringsprogram. Derfor er vejledningen også en hjælp til effektiv risikostyring på forskellige ambitionsniveauer, også i mindre institutioner.

### Vejledningens opbygning og målgruppe

Hovedvægten er lagt på at hjælpe i gang med at etablere basale risikostyringsprocesser, men der lægges også op til, at institutioner, der har behov herfor, kan udvikle risikostyringen og bevæge sig op på et højere niveau.

Hovedmålgruppen er koordinerende medarbejdere med ansvar for at etablere en revideret risikostyringsproces. Men de første fem afsnit kan også være til inspiration for ledelsens planlægning og etablering af risikostyring.

Den anbefalede proces er fuldt kompatibel med anerkendte risikostyringsrammeværker[1].

[1] "Af rammeværk og anbefalinger for risikostyring kan bl.a. nævnes : "COSO - ERM Framework" - The Committee of Sponsoring Organizations of the Treadway Commission, "COCO - Guidance on Control" - The Criteria of Control Board (COCO), "ANZS43602005" - Australian New Zealand Standard, "FERMA" - Federation of European Risk Management Associations.

# 2. Introduktion til risikostyring

*Eksempler på risikodefinitioner for forskellige niveauer og fokusområder for risikostyring*

**Risikodefinition (Managing Risks in Public Organisations, Peter Young)**
En risiko repræsenterer en variation af et resultat set i forhold til det forventede resultat.

**Risikodefinition (COSO)**
Potentialet for, at en hændelse vil ske samt have en negativ indvirkning på resultatopnåelsen.

**Risikodefinition (inspireret af børsnoteret selskab)**
Hændelse eller række af hændelser, som helt eller delvist vil forhindre institutionen i at levere sine kerneydelser.

**Risikodefinition (tænkt eksempel)**
Enhver begivenhed, som vil kunne resultere i en materiel skade for institutionen.

Statslige institutioner har vidt forskellige typer kerneydelser (regulerende, sagsbehandling, drift) og dermed vidt forskellige risici. Men på trods af forskellighederne vil processen for og metoden til risikostyringen oftest være den samme. Processen i denne vejledning er således i høj grad generisk og vil kunne finde direkte anvendelse ved etablering af risikostyring i de fleste statslige institutioner.

### Hvad er risikostyring?

Risikostyring tager udgangspunkt i de usikkerheder, som en institution må forstå og effektivt styre, sideløbende med, at den leverer sine kerneydelser.

Risikostyring omhandler identifikation af potentielle afvigelser fra det planlagte og ønskede samt styring af disse afvigelser for bedst muligt at udnytte muligheder, minimere tab og forbedre beslutningstagen og resultater.

Der findes en række forskellige definitioner på risikostyring. Valget af definition afhænger af, hvor bredt et risikobegreb der anvendes – dels i forhold til, hvilke risikobegivenheder der er omfattet af definitionen, dels i forhold til, om risici ses primært som negative hændelser eller i større omfang også vurderes som risici, institutionen kan påtage sig for at realisere sine målsætninger.

### Vurdering af en risiko – væsentlighed og sårbarhed

Vurderingen af en risiko tager udgangspunkt i kombinationen af væsentligheden af og sårbarheden over for, at en uønsket hændelse indtræffer. Væsentlighed vedrører konsekvensen af en hændelse, herunder økonomisk, omdømme-, helse-, miljø- og sundhedsmæssigt, og dermed potentialet i begivenheden eller udviklingen, som institutionen er eksponeret overfor. Potentialet kan både være positivt og negativt.

Sårbarhed anvendes i denne vejledning frem for sandsynlighed af en hændelse, fordi vurderingen af sandsynlighed typisk giver problemer ved prioriteringen af operationelle risici, hvor ingen eller næsten ingen erfaring er til stede, og hvor tidshorisonten ikke er fast. Sårbarhed giver en indikation af, om institutionen umiddelbart er parat over for en risiko eller ej, når den tager de eksisterende kontroller og aktiviteter med i betragtning. Sårbarhed handler om

kontrolmiljø, eksterne forhold, tidligere erfaring med risiko, kompleksitet og responstid.[2]

**Sårbarhed eller sandsynlighed?**

Sandsynlighed et vurderingskriterium, der oftest anvendes i forbindelse med vurdering af risici. Sandsynlighed er dog kun anvendelig for risikoområder, hvor en stor historik eksisterer. Denne vejledning tager udgangspunkt i vurdering af risici ved brug af kriterierne sårbarhed og væsentlighed. Hvis institutionen har stor positiv erfaring med eller særlige præferencer for brug af vurderingskriteriet sandsynlighed, kan det være en fordel at fortsætte anvendelsen af denne, og det ændrer ikke anvendeligheden af denne vejledning i øvrigt. Institutionen bør dog genoverveje brugen af sandsynlighed som vurderingskriterium, da fordelene ved anvendelse af det mere nuancerede sårbarhedskriterium er mange.

## Etablering af effektiv risikostyring

Effektiv risikostyring handler også om at sætte risikostyringen i system og udvikle risikopolitikker, rapporteringsværktøjer m.v. på et niveau, som passer til institutionens størrelse og kompleksitet. Derfor har denne vejledning også til hensigt at muliggøre effektiv risikostyring på forskellige niveauer.

Der findes som udgangspunkt ikke en færdig pakkeløsning, som passer til alle institutioner. Etablering af en ny eller forankring af en eksisterende risikostyringsproces bør derfor være en lærende og fleksibel proces, der i sidste ende skal resultere i en skræddersyet løsning, der passer til den enkelte institutions kerneydelsers karakteristika.

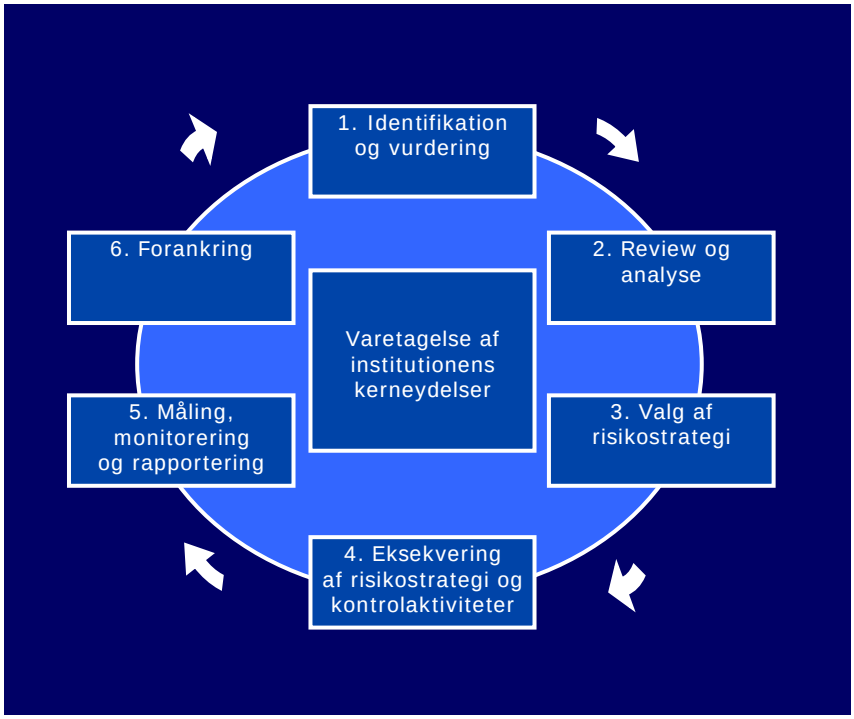
[2] I DS 484 arbejdes der imidlertid med sandsynlighed, idet indholdet af en risikoanalyse beskrives som en listning af potentielle trusler forbundet med virksomhedens anvendelse af IT, et estimat af konsekvenserne af uønskede hændelser samt en vurdering af sandsynligheden for forekomst af sådanne hændelser og en angivelse af, hvor sårbare de indgående informationsaktiver er.

# 3. Risikostyringsprocessen

Formålet med dette afsnit er at beskrive hovedelementerne i risikostyringsprocessens seks faser og give en overordnet forståelse af faserne.

Når en institution overvejer at arbejde med risikostyring, vil det være en god idé at tage udgangspunkt i et allerede etableret risikostyringsrammeværk. Ved valg af rammeværk er der i denne vejledning lagt vægt på en dynamisk model, hvor fokus er fremadrettet.

Det illustrerede rammeværk kan bruges i såvel små som store institutioner og for forskellige fokusområder.



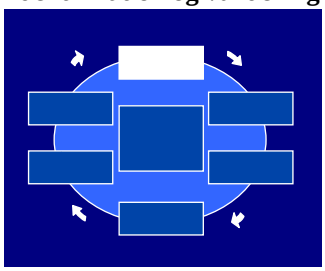

Processen kan deles op i ovenstående seks faser uafhængigt af institutionens nuværende niveau for risikostyring. Faserne indeholder risikostyringens primære elementer. I de følgende delafsnit beskrives hver af faserne.

DS 484 arbejder med 7 trin i processen: Opgavestart, trusselsliste, sandsynlighed og konsekvens, trusselsni-

veau, sikkerhedsmiljø, det samlede risikobillede og risikobegrænsning. Kronologien heri svarer til denne vejlednings 6 faser.

## 3.1. Fase 1. Identifikation og vurdering

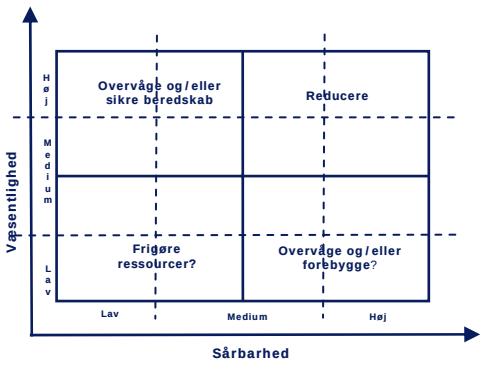
**Identifikation og vurdering**



Vil typisk kunne foregå i januar til og med februar

I fase 1 skal institutionen identificere de risici, den skal adressere. Det er vigtigt, at identifikationen foregår ved hjælp af en velstruktureret systematisk proces, og at institutionen identificerer alle relevante risici i denne fase. Det inkluderer også risici, som institutionen ikke umiddelbart selv kan påvirke. Det er vigtigt, at risici ikke frasorteres i forbindelse med identifikationen. Det er derfor bedre at medtage én risiko for meget end én for lidt.

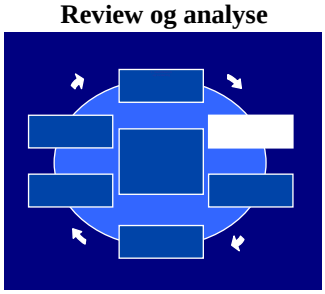
Efter identifikationen skal institutionen vurdere sine risici. Dette kan gøres ved at tegne institutionens risikobillede, som er en kombineret vurdering af de identificerede risicis væsentlighed og sårbarhed.




På baggrund af risikobilledet kan institutionen prioritere risiciene, fx ved i første omgang at opdele risiciene i 4 kategorier. Se en nærmere gennemgang heraf i delafsnit 6.2.

## 3.2. Fase 2. Review og analyse

**Review og analyse**



Vil typisk kunne foregå i marts til og med maj

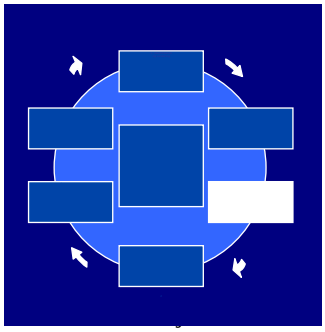
Fase 2 omhandler valg af analysemetoder, en evaluering af eventuelt anbefalede aktiviteter til imødegåelse af risikoen og identifikation af relevante alternativer.

Analysemetode vælges ud fra risikoens karakteristika, fx om den har økonomiske eller andre konsekvenser.

Institutionen skal analysere de udvalgte nøglerisici for så vidt angår årsager, væsentlighed og sårbarhed samt eksisterende og planlagte kontrolaktiviteter. Risiciene vurderes med hensyntagen til eksisterende forhold, som imødegår eller dæmper risiciene (kontrolaktiviteter, overvågning af materiel og materiale etc.), hvorefter der identificeres og dokumenteres mulige fremtidige risikotiltag. Disse indarbejdes i risikobeskrivelserne. Analysen er en mere dybtgående analyse af risici i forhold til de indledende overvejelser i identifikationen. Analysen omhandler evaluering af mulige risikostrategier.

