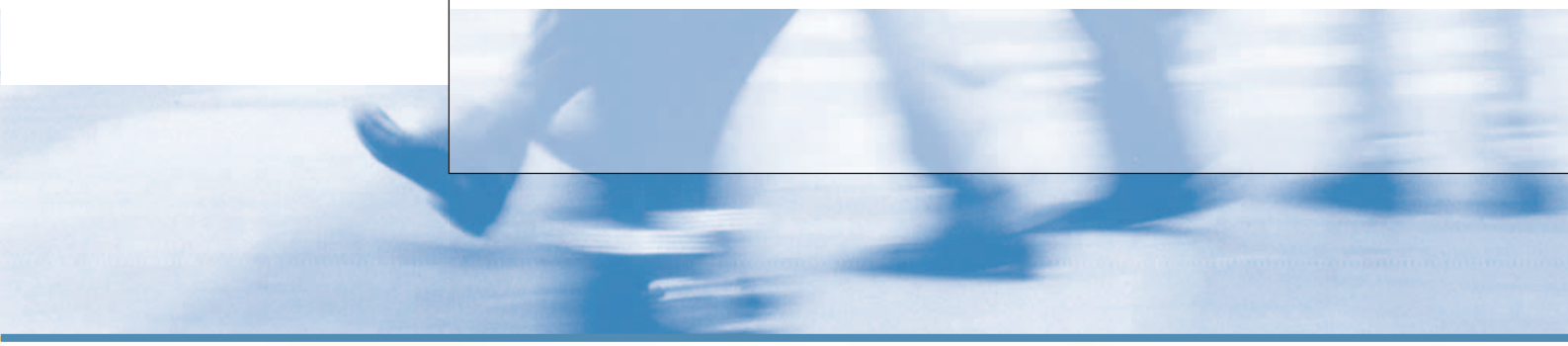
ferma

FEDERATION OF
EUROPEAN RISK
MANAGEMENT
ASSOCIATIONS

STANDARDEN FOR RISIKOSTYRING



Indledning

Standarden for risikostyring er resultatet af et samarbejde mellem Englands største organisationer for risikostyring – The Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC) og ALARM The National Forum for Risk Management in the Public Sector.

Desuden indhentede teamet over en længere periode med konsultationer en lang række synspunkter fra andre professionelle organer med interesse i risikostyring.

Risikostyring er en hurtigt voksende disciplin, og der er mange forskellige synspunkter om og beskrivelser af, hvad risikostyring omfatter, hvordan den bør gennemføres, og hvad formålet er.

Der er behov for en standard for at sikre, at der er enighed om:

- *terminologien i forbindelse med de anvendte ord*
- *den proces, der anvendes til risikostyring*
- *organisationsstrukturen for risikostyring*
- *formålet med risikostyring*

Væsentligt er det, at standarden anerkender, at der er både positive (upside) og negative (downside) aspekter ved en risiko.

Risikostyring er ikke kun egnet til kommunale virksomheder eller offentlige institutioner, men til alle aktiviteter, uanset om de er kort- eller langsigtede. Fordelene og mulighederne skal ikke kun ses på baggrund af selve aktiviteten, men også i forhold til de mange forskellige interessenter, der kan blive berørt.

Målene for risikostyringen kan være forskellige fra virksomhed til virksomhed, og det ville være umuligt at prøve at opstille dem alle i et enkelt dokument. Det har derfor aldrig været ideen at producere en normativ standard, eller at etablere en proces, der kan certificeres. Ved at opfylde de forskellige dele af denne standard, selv om det er på forskellige måder, kan virksomheder rapportere, at de overholder standarden. Standarden repræsenterer den bedste praksis, som virksomhederne kan sammenligne sig med.

Standarden har, hvor det er muligt, anvendt den risikoterminologi, der er opstillet af International Organization for Standardization (ISO) i dens seneste dokument ISO/IEC Guide 73 Risk Management - Vocabulary - Guidelines for use in standards.