## 3.3. Fase 3. Valg af risikostrategi

**Valg af strategi**

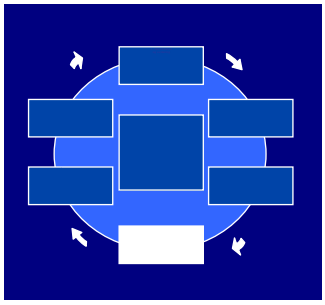


I fase 3 vil institutionen på baggrund af resultaterne af de gennemførte reviews og analyser skulle vælge en strategi for den enkelte risiko. Strategien kan bestå i at undgå, beholde, reducere, overføre eller udnytte den pågældende risiko. Endvidere placeres ansvaret for den pågældende risiko, herunder for handlingsplaner, risikomonitorering og videre rapportering hos en risikoansvarlig.

I forbindelse med valget skal institutionen tage stilling til, hvilke acceptkriterier nøglerisici skal behandles og vurderes ud fra. Acceptkriterier er kriterier, som institutionen finder acceptable eller behandlet til et acceptabelt niveau, fx når en risikos økonomiske effekt er reduceret til et acceptabelt niveau gennem et risikoreducerende tiltag.

## 3.4. Fase 4. Eksekvering af risikostrategi og kontrolaktiviteter

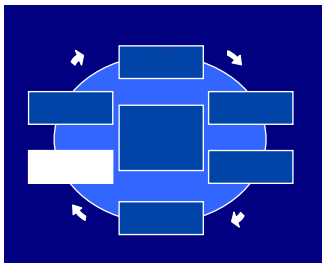
**Eksekvering af risikostrategi og kontrolaktiviteter**



I fase 4 eksekveres de udvalgte risikostrategier og kontrolaktiviteter. Det er her vigtigt, at der er foretaget en klar placering af ansvaret for eksekvering af risikostrategien for den pågældende risiko, herunder handlingsplaner, risikomonitorering og videre rapportering. Eksekveringen handler i høj grad om god opgave- og projektstyring.

## 3.5. Fase 5. Måling, monitorering og rapportering

**Måling, monitorering og rapportering**



Udføres i forhold til aftalt frekvens

I fase 5 opsamler og rapporterer institutionen relevant information, således at eksekveringen kan monitoreres. Information skal samles og kommunikeres i et format og inden for en tidsramme, der gør det muligt for medarbejdere at foretage de handlinger, som påhviler dem. Information om hændelser, årsager, implicerede samt effektivitet af risikostrategier registreres konsistent og ensartet.

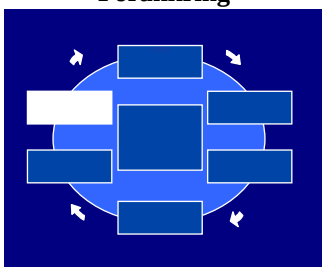
Registreringerne anvendes til løbende at gøre status for institutionens risikoportefølje og imødegående aktiviteter og kan danne grundlag for monitorering, evaluering og korrektion af risikostyringsprocessen.

Processen kræver løbende monitorering og vurdering. Derfor er det nødvendigt løbende at vurdere processens eksistens, funktion og effekt. Dette kan med fordel ske i alle processens faser. Ændrede forhold kan evt. resultere i initiering af review af risici, opdatering af risikoprofil eller ændring af en risikoejers ansvar. Derfor skal eventuelle problemer, mangler eller succeshistorier monitoreres.

Fasen vil typisk kunne systemunderstøttes. På et lavt ambitionsniveau vil der typisk blive anvendt simple systemer til begrænset registrering og rapportering om risici, fx Excel og Word. På højere ambitionsniveauer vil monitorering, måling og rapportering kunne være understøttet af mere avancerede og komplette systemer. På markedet eksisterer allerede flere systemer hertil.

## 3.6. Fase 6. Forankring

**Forankring**



Fasen vil typisk foregå i november samtidig med planlægning af næste års aktiviteter.

Denne fase omhandler opsamling og formidling af informationer til relevante organisatoriske enheder samt integration og anvendelse af den opnåede viden. Fx vil nøglerisici skulle rapporteres op på topledderniveauet, mens mindre risici vil kunne blive og behandles i de enkelte afdelinger. Institutionen skal således forankre og integrere risikostyringen som et element i institutionens øvrige styrings- og rapporteringsprocesser, herunder i mål- og resultatfastsættelsen i institutionen og i opfølgningen herpå.

# 4. Risikostyring på det relevante niveau

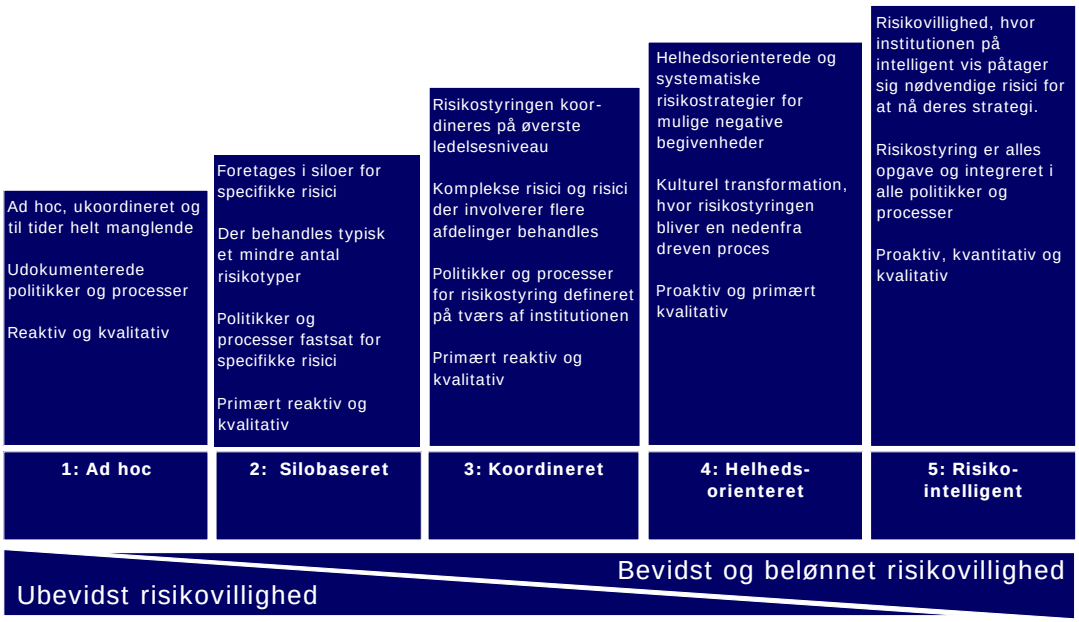
Dette afsnit giver mulighed for at evaluere institutionens nuværende niveau for risikostyring samt for ledelsen at fastsætte et ønsket fremtidigt niveau herfor. Samtidig giver afsnittet en overordnet forståelse af, på hvilke niveauer risikostyring er mulig, samt hvilke karakteristika de enkelte niveauer har.

## 4.1. Ambitionsniveauer for risikostyring

En institutions evne til at udøve effektiv risikostyring kan være på forskellige niveauer. Figur 4.1. kategoriserer en institutions risikokompetencer på fem ambitionsniveauer:

- Ad hoc
- Silobaseret
- Koordineret
- Helhedsorienteret
- Risikointelligent.

**FIGUR 4.1. AMBITIONSNIVEAUER FOR RISIKOSTYRING**




De fem ambitionsniveauer afspejler en stigende evne til risikostyring. Ambitionsniveauet fastsættes af institutionens ledelse. De enkelte niveauer er kort beskrevet her med henvisninger til Dansk Standards DS 484.

### Niveau 1 – Ad hoc

Institutionen udfører risikostyringsaktiviteter ad hoc og typisk reaktivt. En konsistent risikostyringsproces findes ikke, hvilket medfører kaotiske og modstridende aktiviteter. Risikohåndtering afhænger primært af individuelle initiativer. Da processer, aktiviteter m.v. ikke er dokumenterede, foregår eventuel overdragelse af viden og erfaringer verbalt. På informationssikkerhedsområdet skal institutionerne være opmærksomme på, at risikostyring på dette niveau ikke opfylder DS 484.

### Niveau 2 – Silobaseret

Siloer etableres ved at uddelegere ansvaret for risikostyring af specifikke risici til specialister i organisationen. Adskilte roller etableres for et mindre antal risikotyper. De forskellige siloer har typisk etableret deres egen fortolkning og tilgang til forståelse af risici oftest med vidt forskellig risikovillighed og divergerende kompetenceniveauer. Risici aggregeres ikke på tværs af organisationen, og risikostyringsindsatser er oftest ikke allokeret til de mest væsentlige risici og til de områder, hvor institutionen er mest sårbar. På informationssikkerhedsområdet skal institutionerne være opmærksomme på, at på dette niveau er DS 484 nok udmeldt, således at siloerne forholder sig dertil, men det sker på basis af egne fortolkninger.

### Niveau 3 – Koordineret

Topledelsen har defineret og udstukket retningslinjer for risikostyringsaktiviteterne. Alle politikker, procedurer og risikobeføjelser er veldefinerede og kommunikeret af ledelsen. Risikostyring er en defineret funktion i institutionen. De værktøjer, der arbejdes med, er primært kvalitative, dog vil enkelte silobaserede risici kunne håndteres med avancerede værktøjer. Selvom en risikostyringsstruktur eksisterer i det store hele, håndteres risici, efterhånden som de forekommer, og ikke proaktivt. På informationssikkerhedsområdet er DS 484 implementeret på dette niveau.

### Niveau 4 – Helhedsorienteret

Den systematiske og helhedsorienterede risikostyring er kendetegnet ved klare risikostrategier for mulige udviklinger og begivenheder, institutionen er eksponeret for. Medarbejderne forstår eskaleringsprocedurerne. Institutionen oplever en kulturel forandring, da risikostyringen er blevet en mere nedefra dreven proces. Dette gør, at med-

arbejderne forstår, hvordan deres funktion bidrager til realisering af strategien, og får dem til at agere proaktivt i forhold til håndtering af risici. På informationssikkerhedsområdet er DS 484 forankret på dette niveau.

#### Niveau 5 – Risikointelligent

Med en risikointelligent risikostyring er der skabt beredygtighed på alle niveauer. Risikostyringsprocessen er en integreret del af institutionens beslutningsprocesser og er en del af alle medarbejderes job. Institutionen er bevidst om sin risikovillighed, og der gennemføres kvantitative og kvalitative risikoanalyser, der medvirker til, at institutionen på intelligent vis påtager sig de risici, der medfører, at institutionen kan realisere sine målsætninger. På informationssikkerhedsområdet er DS 484 forankret på dette niveau.

#### Særligt om IT-sikkerhed (DS 484)

Et eksempel, jf. ovenfor, på silobaseret risikostyring er en isoleret implementering af it-sikkerhedsstyring.

Med regeringens beslutning om, at alle ministerier og underliggende institutioner skal implementere de basale krav i den danske standard for informationssikkerhed, er en it-sikkerhed et område, hvor alle statslige institutioner skal gennemføre risikostyring.

Standarden er baseret på Dansk Standards DS 484, som er udarbejdet på baggrund af best practice for styring af it-sikkerhed. IT- og Telestyrelsen har udarbejdet en pjece og et hjælpeprogram, der beskriver en 12 trins model målrettet implementering af it-sikkerhedsstyring, herunder udarbejdelse af it-sikkerhedspolitik, risikovurdering, beredskab og kontrol.

Mere info herom findes på www.oio.dk/itsikkerhed/sisis

## *4.2. Vurdering af niveau for risikostyring*

Institutionen kan ved hjælp af en selvevaluering vurdere sit nuværende risikostyringsniveau.

Dette kan foregå på flere niveauer. I denne vejledning tages udgangspunkt i et overordnet niveau med en enkel og umiddelbar vurdering ud fra nogle overordnede og subjek-

tive kriterier fordelt på 8 parametre. De 2 første parametre vedrører institutionens generelle miljø for risikostyring samt fastsættelse af målsætninger for risikostyring. De sidste 6 parametre vedrører hver af de 6 faser i risikostyringsprocessen.

Når institutionens risikostyringsniveau skal evalueres, kan institutionens kompetencer inden for hvert af nedenstående parametre vurderes på en skala fra 1-5. En efterfølgende gennemsnitsbetragtning kan give et billede af risikokompetencen i institutionen. Fastsættelse af ønskeligt fremtidigt niveau kan foretages ud fra samme princip.

### Miljø

Miljø for risikostyring omfatter tonen i institutionen, der påvirker risikobevidstheden hos medarbejderne, og som danner basis for alle andre komponenter i risikostyring. Miljø for risikostyring giver disciplin og struktur.

### Målsætning og beslutningstagning

Målsætninger bliver formuleret på det strategiske niveau og danner baggrund for operationelle, rapporteringsmæssige og compliancemål.

### Identifikation og vurdering

Ledelsen identificerer potentielle hændelser, som, hvis de indtræffer, vil kunne påvirke institutionen. Ledelsen vurderer, om disse hændelser repræsenterer en positiv mulighed eller vil kunne have en negativ indvirkning på institutionens mulighed for succesfuldt at implementere den valgte strategi og opnå de strategiske mål.

### Review og analyse

Risikoanalyse og review tillader en institution at overveje, i hvilket omfang en potentiel hændelse vil påvirke muligheden for at nå de opstillede mål.

### Valg af risikostrategi

Risikostrategi er ledelsens fastlæggelse af, hvordan der skal reageres baseret på risikovurderinger af relevante risici.

### Eksekvering af risikostrategi og kontrolaktiviteter

Eksekvering af risikostrategi og kontrolaktiviteter indebærer fastlæggelse af politikker og procedurer, som sikrer, at ledelsens risikostrategi bliver fulgt.

### Måling, monitorering og rapportering

Relevant information bliver identificeret, opsamlet og kommunikeret i et format og inden for en tidsramme, der gør det muligt for medarbejdere at leve op til deres ansvar og udføre de nødvendige handlinger.

### Forankring

Risikostyringsprocessen, værktøjer og metoder bliver kommunikeret ud i institutionen. Medarbejderne informeres om og uddannes løbende i risikostyring. Ledelsen støtter aktivt risikostyringen og sikrer, at de nødvendige ressourcer er til stede. Der er defineret og etableret en risikoorganisation i organisationen.

Hvis en institution vurderer, at den ikke er på det ønskede ambitionsniveau, vil den nuværende organisatoriske forankring typisk ikke være den mest hensigtsmæssige.

## *4.3. Valg af fremtidigt ambitionsniveau*

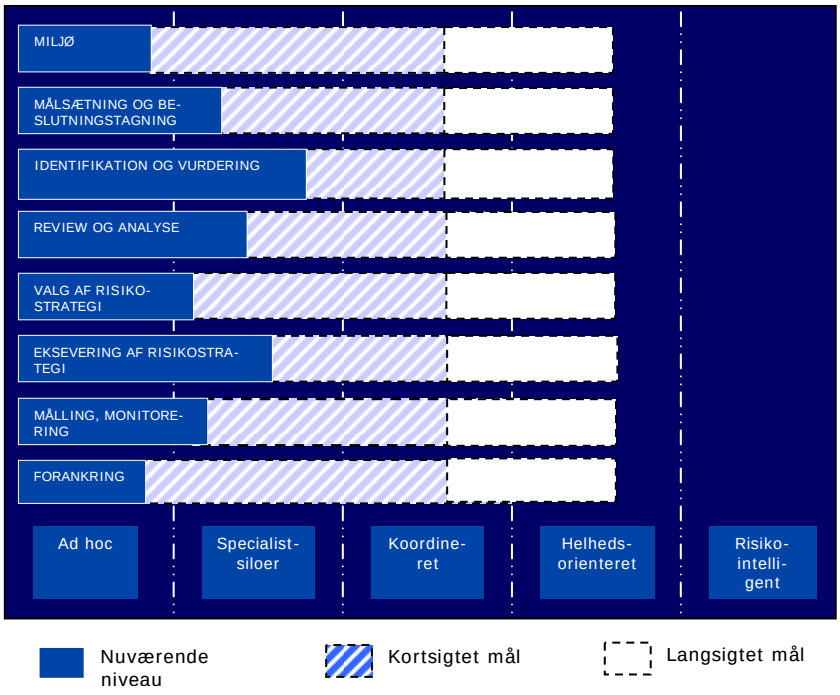
Efter vurderingen af sit nuværende risikostyringsniveau kan institutionen overveje det ønskede fremtidige niveau. Forskellen mellem nuværende og ønsket risikostyringsniveau kan herefter bruges til at målrette indsatsen mod de parametre, hvor der er et lavere – eller i enkelte tilfælde måske højere - risikostyringsniveau end ønsket.

Dette er illustreret i figur 4.2, hvor der med blåt er angivet det nuværende risikostyringsniveau for en institution for hvert af de 8 parametre. Med skraveret er angivet en realistisk ambition for ønsket niveau på kort sigt, og med hvidt det ønskede niveau på langt sigt.

Institutionen fastsætter først en realistisk målsætning for ønsket risikostyringsniveau på kort sigt. Når dette mål er nået, kan den sætte sig konkrete mål for at nå det ønskede langsigtede ambitionsniveau. Målsætningen vil bl.a. afhænge af institutionens størrelse og kompleksitet. Gennem en selvevaluering af sit niveau for risikostyring vil institutionen kunne klarlægge, hvor den kan forbedre sin ri-

sikostyring, og hvor den allerede er på det fornødne niveau.

**FIGUR 4.2. NUVÆRENDE NIVEAU OG FREMTIDIGT AMBITIONSNIVEAU FOR RISIKOSTYRING**




Endvidere vil en realistisk målsætning på kort sigt være afhængig af institutionens nuværende risikostyringsniveau. Det er vigtigt, at institutionen sætter realistiske kortsigtede mål. Et af formålene med vurderingen er at identificere, hvor der først skal fokuseres. Hvis en institution er relativt langt med metode til fx identifikation og vurdering af risici, skal der indledningsvist fokuseres på at oparbejde kompetencer på områder, hvor institutionen har relativt mindre erfaring. For at opnå det bedst mulige grundlag er det derfor mest hensigtsmæssigt at søge at forbedre kompetenceniveauet på de områder, hvor gabet op til det kortsigtede ønskelige niveau er størst.

Efter identifikation af ønskeligt niveau for risikostyring, vil det være muligt for institutionen at udarbejde følgende:

- Generelle kommentarer/beskrivelse af institutionens niveau for risikostyring
- Plan for, hvorledes institutionen vil udvikle sin risikostyring
- Specifikke anbefalinger til forbedringer inden for hvert område

- Forslag til, hvorledes de nødvendige ressourcer mobiliseres

Modellen med ambitionsniveauer for risikostyring skal således understøtte institutionens arbejde mod en bedre og mere helhedsorienteret risikostyring.

# 5. Start og planlægning af risikostyring

Dette afsnit beskriver forhold, som institutionen skal overveje, inden den sætter risikostyringsprocessen i gang.

Afsnittet er opbygget med udgangspunkt i en gennemgang af følgende forhold, som vurderes at være nødvendige at have overvejet og i videst muligt omfang have afklaret for at sikre en hensigtsmæssig efterfølgende implementering af risikostyringsprocessen.

- Ledelsens rolle
- Infrastruktur for risikostyring
- Integration med institutionens øvrige processer
- Etablering af risikokultur
- Centrum af institutionens risikounivers
- Valg af organisatorisk opbygning af risikostyringen
- Initiering af projektet

## 5.1. Ledelsens rolle

En institutions risikostyring er altid ledelsens ansvar. Det er ledelsen, der overordnet fastlægger institutionens ønskede ambitionsniveau for risikostyring og udmønter dette i en politik.

Etablering af risikostyring kan være omfattende og kræve høj organisatorisk forankring og deltagelse, hvis ambitionsniveauet er højt. En institution med lavere ambitionsniveau kan derimod nøjes med at implementere delelementer af risikostyringsprocessen i enkelte afdelinger, hvilket vil reducere omfanget og effekten af risikostyringen.

Hvis det er besluttet, at institutionen skal have risikostyring med et relativt højt ambitionsniveau, er det vigtigt, at ledelsen er involveret med tid, engagement og støtte. Hvis dette ikke er muligt, bør ambitionsniveauet sænkes.

Ledelsens rolle omhandler primært igangsætning af risikostyring, uddelegering af ansvar samt løbende beslutningstagning, når risikostyringen implementeres og idriftsættes.

Det er også ledelsen, der har ansvaret for, at medarbejderne er kvalificerede til at løse den stillede opgave, og at de nødvendige ressourcer er til stede. Det er særligt vigtigt, at ledelsen udvælger medarbejdere med gennemslagskraft til implementeringen af risikostyringen. I forlængelsen heraf skal ledelsen også sikre den nødvendige uddannelse i risikostyring af disse medarbejdere.

## 5.2. Set up for risikostyring

Set up'et for risikostyring er de systemer, som udgør forbindelsen mellem institutionens risikostyringsdele, såsom:

- Organisering
- Politikker og procedurer
- Strukturer for projekter og processer
- Teknologier og værktøjer.

Inden for samtlige elementer skal institutionen overveje, om den har brugbare erfaringer, den kan anvende i forbindelse med implementeringen af risikostyringen.

### Organisering

Hvilke muligheder har institutionen for at etablere en risikoorganisation set i forhold til den eksisterende organisation? Hvilke eksisterende jobfunktioner/roller vil kunne varetage risikostyringens forskellige elementer, og hvilke roller er nødvendige for at sikre en effektiv risikostyring?

### Politikker og procedurer

Institutionen skal aktivt tage stilling til, om en eventuel politik for risikostyring er i overensstemmelse med eller har indflydelse på eksisterende politikker og procedurer.

### Strukturer for projekter og processer

Har institutionen brugbare erfaringer om strukturering af projekter og processer, skal den overveje at anvende dem i forbindelse med etableringen af en risikostyringsproces. Foreligger der sammenlignelige projekter eller processer, som er anerkendte og anvendte i hele organisationen, kan disse med fordel bruges som inspiration til struktureringen og implementeringen af risikostyringsprocessen.

### Teknologier og værktøjer

Som praktisk forberedelse kan institutionen gennemgå eksisterende og/eller ønskværdige værktøjer og teknikker, som kan eller skal være en del af risikostyringen. Er der i

forvejen risikostyringsaktiviteter i form af fx monitorering, registrering og rapportering, skal institutionen overveje, om disse fortsat skal være en del af risikostyringen.

## 5.3. Integrationen med institutionens øvrige processer

Risikostyring kan helt eller delvist hænge sammen med institutionens øvrige styrings-, optimerings- og/eller planlægningsaktiviteter. Fx kan risikostyringen integreres som eksekveringsværktøj i strategiprocessen, i mål- og resultatstyringen, i budget- og regnskabsopfølgning m.m. Typisk vil en del af de personer, der skal arbejde med risikostyring, allerede beskæftige sig med de nævnte områder, hvorfor et samspil allerede eksisterer.

## 5.4. Etablering af risikokultur

Den risikokultur, ledelsen ønsker at fremme i institutionen, skal den implementere ved hjælp af en række virkemidler såsom forandringsledelse, projektledelse, uddannelse, teknologi, best practices, bæredygtighed, kommunikation m.m. Institutionen kan derfor med fordel bygge videre på de områder, hvor institutionen har stærke kompetencer og erfaringer, der kan understøtte etableringen af en risikokultur.

Etablering af en risikokultur kan være et ømtåleligt emne, hvor mange følelser og meninger vil blive luftet. Da formålet med risikostyring er at fokusere på de væsentligste risici og de områder, hvor institutionen er mest sårbar, rækker risikostyringen ind i de mest vitale dele af institutionen. Viden og information om disse dele af institutionen vil altså blive kanaliseret igennem risikostyringsorganisationen. Den organisatoriske forankring af risikostyring kan derfor, hvis den ikke gribes rigtigt an, hurtigt udvikle sig til en diskussion om, hvem der skal vide hvad, og hvem det egentlig er, der styrer institutionens centrale risici. Disse diskussioner kan i værste fald udvikle sig til en hæmsko for arbejdet med at øge institutionens niveau for risikostyring.

Inden de organisatoriske drøftelser om risikostyring påbegyndes, skal ledelsen derfor overveje, hvilke barrierer institutionen kan møde, og hvordan ansvar og beføjelser skal fordeles. Det er vigtigt, at ledelsen forstår og forholder sig til, om institutionens kultur er forenelig med den risikoorganisation, ledelsen ønsker at introducere.