Da dette område er i kraftig udvikling, vil forfatterne sætte pris på feedback fra organisationer og virksomheder, efterhånden som disse begynder at anvende standarden (adresserne kan findes på bagsiden af denne Guide). Det er hensigten, at der vil blive foretaget regelmæssige ændringer af standarden på baggrund af bedste praksis.

1. Risiko

Risiko kan defineres som kombinationen af en hændelses sandsynlighed og dens konsekvenser (ISO/IEC Guide 73).

I alle typer virksomheder vil der potentielt forekomme hændelser og konsekvenser, der giver mulighed for gevinst (positive aspekter), eller som truer succesen (negative aspekter).

Risikostyring anses i stigende grad at omfatte en behandling af både de positive og negative aspekter ved risici. Derfor betragter denne standard risikoen ud fra begge perspektiver.

Inden for området sikkerhed er det almindelig anerkendt, at der kun findes negative konsekvenser, og derfor fokuserer styringen af sikkerhedsrisici på at hindre og mindske skader.

2. Risikostyring

Risikostyring er en central del af enhver organisations strategiske styring. Det er den proces, organisationer benytter til metodisk at tage fat på de risici, der er forbundet med deres aktiviteter, med det formål at opnå vedvarende fordele inden for hver enkelt aktivitet og på tværs samtlige aktiviteter.

Den gode risikostyring skal fokusere på identifikation og behandling af disse risici. Dens formål er at tilføre alle virksomhedens aktiviteter værdi. Den understøtter forståelsen for de potentielle positive og negative aspekter ved alle de faktorer, der kan påvirke virksomheden. Den øger sandsynligheden for succes og reducerer både sandsynligheden for fiasko og usikkerheden omkring, hvorvidt man kan nå virksomhedens overordnede mål.

Risikostyring skal være en kontinuerlig udviklingsproces, der går igennem hele virksomhedens strategi og implementeringen af denne strategi. Den skal metodisk tage fat på alle de risici, der omgiver virksomhedens tidligere, nuværende og specielt fremtidige aktiviteter.