## 5.5. Centrum af institutionens risikounivers

Et centralt punkt for den enkelte institutions arbejde med risikostyring er at tage stilling til, hvilke risici institutionen vil fokusere på. Dette er et ofte undervurderet spørgsmål, der skal adresseres, når et risikostyringsprojekt igangsættes. Institutionen skal tage stilling til, hvad risici skal sættes i forhold til.

Et naturligt første skridt for institutionen vil være at fokusere på risici forbundet med institutionens materielle aktiver eller alternativt på en delmængde af institutionens kerneydelser, hvor en fokuseret risikostyringsindsats vurderes at have den største effekt (ambitionsniveau 2).

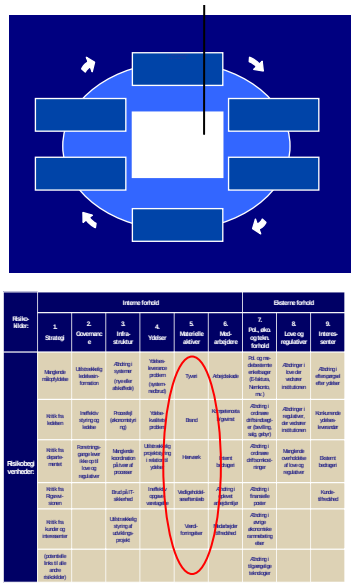
Et fokus på eksempelvis materielle skader vil være et godt udgangspunkt, idet der er tale om meget konkrete risici på et snævert område. Nogle gange vil skader på aktiver dog også have effekt på institutionens mulighed for at levere sine ydelser. Det er vigtigt, at disse effekter indgår i risikoanalysen forbundet med skader på de materielle aktiver. Fokusering på etablering af risikostyring af disse aktiver vil naturligt kunne foretages i forbindelse med en samtidig forbedring af institutionens skadesregistrering.

Institutioner, som har et højere ambitionsniveau (niveau 3), kan brede risikostyringen ud til at omfatte institutionens kerneydelser. Dette indebærer et forholdsvist bredt risikounivers med flere forskellige risikokilder. Til at hjælpe institutionen med at udarbejde dets risikounivers kan der derfor med fordel tages udgangspunkt i en risikomodel. Risikomodellen specificerer de hovedkategorier, hvor risici typisk opstår eller eksisterer. Som hjælp til udarbejdelse af en risikomodel er der i bilag 1.4 en generisk risikomodel til identificering af risici forbundet med institutionens kerneydelser. Risikomodellen kan endvidere med fordel anvendes i forbindelse med identifikationen og klassificeringen af institutionens risici (se også afsnit 6).

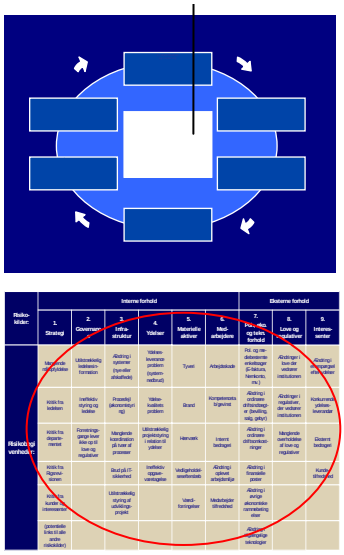
På baggrund af disse overvejelser skal institutionen herefter vælge en specifik risikodefinition, der svarer til institutionens ønskede niveau og fokusområde for risikostyring, jf. eksemplerne på risikostyringsdefinitioner i afsnit 2.

Endvidere skal der foretages en konkretisering af anvendelsen af risikovurderingskriterier for en risikos væsentlighed og sårbarhed, idet risikovurderingskriterierne er af

Snævert fokus, eksempelvis minimering af skadesomkostninger



Bredt fokus, eksempelvis varetagelse af institutionens kerneydelser



stor betydning for, hvilke risici der arbejdes videre med og rapporteres på.

Mulige risikovurderingskriterier for væsentlighed kunne være:

- Økonomiske konsekvenser
- Skader på helse, miljø og mennesker
- Omdømme, mv.

Mulige risikovurderingskriterier for sårbarhed kunne være:

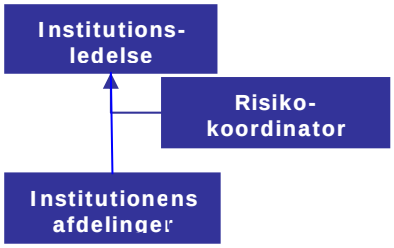
- Kontroleffektivitet
- Eksterne forhold
- Tidligere risikoerfaring
- Kompleksitet

Ud over disse eksempler på generelle vurderingskriterier vil det ofte være relevant for institutionen at fastsætte sine egne specifikke kriterier. Inspiration hertil kan institutionen ofte finde i sine eksisterende krav til overholdelse af eksterne samt interne regler, strategier, regulativer, lovgivning, mål- og resultatkrav.

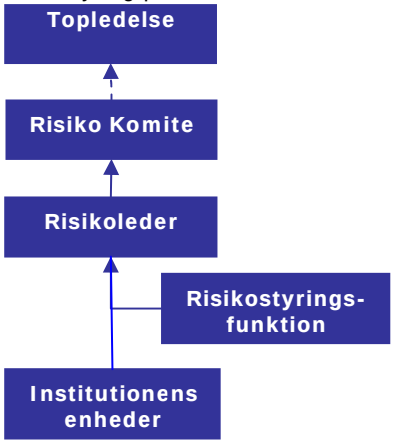
Netop de fastsatte risikovurderingskriterier samt risikodefinition medfører en konsistent risikostyring, da risikostyringen dermed foregår med et fælles sprog.

## 5.6. Organisatorisk opbygning

Eksempel på organisatorisk opbygning af risikostyring på niveau 3.




Eksempel på organisatorisk opbygning af risikostyring på niveau 4.




I de fleste statslige institutioner foregår arbejdet med risikostyring silobaseret (niveau 2) med uafhængige risikoejere placeret i institutionernes forskellige afdelinger. Typisk er det daglige ansvar for risikostyring delegeret til en eller flere nøglemedarbejdere.

Institutioner, som ønsker at arbejde mere tværgående med risikostyring (niveau 3), vil derfor skulle ændre på de nuværende organisatoriske rammer. Integrationen af en risikoorganisation i institutionen skal passe til den øvrige del af organisationen. Det betyder, at nye aktører skal tildeles nogenlunde samme beføjelser og forpligtelser, som ligestillede i den øvrige del af organisationen. Der findes adskillige organisationsmodeller for risikostyring, som relaterer sig til forskellige ambitionsniveauer. Nogle har en særlig risikoleder, som sidestilles med fx økonomidirektøren og den tekniske direktør, og udpegede risikoansvarlige for de forskellige afdelinger. Oftest vil risikolederrollen dog blive varetaget af et eksisterende direktionsmedlem. An-

dre modeller fordrer, at de enkelte afdelingsledere får ansvaret for risikostyringen i deres afdeling og for rapportering videre op i organisationen.

Valg af organisatorisk struktur for arbejdet afhænger af den eksisterende struktur samt institutionens risikostyringsambitionsniveau. I det følgende gennemgås nogle af de vigtigste og mest anvendte roller og organisatoriske elementer.

Det vigtigste budskab i denne forbindelse er ikke, hvor mange led og roller der identificeres i en risikoorganisation, men at institutionen aktivt tager stilling til, hvordan ansvar og beføjelser skal delegeres, og samtidigt vælger at prioritere arbejdet med risikostyring i ledelsen.

**Risikokomité:** Formålet med at etablere en risikokomité er oftest at sikre en overordnet monitorering og evaluering af risikostyringsprocessen. Komitéen vil typisk på baggrund af etableret dokumentation løbende evaluere risikostyringsprocessens enkelte elementer. Det vil således ofte være risikokomitéen, der udarbejder anbefalinger til ledelsen om eventuelle ændringer/forbedringer fx i form af uddannelse af personale i risikostyring eller implementering af udvalgte og identificerede risikostrategier eller kontrolaktiviteter. En risikokomité vil ofte bestå af få medlemmer af organisationen. Nogle risikokomitéer indeholder samtlige afdelingsledere samt risk manageren, andre kun enkelte afdelingsledere, mens andre også har tilknyttet en ekstern ekspert i forbindelse med risikostyringsprocessens første år. Risikokomitéen ledes af risikolederen.

**Risikoleder:** Risikolederens, ofte kaldet Chief Risk Officer (CRO), rolle er at sikre, at institutionen opfylder den fastsatte strategi for risikostyring. Risikolederen er typisk medlem af topledelsen eller direktionen og er ansvarlig for, at den øvrige ledelse og direktionen løbende er informeret om institutionens nøglerisici samt status for risikostyringsprocessen. Risikolederens overordnede ansvar er:

- At etablere en risikobevist organisationskultur
- At sikre, at den praktiske risikostyring understøtter realiseringen af institutionens kerneydelser
- At sikre, at institutionens medarbejdere har den fornødne viden om og ekspertise inden for risikostyring
- At kommunikere til interessenter og fungere som rådgiver for øvrige medlemmer af topledelsen samt direktionen

**Risk manager:** Risk managerens rolle er at holde den samlede risikostyringsproces og -indsats i gang og sikre, at institutionen bevæger sig mod det ønskede niveau for risikostyring. Samtidig er risk manageren den, der modtager informationer om risici fra den samlede organisation og formidler dem videre til en eventuel risikokomité eller direkte til ledelsen.

**Risikoejer:** Identificeret og udpeget ejer af en eller flere af institutionens risici. Risikoejeren har ansvar for løbende at monitorere, evaluere, rapportere samt eksekvere planlagte risikostrategier og kontrolaktiviteter.

## *5.7. Initiering af projektet – start med et pilotprojekt*

Den institution, som ønsker et højere niveau for risikostyring, skal overveje organiseringen af dette arbejde. Det vil typisk være en fordel at organisere det som et projekt med en styregruppe forankret i topledelsen og en projektgruppe med veldefinerede beslutnings- og ansvarsområder.

Det vil være afgørende, at der skaffes de nødvendige ressourcer, at de medarbejdere, der skal indgå i arbejdet, fritages for andre opgaver, og at der i øvrigt er sikret den fornødne ledelsesmæssige støtte. Samtidig skal institutionen ved påbegyndelsen overveje, hvordan den skal rapportere og monitorere risikostyringen, og om det er muligt/nødvendigt at anvende it-understøttelse. Desuden vil målbare succeskriterier for risikostyring skulle defineres, således at institutionen kan evaluere løbende.

I de fleste tilfælde kan det anbefales, at institutionen starter med et pilotprojekt.

# 6. Etablering af risikostyring med forskellige ambitionsniveauer

Dette afsnit indeholder en praktisk vejledning i etablering af risikostyring med forskellige ambitionsniveauer. Der henvises til hjælpeværktøjer, som fremgår og er nærmere beskrevet i bilag.

Den praktiske vejledning tager udgangspunkt i de forskellige ambitionsniveauer for risikostyring og vil dermed være tilpasset institutionens udgangspunkt og ambitioner. Hovedfokus vil være på at etablere risikostyring på henholdsvis ambitionsniveau 2 samt 3. Vejledningen lægger dog også op til, at institutionerne over tid kan udvikle risikostyringen og dermed bevæge sig op på et højere risikostyringsniveau. Konkret vejledning og anvisninger til etablering af et niveau for risikostyring over niveau 3 ligger dog ud over denne vejlednings sigte.

Endelig er der til inspiration angivet praktiske eksempler på risikostyring i statslige institutioner, der allerede har arbejdet med risikostyring på et niveau for risikostyring mellem niveau 2 og 3.

## 6.1. Etablering af silobaseret risikostyring (niveau 2)

Etablering af silobaseret risikostyring vil være relevant for institutioner, som ikke har eller kun har meget begrænsede og tilfældige aktiviteter inden for risikostyring. Det vil være institutioner, hvor uønskede hændelser først identificeres, vurderes og håndteres, når de indtræffer, og risikohåndteringen derfor hovedsageligt udføres reaktivt som krisehåndtering.

Nedenfor gennemgås et eksempel på, hvorledes risikostyring på ambitionsniveau 2 kan foregå. Institutionen bør udvælge de elementer, den finder anvendelige i forbindelse med implementeringen af risikostyring i organisationen.

Med etablering af silobaseret risikostyring (niveau 2 for risikostyring) foretages identifikation og rapportering, som

muliggør analyse og kvantificering af institutionens risici inden for et særligt område (silo).

Rapporteringen vil muliggøre identifikation af årsager samt omstændigheder ved risikobegivenheden, hvorved fastsættelsen og/eller modificering af risikostrategier muliggøres. I det følgende gives konkrete anvisninger og hjælpeværktøjer for hver fase i risikostyringen med henblik på etablering af en silobaseret risikostyring. Etableringen af risikostyring er således beskrevet med udgangspunkt i de seks faser gennemgået i afsnit 3.

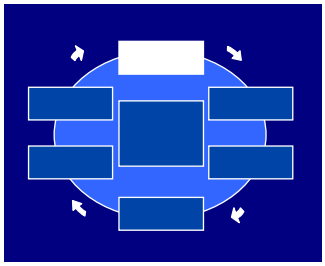
1. Identifikation og vurdering
2. Review og analyse
3. Valg af risikostrategi
4. Eksekvering af risikostrategi og kontrolaktiviteter
5. Måling, monitorering og rapportering
6. Forankring

Det første skridt mod etableringen af silobaseret risikostyring er, at institutionen skal vælge, hvilke områder (siloer) den vil fokusere risikostyringen indenfor.

I de fleste tilfælde kan det anbefales, at institutionen starter med et pilotprojekt på et overskueligt delområde af organisationen. Der bør startes med et veldefineret og afgrænset projekt med et entydigt formål. Det vil typisk vedrøre risici forbundet med en af institutionens væsentligste kerneydelser.

Et pilotprojekt af seks til ti ugers varighed vil typisk kunne omfatte rammeværkets tre første hovedfaser. Inden de sidste tre faser i rammeværket gennemføres, er det ikke unormalt, at en institution har gennemført et par iterationer for de tre første faser. Dette skal ses som et naturligt resultat af den oparbejdede viden og erfaring, organisationen får gennem pilotprojektet.

Implementeringen af risikostyringen kan herefter inddrage de resterende faser i risikostyringsprocessen. Risikostyringen kan dermed løbende forbedres, og implementeringen kan ses som en struktureret lærende proces med plads til løbende konceptforbedringer. En risikostyringsproces vil altid involvere samtlige faser i rammeværket uafhængigt af ambitionsniveau.



## Fase 1. Risikoidentifikation og vurdering

### Risikoidentifikation

Som *forberedelse* til risikoidentifikation udvælgesforetages en udvælgelse af relevante nøglepersoner for udvalgte områder. Det kan for eksempel være afdelingsledere eller andre, der er ansvarlige for nøgleaktiviteter og processer på det pågældende område. De udvalgte personer samles til en workshop, interviewes eller får tilsendt spørgeskemaer med det formål at identificere risici (se interviewskabelon i bilag 1.3).

Selve risikoidentifikationen kan *udføres* med udgangspunkt i den valgte risikomodel (se bilag 1.4) og de valgte risikovurderingskriterier.

### Risikovurdering

For at foretage en risikovurdering og prioritering af de identificerede risici inden for området kan det være hensigtsmæssigt at samle nøglepersoner og risikoejere til en ny workshop eller et kort møde med det formål at få udpeget de nøglerisici inden for det pågældende område, som det er vigtigst at styre og analysere.

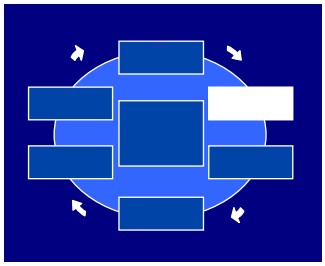
På workshoppen vurderes og prioriteres de identificerede risici ud fra væsentlighed og institutionens sårbarhed over for dem. Vurderingen udmøntes i et risikobillede med væsentlighed ud ad den vertikale akse og sårbarhed ud ad den horisontale akse. En mere detaljeret beskrivelse af fremgangsmåden findes i delafsnit 6.3.

### Risikoprioritering

Når alle risici er vurderet, prioriteres de for at udvælge en række nøglerisici til videre behandling. På ambitionsniveau 2 vil der typisk udvælges 1 til 3 risici på enkelte af institutionens områder til videre review og analyse.

Efter valg af nøglerisici til videre behandling udvælges risikoejere, der skal analysere risikoen nærmere og opstille en eventuel risikostrategi for adressering af den pågældende risiko.

Tidsforbruget for risikoidentifikation og -vurdering på dette niveau vil afhænge af områdets størrelse, aktiviteter, kompleksitet samt antallet af involverede personer. Hvis der er tale om et større område med høj kompleksitet kan flere workshopper være nødvendige. På mindre områder med mindre kompleksitet vil det typisk kunne foretages på en enkelt halvdags workshop. En kortlægning og review eller vurdering af områdets risici vil typisk tage mellem et par timer og en halv dag.



### Fase 2. Review og analyse

Review og analyse omhandler institutionens muligheder for at behandle de identificerede nøglerisici. Fasen indeholder en kortlægning af eksisterende risikostyringsaktiviteter samt identifikation af fremtidige potentielle aktiviteter, således at uacceptable risici nedbringes til et acceptabelt niveau eller elimineres.

Den konkrete analysemetode vælges dels ud fra risikoens karakteristika, f.eks. risikotype, og dels ud fra i hvilket omfang institutionen kan kvantificere den pågældende risiko. Endvidere er valg af analysemetode afhængigt af formålet med analysen, for eksempel om det primære formål er en dybtgående analyse af risicienes årsager, eller en kortlægning af fordele og ulemper ved forskellige handlinger til imødegåelse af risikoen. Se eksempler på hyppigt anvendt analysemetoder i delafsnit 6.2 om etablering af en koordineret risikostyring.

De valgte analyser kan typisk gennemføres i et samarbejde mellem den ansvarlige for etableringen af risikostyringen og risikoejeren inden for det pågældende område. En væsentlig del af pilotprojektets tid må forventes at ligge i denne fase, da det er her, risikostyringen for alvor starter.

**Risikostyring af forsvarets olie, lager og distributionssystem i forhold til forurening af jord, vand og grundvand**

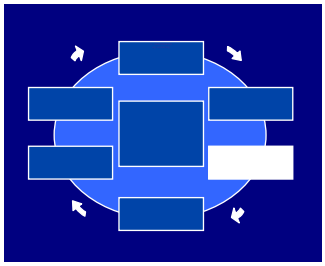
**Forsvarets Bygnings- og Etablissementstjeneste har i løbet af 2006 foretaget en miljømæssig risikoanalyse af en række af forsvarets ledningsanlæg, pumpestationer, tankområder samt andre væsentlige olieinstallationer. Formålet med risikoanalysen har blandt andet været at udpege mulige uheldssituationer, som kan give anledning til miljøpåvirkning fra de enkelte anlæg, samt skabe grundlaget for en prioritering af forebyggende tiltag med henblik på at reducere risikoen for uheld, som kan påvirke miljøet.**

***Risikoidentifikation og vurdering***
**Projektet blev igangsat med en række workshopper med drifts-personale og ansvarlige for anlæggene med henblik på at registrere og beskrive anlægsudformning og -tilstand samt drifts- og sikkerhedsprocedurer på de enkelte anlæg.**

**På en række nye workshopper blev der i forlængelse heraf foretaget en identifikation af risikoelementerne for hver anlægsdel. Der blev taget udgangspunkt i analysemetoden Hazard and Operability Study (HAZOP), som anvendes til systematisk risikoanalyse til vurdering af fare og risikoelementer ved processer og anlæg. Analysen omfattede alle driftsrelaterede risici, herunder risici for utætheder og beskadigelser af rør, risici for fejlfunktion af ventiler, risici for lækage på tankanlæg under fyldning og tømning, risici forbundet med reparation og vedligehold samt risici forbundet med brand.**

***Review og analyse***
**HAZOP-analysen vil blive dokumenteret, og der vil blive foretaget vurderinger af konsekvenserne for hver af de identificerede risici. Der vil i den forbindelse blive udarbejdet et risikobillede, hvor risiciene bliver vurderet ud fra vurderingskriterierne konsekvens og sandsynlighed.**

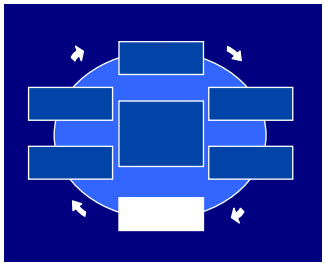
**På baggrund af HAZOP-analysen vil de nuværende tekniske anlæg samt drifts- og sikkerhedsprocedure blive vurderet, og der bliver om nødvendigt opstillet forslag til opdatering af anlæg, sikkerhedsprocedure og beredskabsplaner. Sikkerhedsniveauet vil blive differentieret ud fra vurderingen af risicienes sandsynlighed og konsekvens – for eksempel differentieres sikkerhedsniveauet afhængigt af risikoen for forurening af sårbare vandressourcer.**



## Fase 3. Valg af risikostrategi

På baggrund af de identificerede og analyserede mulige aktiviteter til imødegåelse af risici udarbejdes en anbefaling om valg af risikostrategi. Anbefalingen bør indeholde en gennemgang af risikoanalyse, overvejelser vedrørende forskellige mulige aktiviteter, deres effektivitet, omkostning samt overvejelser om muligheden for implementering af de anbefalede aktiviteter og en eventuel tidshorisont.

Fasen kan med fordel realiseres med afholdelse af små arbejdsmøder med nøglepersoner og risikoejere for hver af de identificerede risici, ligesom erfaringer fra lignende institutioner eller private virksomheder kan inddrages. Specialister inddrages i fornødent omfang eventuelt også. Resultatet er et valg eller anbefaling af en risikostrategi. Se eventuelt delafsnit 6.2 for inspiration til mulige risikostrategier.



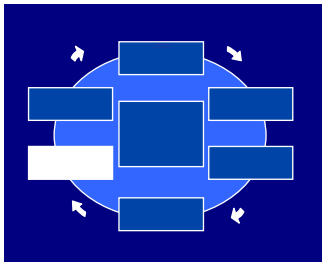
### Fase 4. Eksekvering af risikostrategi og kontrolaktiviteter

Efter at anbefalinger om risikostrategier er udarbejdet, er det tid til at vælge strategier og kontrolaktiviteter, typisk ved hjælp af overvejelser om eksisterende metoder, processer, teknikker mv. Ved valg af risikostrategi og kontrolaktiviteter skal kontrolaktiviteter samt ressourceforbrug for den pågældende risikostrategi planlægges.

Fastsættelse af risikoejere samt målbare kontrolaktiviteter er elementer, som er nødvendige for at understøtte succesfuld eksekvering af de valgte risikostrategier og kontrolaktiviteter. Når dette er gjort, er det op til den enkelte risikoejer at sikre, at strategien eller kontrolaktiviteten bliver udført i henhold til den fastsatte strategi.

Risikoejerne vælger i samråd med de projektansvarlige for etableringen af risikostyringen en eller flere risikostrategier, institutionen skal eksekvere. Samtidig opstilles der målbare kontrolaktiviteter og en ressourceplan for fremtidige aktiviteter.

### Fase 5. Måling, monitorering og rapportering

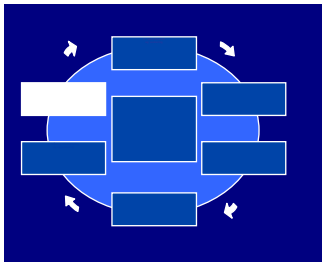


På ambitionsniveau 2 sker monitorering af enkelte risikostyringsaktiviteter, men ingen overordnet monitorering af hele risikostyringsprocessen. Inden for enkelte af institutionens kerneydelser anvendes således en årlig evaluering af de enkelte risikostyringsaktiviteter.

På et område, der vedrører skader, kan der eventuelt ske skadesregistrering og rapportering heraf, som muliggør analyse og kvantificering af institutionens gennemsnitlige omkostninger ved ofte forekommende skader. Ligeledes vil det på den baggrund være muligt at identificere årsager samt omstændigheder ved skaderne, hvorved fastsættelsen og/eller modificering af risikostrategier gøres lettere. Samtidig vil ressourceforbrug og gevinst ved risikostyring kunne opgøres på specifikke områder i institutionen.

Udviklingen i nøglerisici vil skulle opdateres og rapporteres minimum én gang årligt til risikoejeren og eventuelt på topledernіveau med henblik på videre stillingtagen og handlinger. Rapporteringen sker ofte i forbindelse med processen for årsrapporten. Udviklingen i nøglerisiciene skal endvidere opdateres og rapporteres med en passende

frekvens, der er afstemt efter den enkelte risiko, således at det er muligt at gribe ind, hvis en risiko udvikler sig.



### Fase 6. Forankring

I forankringen på ambitionsniveau 2 sker ofte kun en opsamling og formidling af informationer til de udvalgte personer med interesse inden for det pågældende område.

**Risikostyring i forbindelse med drift og vedligehold af Slots- og Ejendomsstyrelsens (SES) kontorbygninger**

**En af SES' kerneydelser er at forsyne staten med kontorlokaler, herunder administration og udlejning af statens kontorejendomme til ministerier og styrelser. Endvidere er SES ansvarlig for den daglige drift og udvendige vedligehold af ejendommene.**

**SES' kontorejendomme er underlagt den statslige huslejeordning, jf. Akt 331 4/9 2000. Formålet hermed er at gøre statens lokaleforsyning mere markedsorienteret og sikre større effektivitet i lokaleanvendelsen. SES fastsætter derfor huslejen ud fra, hvad ejendommen forventes at kunne indbringe ved udlejning på det private kontorejendomsmarked. SES har som følge heraf også en forsøgsordning med privat forsikring og er således undtaget statens selvforsikring. Forsikringsaftalen dækker alle SES' kontorejendomme og omfatter blandt andet forsikring mod bygningsbrand, stormskader, vandskader, svampe og insekter, huslejetab, husejeransvar og rørskade.**

***Miljø***
**SES har ikke gennemført en overordnet risikostyringspolitik for hele institutionen, men har valgt at gennemføre risikostyring på de mest kritiske områder. Inden for disse områder arbejdes der med risikostyring på alle niveauer i institutionen.**

***Målsætning og beslutningstagning***
**Målsætningen med risikostyring er at optimere nytteværdien af de midler, der anvendes til drift og vedligeholdelse af bygninger og anlæg, samt at bygninger og anlæg vedligeholdes på et højt, passende niveau i forhold til driftsikkerhed, anvendelighed, forsvarlighed, kulturhistorisk værdi/udtryk mv. Risikostyringen varetages af nøglemedarbejder inden for de enkelte områder, men der er fokus på at udbrede ansvaret for, at der udarbejdes risikostyring i forbindelse med alle større projekter.**

***Risikoidentifikation***
**Identifikation af risici forbundet med skader på SES' kontorejendomme vedrører dels risici i forbindelse med driften af ejendommene, dels identifikation af risici i forbindelse med større bygge- og anlægsarbejder.**

**I forhold til de løbende driftsmæssige risici foretages identifikation af skadesrisikoen i forbindelse med byggesyn og tekniske syn, der foretages hvert 2. eller 4. år.**

**Der foretages herudover en særskilt risikoidentifikation i forbindelse med større bygge- og anlægsarbejder. Denne risikoidentifikation indebærer typisk, at projektteamet udarbejder en identifikation af mulige ting, som kan gå galt i forbindelse med byggearbejdet. Det kan for eksempel være, at omfanget af råd og svamp i bygningerne er mere omfattende end antaget, at byggetilladelser forsinkes, at væsentlige eksterne interessenter (fx naboer, bebo-**

**ere) gør indsigelse mod projektet m.v.**

***Review og analyse***
**På baggrund af byggesynene og de tekniske syn udarbejdes tiårige vedligeholdelsesplaner for hver ejendom. Byggesynene og de tekniske syn munder ud i en række anbefalinger til genopretning og istandsættelse, som prioriteres i fire kategorier rangerende fra umiddelbart kritisk til økonomisk hensigtsmæssigt.**

**For de større bygge- og anlægsarbejder gennemføres en vurdering af konsekvens og sandsynlighed forbundet med de identificerede risici, og der iværksættes forebyggende handlinger.**

***Valg af risikostrategi***
**SES har på baggrund af både egne og eksterne erfaringer valgt en overordnet risikostrategi baseret på fastlæggelse af det langsigtede økonomisk mest hensigtsmæssige vedligeholdelsesniveau. Det indebærer et mål om at optimere nytteværdien af de midler, der anvendes til drift og vedligeholdelse af bygninger og anlæg, samt at bygninger og anlæg vedligeholdes på et højt, passende niveau i forhold til driftsikkerhed, anvendelighed, forsvarlighed, kulturhistorisk værdi/udtryk mv.**

**I forbindelse med byggesynene er der udarbejdet konkrete forslag for hver bygning til, hvilke typer af istandsættelses projekter der skal iværksættes for at minimere vedligeholdelsesomkostningerne. SES foretager én gang årligt på baggrund af de samlede tiårsplaner for alle bygninger en overordnet valg af, hvilke vedligeholdelsesprojekter der skal iværksættes.**

**For de konkrete udbedringsprojekter vælges strategien for den enkelte risiko typisk af styregruppen for projektet på baggrund af forslag fra projektgruppen.**

***Eksekvering af risikostrategi og kontrolaktiviteter***
**Gennemførelse af og tilsyn med bygge- og anlægsarbejder er udliciteret og varetages af private rådgivende arkitekt- og ingeniørfirmaer. Kundekoordinatorer, driftsansvarlige, byggekoordinatorer og teknikere i SES foretager løbende leverandøropfølgning og kvalitetssikring.**

**Af særlige tiltag kan endvidere nævnes, at SES har haft fokus på opsætning af brandalarmer og håndslukningsmateriel. Endvidere har SES udarbejdet en instruks for håndværkere, som alle relevante entreprenører og tjenesteydere, som SES indgår aftale med, er forpligtet til at overholde.**

***Måling, monitorering og rapportering***
**Skadesregistreringen indgår som en vigtig parameter i forbindelse med risikostyringen af den løbende drift. Skadesregistreringen har medvirket til at tydeliggøre sammenhængen mellem bygningernes stand og antallet af skader og har dermed resulteret i, at der er iværksat en række processer for at minimere skader ved genopretning og istandsættelse af bygningsmassen. For eksempel er der kommet øget opmærksomhed omkring svampeskader. Dette er i høj grad sket i dialog med de private forsikringsmæglere og -selskaber og dermed også på baggrund af erfaringer fra det private forsikringsmarked.**

**SES foretager skadesregistrering af alle skader. SES bliver orienteret om skader fra kunder, ejendomsteknikere, driftsansvarlige, kundekoordinatorer, mv. En medarbejder hos SES registrerer alle skader via en internetbaseret formular. SES får på baggrund af de elektroniske indberetninger udarbejdet skadesstatistik og ved derfor, hvilke skader der er sket, hvornår de er sket, og hvad omfanget af skaderne har været. Dokumentationen for skaderne journaliseres endvidere på de enkelte ejendommes sager.**
**Endelig foregår der en løbende benchmark af blandt andet SES'**

**forsikrings- og vedligeholdsomkostninger set i forhold til Dansk Ejendoms Indeks. Udviklingen heri rapporteres i SES' årsrapporter.**

***Forankring***
**Opsamling og formidling af information til topledelsen i SES foregår primært via prioriteringsprocessen omkring udarbejdelsen og offentliggørelse af tiårsbudgetterne. Denne vurdering og prioritering indgår således i forbindelse med processerne forbundet med den årlige udarbejdelse af SES' budget.**

**For større byggeprojekter sker der typisk en løbende afrapportering om udviklingen af større risici til projektets styregruppe, som omfatter dele af topledelsen i SES. Den løbende udvikling i skadesstatistikkerne rapporteres til ledelsen efter behov.**

## 6.2. Etablering af en koordineret risikostyring (niveau 3)

Etablering af en mere koordineret risikostyring vil være relevant for institutioner, som allerede har en del erfaringer med risikostyring inden for et specifikt område, men endnu ikke har gennemført en tværgående og overordnet koordineret risikostyring.

Det kan eksempelvis være institutioner, som har gennemført risikostyring af deres materielle aktiver for et specifikt område. Et naturligt næste skridt for disse institutioner vil være at udbrede risikostyringen af dets materielle aktiver til at omfatte alle materielle aktiver i institutionen samt konsekvensen af eventuelle materielle skader på institutionens evne til at levere dets kerneydelser. Eventuelt kan institutionen også udbrede risikostyringen til at omfatte andre risici end skadesmæssige risici – fx risici i forhold til institutionens kerneydelser, sikkerhedsmæssige risici eller risici forbundet med konkrete projekter.

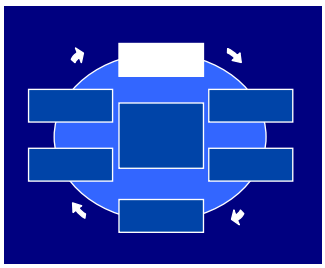
Med etablering af en koordineret risikostyring (ambitionsniveau 3) gennemføres tværgående politikker, processer, metoder og definerede ansvarsroller for risikostyring. På dette niveau behandles flere risici og selv enkelte risici af høj kompleksitet. Risikoidentifikation, review, analyse og valg af risikostrategi foretages mere grundigt. Endvidere foretages monitoreringen og rapporteringen oftere og med et bredere indhold. Der foretages således monitorering og rapportering af målsætninger. Rapporteringen vil derfor muliggøre en løbende evaluering og eventuel justering af risikostyringens mål, indhold og metoder.

Etablering af en koordineret risikostyring stiller krav til involvering af topledelsen. Det er således essentielt, at le-

delsen er involveret med tid, engagement og støtte i forbindelse med igangsætning af risikostyringen, uddelegering af ansvar/roller, sikring af nødvendige ressourcer til gennemførelse samt løbende beslutningstagning.

Risikostyring på ambitionsniveau 3 stiller også krav til den løbende koordination og kommunikationen af risikostyringen. Dette skal afspejles i den organisatoriske struktur, hvor risikostyringen både skal forankres lokalt i de enkelte områder og i en koordinerende funktion enten i institutionens ledelsessekretariat eller hos en selvstændig risk manager.

Etablering af risikostyring på ambitionsniveau 3 vil indebære en udvidet og dybere risikostyring end på ambitionsniveau 2. Der vil dog i høj grad være tale om de samme typer aktiviteter, og elementerne i processen vil være de samme. I det følgende gennemgås derfor for hver af de seks faser i risikostyringen, hvordan etablering af ambitionsniveau 3 adskiller sig fra etableringen af ambitionsniveau 2 i delafsnittet ovenfor.



## Fase 1. Risikoidentifikation og vurdering

### Tværgående risikoidentifikation

Som *forberedelse* til den tværgående risikoidentifikation på tværs af institutionen skal der udarbejdes en oversigt over institutionens samlede ydelser og aktiviteter. Hvis institutionen allerede har udarbejdet et opgavehierarki, kan der tages udgangspunkt heri. Alternativt kan institutionens mål- og resultatstyring bruges til at strukturere oversigten.

Oversigten over ydelser og aktiviteter (evt opgavehierarki) bruges til at identificere risici forbundet med institutionens kerneydelser samt til at sikre, at hele institutionens opgaveportefølje er omfattet af risikoidentifikationen.

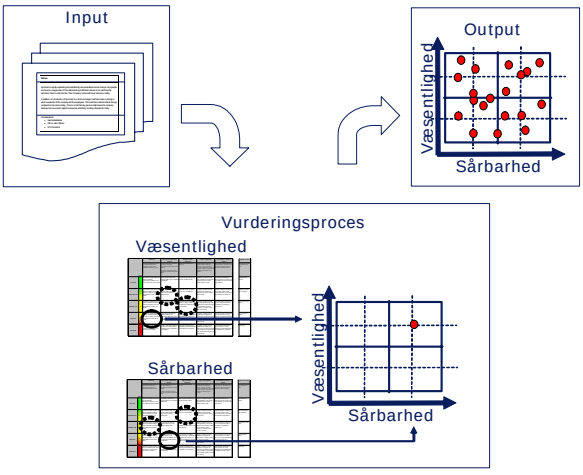
Der foretages herefter en udvælgelse af de nøglepersoner, som har ansvaret for virksomhedens overordnede måloplyldelse. Der vil typisk være tale om direktionen og niveauet under med ansvar for institutionens kerneydelser. De udvalgte personer interviewes enkeltvist for at opnå en forståelse for og foretage en overordnet identifikation af institutionens risici.

Som *dokumentation* udarbejdes en risikobeskrivelse for alle identificerede risici, hvori der indgår en kort beskrivelse af karakteristika og forhold ved hver risiko såsom økonomisk effekt, frekvens, eksisterende forebyggende aktiviteter m.v. Til brug for udarbejdelsen af risikobeskrivelsen kan anvendes interviewskabelonen i bilag 1.3.

### Tværgående risikovurdering – væsentlighed og sårbarhed

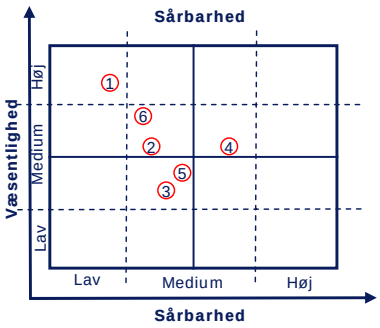
For at foretage en risikovurdering og prioritering af de identificerede risici er det nødvendigt at samle alle de udvalgte nøglepersoner, som har ansvar for institutionens målopfyldelse, til en workshop. Workshoppen har til formål at få udpeget de nøglerisici, det er vigtigst for institutionen at styre og analysere.

På workshoppen foretages på baggrund af de identificerede risici og de udarbejdede risikobeskrivelser en vurdering og prioritering af risici ud fra deres væsentlighed og institutionens sårbarhed.




Væsentligheden vurderes eksempelvis på en skala fra 1-5 (lav, moderat, medium, høj og fatal risiko) ud fra de tidligere valgte risikovurderingskriterier for væsentlighed, jf. delafsnit 5.5. Kriterierne kan eventuelt vægtes forskelligt, hvorefter en endelig vurdering af risikoen kan ske ud fra en gennemsnitsbetragtning. Hvis vurderingen ligger mellem to niveauer, kan en tidsbetragtning evt. medtages i vurderingen. Fx kan responstid ved indtrædelse af hændelse være med til at vægte vurderingen op eller ned.

Sårbarheden kan ligeledes vurderes på en tilsvarende skala fra 1-5 ud fra de tidligere valgte risikovurderingskriterier for sårbarhed, jf. delafsnit 5.5.

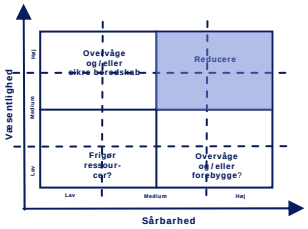



### Tværgående risikoprioritering

Med udgangspunkt i risikobilledet foretages på workshoppen en prioritering af risici med det formål at udvælge nøglerisici til videre behandling.

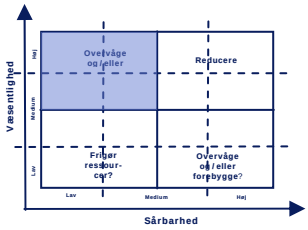
Hvis alle vurderede risici befinder sig i ét område, vanskeliggøres prioriteringen, og det kan overvejes, om vurderingen er foretaget korrekt, eller om vurderingsskalaen skal revurderes. Et rimeligt antal nøglerisici til videre behandling er 15-20. De udvalgte risici skal give et dækkende billede af institutionens forskellige kerneydelser, uden at der bliver tale om et uoverskueligt stort antal.

## Overordnede risikostrategier for de fire områder i risikobilledet



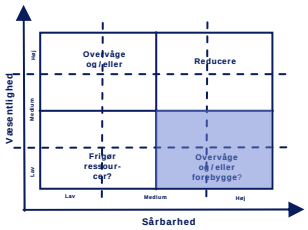

*Reducere*

Risici med høj sårbarhed og høj væsentlighed kan betragtes som højrisici. Hvis muligt skal det overvejes, om der skal ske en risikomitigering gennem forbedring af beredskab og/eller kontroller eller nedbringelse af sårbarhed.



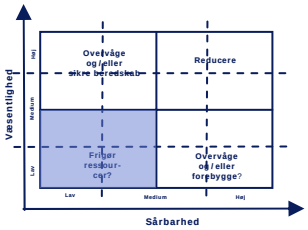

*Overvåge og/eller sikre beredskab*

Heri befinder sig risici, hvor organisationens sårbarhed er lav, samtidig med at væsentligheden er høj. Dette kan eksempelvis være risici, som har en potentielt stor økonomisk eller omdømmemæssigt negativ indflydelse på organisationen, men hvor institutionen allerede har sikret sig gennem eksisterende risikostrategier som for eksempel intensiv overvågning og et tilstrækkeligt beredskab til at håndtere, hvis en given risikobegivenhed forekommer. Institutionen skal sikre sig, at den vurderede sårbarhed til stadighed er så lav, som det er vurderet, eller om eksponeringen er lidt større end antaget, eksempelvis fordi kontrolaktiviteterne ikke længere afdækker risikoen tilstrækkeligt og/eller effektivt. Der kan ofte være en tendens til at indkalkulere "hensigtserklæringer", det vil sige planlagte fremtidige aktiviteter, når der foretages vurdering af aktuel sårbarhed. Det kan få katastrofale konsekvenser at indkalkulere disse fremtidige tiltag, som institutionen har tænkt sig at gennemføre i nær eller fjern fremtid.



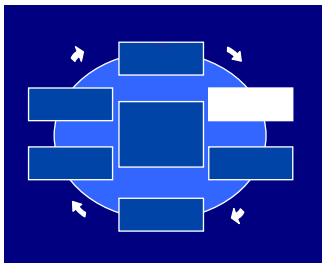

*Overvåge og/eller forebygge*

Her er der tale om potentielle hændelser, som har en relativ lav væsentlighed på institutionen, men hvor sårbarheden er høj. Der skal dog også her foretages en evaluering af risicis indbyrdes effekt for at sikre mod en akkummuleret væsentlighed. Her kan det være relevant at sikre sig, at den vurderede væsentlighed til stadighed har den identificerede lave værdi.




*Frigøre ressourcer*

Her er væsentligheden lille, samtidig med at sårbarheden er lav, hvilket vil kunne sætte spørgsmålstegn ved, hvorvidt organisationen bruger for mange ressourcer på overvågning og kontrol af disse risici, og om nogle ressourcer derfor kan frigøres. Der skal dog foretages en evaluering af risicis indbyrdes effekt for at sikre mod en akkummuleret væsentlighed.



## Fase 2. Review og analyse

Efter valg af nøglerisici til videre behandling udvælges risikoejere, der skal analysere risikoen nærmere og opstille en eventuel risikostrategi for behandling af den pågældende risiko. Den nærmere risikoanalyse foretages på et lavere organisatorisk niveau og vil kunne foretages som beskrevet i delafsnit 6.1.

Til forskel fra ambitionsniveau 2 behandles enkelte risici i et samarbejde mellem flere afdelinger. Eventuelt anvendes også eksterne eksperter til analyse og vurdering af mere komplekse risici.

Nedenfor er givet en kort beskrivelse af mulige analysemetoder for ambitionsniveau 3. En nærmere introduktion til metoderne og anvendelsen kan læses i den almindelige risikostyringslitteratur, jf. bilag 1.5.

### Analysemetoder

**Beslutningstræer** er et hjælpeværktøj i forbindelse med analyse og valg af forskellige mulige scenarier og handlinger. Beslutningstræerne muliggør en effektiv struktur for beslutningsanalysen, som kan anvendes til opstilling af muligheder og vurdering af mulige output ved valg af forskellige handlinger. Beslutningstræer kan ligeledes hjælpe med at skabe et balanceret billede af de risici og fordele, der kan være relateret til forskellige handlings- og procesforløb.

**HAZOP** (HAZard and OPerability Study) er en systematisk risikoanalyse til vurdering af fare- og risikomomenter samt risikoklassifikation. Metoden bruges især til at undersøge, om processer og anlæg afviger fra den måde, de blev designet på. HAZOP anvendes typisk som en metode på en workshop til at foretage en systematisk gennemgang af designet af en given proces eller et givent anlæg. HAZOP er som metode bedst anvendelig, når designet af en proces eller et anlæg er forholdsvist fastlagt.

**Fejl Måde og Effekt Analyse** (FMEA) er en metode til tidligt at kunne lave analyser af potentielle pålidelighedsproblemer i udviklingsfasen, hvor det er let at lave ændringer for at overkomme de identificerede problemer. FMEA kan med fordel anvendes til identifikation af potentielle fejltilstande, estimering af deres konsekvens samt identifikation af mulige aktiviteter i forbindelse med forebyggelse eller mitigering af de identificerede uønskede hændelser.

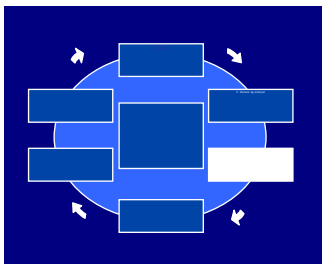
**Root Cause**-analyse omhandler identifikation af årsager til problemer eller hændelser. Metoden bygger på en grundlæggende antagelse om, at et problem løses bedst gennem ændring eller eliminering af grundlæggende årsager i modsætning til blot at behandle de umiddelbart synlige konsekvenser. Gennem behandling eller sikring/kontrol af årsag håbes der på, at væsentligheden eller sandsynligheden for problemet reduceres.

**Bayesiske beslutnings netværk** (BBN) tilbyder en avanceret løsning på analyse af de problemer, der oftest løses ved hjælp af kvalitative analyser såsom anvendelsen af Scorecards eller Key Risk Indicators. De bayesiske netværk muliggør kombination af både kvalitative og kvantita-

tive informationer til brug i risiko- og beslutningsanalyser. De muliggør probalistisk estimering af tab/gevinst samt identificering af mest sandsynlige udfald og årsag for det ønskede scenario. Netværket har fortræffelige egenskaber til analyse af processer, scenarier, tekniske systemer og procedurer. Der kan f.eks. analyseres kontroleffektivitet for komplekse systemer, estimeres mest sandsynlige hændelses udfald og/eller årsag samt deres omkostning/gevinst for givne scenarier. De er ydermere særligt anvendelige til modellering af operationelle risiko med ingen eller næsten ingen historik.

**Value-at-Risk** (VaR) anvendes af virksomheder til opgørelse af risici. En porteføljе risk manager kan med fordel anvende VaR til probalistisk at beskrive risikoen for virksomhedens aktiver. Således beskriver VaR hvor meget værdien af et aktiv eller en portefølje af aktiver vil falde over en given periode med en given sandsynlighed (konfidens niveau).

**Cash flow analyse** (pengestrøms analyse) omhandler en vurdering af om institutionens indsatser er værdiskabende. I forbindelse med risikostyring, vil cash flow analyser typisk udarbejdes for én risiko med forskellige scenarier, hvorved mulige udfald for forskellige scenarier kan vurderes.



## Fase 3. Valg af risikostrategi

Risikoejerne tager med udgangspunkt i eventuelle review og analyser stilling til, hvilken risikostrategi der anbefales over for institutionens ledelse, og udarbejder en anbefaling/indstilling til ledelsen. Stikordene i de forskellige strategikategorier nedenfor kan bruges som inspiration til opstilling af mulige risikostrategier for institutionen.

### Risikostrategier

#### Undgå

- **Afhænde** risikoen ved at undgå at beskæftige sig med det pågældende område
- **Forbyde** de aktiviteter, der resulterer i en risiko
- **Standse** specifikke aktiviteter for eksempel gennem reallokering af ressource
- **Sigte** efter mindre risikoholdige aktiviteter
- **Eliminere** kilden gennem design og implementering af forebyggende aktiviteter

#### Beholde

- **Acceptere** risikoen på det nuværende niveau
- **Revurdere** prisfastsættelse af produkter, services, inkluderende udgifter til forsikring eller kompensation for risikovillighed
- **Samle** risiko i gruppe med andre risici
- **Planlægge og dokumentere** eventuelle handlingsplaner i tilfælde af indtrædelse af hændelse

#### Reducere

- **Sprede** risikoen ud på flere geografiske områder for at reducere væsentligheden

- **Kontrollere** risikoen gennem interne processer, kontroller og handlinger, der reducerer sårbarheden

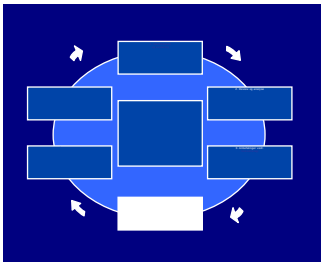
**Overføre**

- **Dele risiko og gevinst** gennem indgåelse af partnerskab
- **Udlicitere** opgaver og processer

**Udnytte**

- **Allokere** interne ressourcer til at imødekomme risiko
- **Udvide** forretningsområde
- **Skabe** nye produkter/ydelser, som medfører yderligere værdi
- **Reorganisere** processer
- **Prisfastsætte** produkter for at påvirke kunder
- **Genforhandle** eksisterende kontrakter og aftaler
- **Påvirke** lovgivning, organisationer og andre interessenter

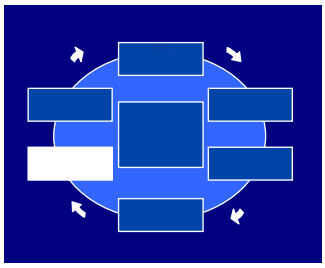
### Fase 4. Eksekvering af risikostrategi og kontrolaktiviteter



Institutionens ledelse skal ud fra givne anbefalinger udvælge et antal risikostrategier og kontrolaktiviteter til eksekvering. Ledelsen udpeger ansvarlige for udførelse af risikostrategier, kontrolaktiviteter samt måling, monitorering og rapportering af effekt af valgte risikostrategier.

Samtidig er ledelsen ansvarlig for, at budgetter samt eventuelle tidsplaner for de enkelte risikostrategier etableres, før de enkelte risikostrategier eksekveres.

### Fase 5. Måling, monitorering og rapportering



Der skal løbende foretages registrering og rapportering til de forskellige organisatoriske niveauer. Rapporteringen foregår med en passende, normalt årlig frekvens. Afhængigt af niveau og karakteristika ved institutionens risici skal der rapporteres en eller flere gange årligt og med forskelligt indhold.

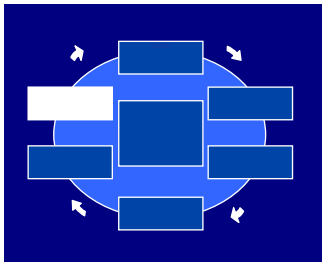
For hvert organisatorisk niveau skal der udpeges ansvarlige, som skal evaluere den aktuelle risikostyring i institutionen med passende frekvens. På ambitionsniveau 3 kan den overordnede evaluering af risikostyring varetages af en etableret risikokomité.

Udviklingen i nøglerisiciene skal endvidere opdateres og rapporteres topledelsen, risikokomité og risikoejerne med en frekvens, der er afstemt efter den enkelte risiko, såle-

des at det er muligt at gribe ind, hvis en risiko udvikler sig.

Rapporteringen vil eventuelt kunne foregå i forbindelse med processen for årsrapporten. Risikostyringen vil således kunne integreres som et element i institutionens generelle rapporteringsmæssige processer.

### Fase 6. Forankring



Erfaringer og metoder deles med øvrige fagspecialister samt eventuelle risiko-områdeansvarlige eller afdelingsledere på tværs af områder og afdelinger. Institutionen arbejder dermed hen mod en fælles forståelse af risici.

For at understøtte forankringen er det væsentligt, at ledelsen får løbende review af risikostyringsprocessen og på den baggrund sikrer, at oplevede effekter kommunikeres ud i hele institutionen.

Der skal endvidere udsendes årlige rapporter/notater om risikostyring i institutionen for at skabe øget forståelse, accept og engagement. Endvidere kan risikostyring indgå i årsrapporten.

**Risikostyring i SKAT**

**SKAT har igennem en årrække arbejdet med risikostyring på flere niveauer. Netop nu er man ved at lægge sidste hånd på en ny model for risikoledelse, som er planlagt til at gå i luften 1. januar 2007. Modellen indebærer, at der fremover sondres imellem henholdsvis strategisk risikoledelse og operationel risikostyring i SKAT.**

**Målet med den strategiske risikoledelse er ved en kontinuer proces at overvåge væsentlige strategiske risici i SKAT. Processen indebærer løbende identifikation, evaluering samt håndtering af de strategiske risici. Inputtet til risikoledelsen skal komme ad flere kanaler i SKAT, herunder fra SKATs styringsmodel, via ledelsesinformationen samt fra sikkerhedsfunktionen.**

**Samarbejdet mellem direktionen og samarbejdsdirektionerne i SKAT skal sikre en helhedsorienteret proces, hvor ledelsen ikke kun forholder sig til enkelte risici, men også forholder sig til tværorganisatoriske problemstillinger.**

**Målet med den operationelle risikostyring i SKAT er at udføre en række obligatoriske og valgfrie interne kontrolaktiviteter, med fokus på kvalitet, effektivitet samt overholdelse af relevante retningslinjer og love. Uhensigtsmæssige forhold, der måtte fremkomme ved gennemførelsen af de interne kontrolaktiviteter, vil i nødvendigt omfang blive eskaleret til adressering under den strategiske risikoledelse. Hvor den strategiske risikoledelse er tænkt fremadrettet, er den operationelle risikostyring primært bagudrettet.**

**Facilitering af begge risikostyringsdiscipliner skal ske via en central risikostyringsfunktion.**

**SKATs risikokompetencer pr. 1. januar 2007 er nedenfor beskrevet i forhold til de 8 evalueringskriterier i denne vejlednings model for ambitionsniveau.**

***Miljø***
**SKATs risikoledelses- og styringsaktiviteter udspringer af en overordnet risikopolitik. Risikopolitikken udgør det overordnede grundlag for såvel den strategiske risikoledelse som den operationelle risikostyring. Risikopolitikken fastsætter bl.a. formål, risikoområder, ansvarsfordeling, risikovillighed samt den organisatoriske forankring af risikoledelse og -styring.**

***Målsætning for risikostyring***
**Målsætningen med SKATs risikoledelse og risikostyring er at sikre fokus på og udbredelse af ansvaret for, at der udøves en dynamisk og proaktiv risikoledelse og risikostyring i hele organisationen. Risikoledelse og risikostyring skal udføres på alle niveauer og skal sikre SKATs realisering af mission, vision og strategiske målsætninger.**

***Risikoidentifikation og vurdering***
**Identifikation af risici i SKAT er flerdimensional, og sker blandt andet ved direktionens initiale risikoanalyse, indsamling af input fra direktionsmedlemmer, samarbejdsdirektioner samt eskalering af risici fra den operationelle risikostyring.**

**For alle de identificerede risici dokumenteres en række stamdata, såsom risikobeskrivelse, kategori, konsekvensbeskrivelse. Den enkelte risiko vurderes ligeledes for så vidt angår sandsynlighed og konsekvens. Samlet set beregnes en score for den enkelte risiko, og denne score afgør, hvordan risikoen efterfølgende skal behandles.**

***Review og analyse***
**Afhængigt af bl.a. risikoens score besluttes det, om der skal udarbejdes risikoplaner med henblik på iværksættelse af imødekommende foranstaltninger. Vælges der ikke straks at udarbejde en risikoplan, vil udviklingen for den enkelte risiko løbende blive overvåget.**

***Risikostrategi***
**Strategien for den enkelte risiko vil dels fremgå af risikologgen, dels af risikoplanen, såfremt en sådan er udarbejdet.**

***Eksekvering af risikostrategi samt kontrolaktiviteter***
**Eksekvering af imødekommende foranstaltninger sker i henhold til risikologgen og risikoplanen.**

**Derudover gennemføres der kontinuert en række kontrolaktiviteter, som beskrevet ovenfor vedrørende operationel risikostyring.**

***Måling, monitorering og rapportering***
**Status for de enkelte risici bliver løbende overvåget af den centrale risikostyringsfunktion. Der sker bl.a. via udarbejdelse af statistisk ledelsesinformation samt via løbende indhentning af status på risikoplaner, iværksatte aktiviteter mv. fra den pågældende ansvarlige for den enkelte risiko. Dokumentationen sker i risikologgen, som er centralt udviklet og styret.**

***Forankring***
**Risikoledelsen er forankret hos den øverste ledelse i SKAT – hos Direktionen og samarbejdsdirektionerne, som løbende forholder sig til de aktuelle strategiske risici. Direktionen i SKAT vil årligt tage stilling til om den aktuelle risikopolitik og model for risikoledelse skal justeres. Denne proces faciliteres ligeledes af den centrale risikostyringsfunktion.**

## 6.3. Etablering af en helhedsorienteret risikostyring (niveau 4)

Etablering af en helhedsorienteret risikostyring er kun relevant for institutioner af en vis størrelse, og som allerede har gjort sig en del erfaringer med risikostyring.

Med etablering af helhedsorienteret risikostyring etableres klare risikostrategier for samtlige nøglerisici, institutionen vil være eksponeret overfor. Medarbejderne forstår eskaleringsprocedurerne, og hvordan deres funktion bidrager til realisering af strategien, og de agerer proaktivt i forhold til håndtering af risici.

For at etablere helhedsorienteret risikostyring er det nødvendigt, at risikostyringens elementer og indhold i høj grad kommunikeres ud og integreres i hele organisationen. Risikostyringsprocessen er en integreret del i hele organisationen, og alle afdelinger er berørt og følger frekvensvist risikostyringsprocessens faser. Det kræver, at risikostyringsprocessen integreres fuldt ud i institutionens processer.

Helhedsorienteret risikostyring indebærer også, at der opnås erfaring i institutionen med forskellige analysetyper og mere dybtgående analyser, hvor afledte effekter og korrelationer mellem eksisterende risikoaktiviteter tages med i betragtning. Det kræver, at institutionen opbygger og indsamler erfaringer samt uddanner medarbejdere i risikostyringsprocesser og analysemetoder.

Rapporteringen på ambitionsniveau 4 indebærer en løbende rapportering på alle niveauer i institutionen. Helhedsorienteret risikostyring indebærer således, at risikostyringen indgår i den almindelige faste ledelsesrapportering. Effekten af risikostyringen for hele organisationen evalueres og monitoreres dermed løbende.

Risikostyringen på ambitionsniveau 4 kræver også, at der etableres systemunderstøttelse, som dermed kan give hele institutionen mulighed for løbende at følge udviklingen.
Endelig kræver helhedsorienteret risikostyring, at kommunikationen af risikostyringstiltag og opfølgning når ud til alle i institutionen. Det kræver derfor en yderligere forankring af risikostyring i organisationen, fx med etablering af en risk manager-funktion samt en risikokomité.

## 6.4. Etablering af en risikointelligent tilgang til risikostyring (niveau 5)

Etablering af en risikointelligent tilgang til risikostyringen er forbeholdt meget store offentlige institutioner med komplekse risici, hvor risikostyring allerede har haft værdi over en lang periode.

En risikointelligent institution adskiller sig fra andre institutioner ved, at alle medarbejdere deltager aktivt i informationsindsamlingen og rapporteringen. Ændrede forhold videregives automatisk til de risikoansvarlige, som rapporterer videre hvis nødvendigt. Risici analyseres med både kvantitative og kvalitative metoder, og institutionen påtager sig på den baggrund de risici, der medfører, at institutionen kan realisere sine målsætninger på bedste vis.

Etableringen af en risikointelligent institution kræver først og fremmest, at ledere og medarbejderne har fået risikostyring på rygmarven gennem erfaring, videndeling og generel uddannelse i risikostyring. Risikostyring skal således være blevet en del af alle medarbejderes job, og effekten er kendt og anerkendt af samtlige medarbejdere.

For at blive en risikointelligent institution skal institutionen også kunne gennemføre avancerede kvantitative og kvalitative risikoanalyser, og resultatet heraf skal indgå i den konkrete beslutningstagning, således at risici påtages på intelligent vis.

Endvidere kræver ambitionsniveau 5, at risikostyringen benchmarkes både internt i institutionen og med andre institutioner. Resultaterne heraf kan dermed indgå som et element i risikoanalysen.

Ambitionsniveau 5 kræver også implementering af et system, der understøtter hele risikostyringsprocessen og derved muliggør en systemunderstøttet sammenkædning af identifikation, analyse, valg af strategi og rapportering.

Endelig kræver en intelligent risikostyring, at ny viden og nye risici straks kommunikeres systematisk ud til de relevante parter. En intelligent risikostyring kræver derfor også en egentlig risikoorganisation, for eksempel i form af en risikokomité og en risk manager.