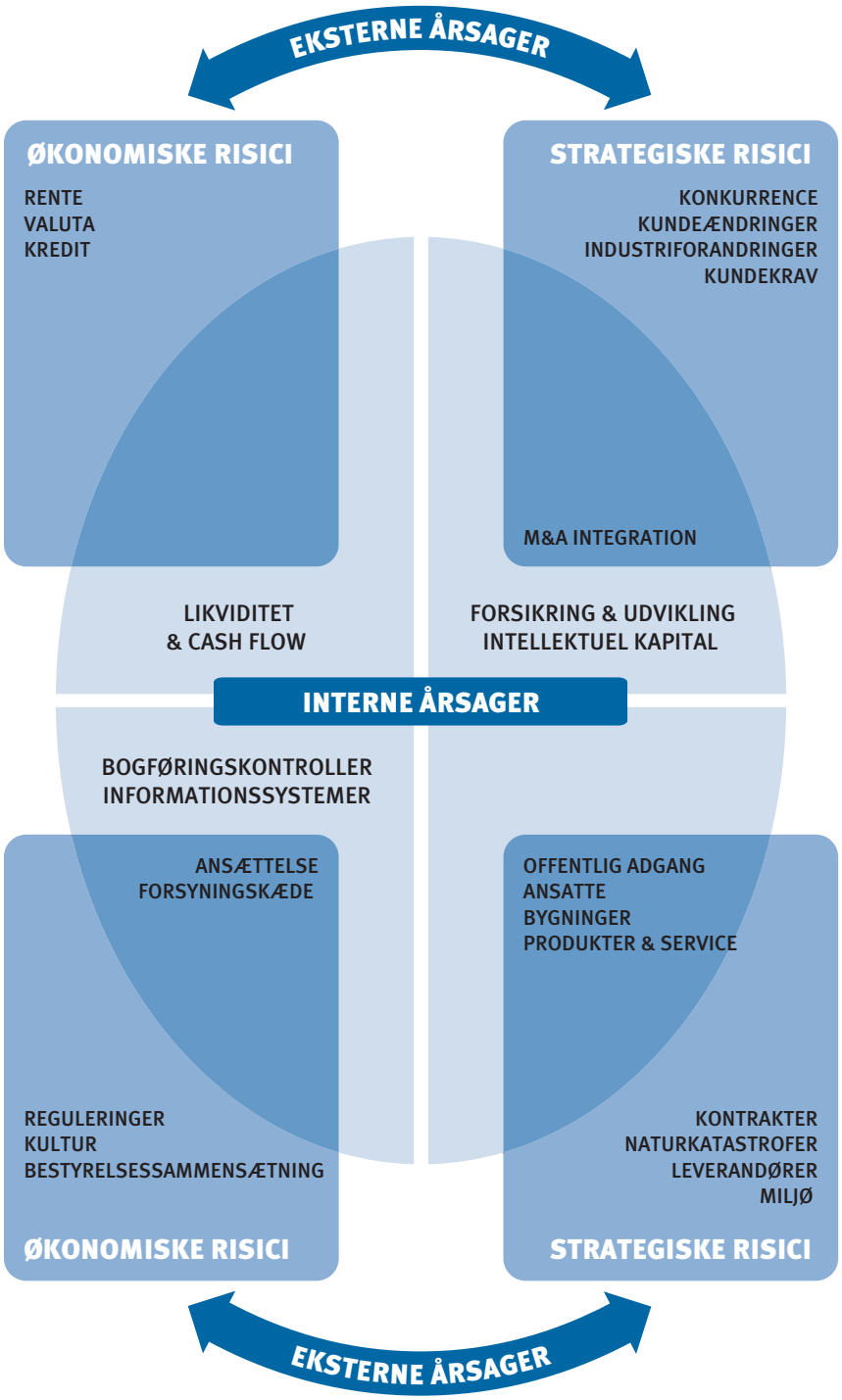
Den skal integreres i virksomhedskulturen med en effektiv politik og et program, der styres af den øverste ledelse. Den skal omsætte strategien til taktiske og driftsmæssige mål og fordele ansvaret i hele virksomheden til alle ledere og medarbejdere, der har ansvaret for risikostyringen som en del af deres jobbeskrivelse. Den understøtter ansvarlighed, præstationsmåling og belønning, hvorved arbejdseffektiviteten øges på alle niveauer.

2.1 Eksterne og interne faktorer

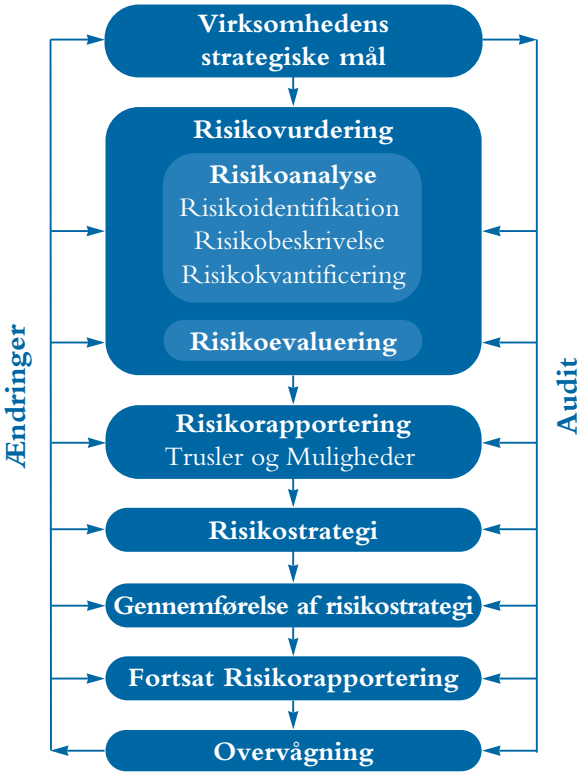
De risici, en virksomhed og dens aktiviteter står over for, kan skyldes både eksterne og interne faktorer.

Diagrammet på næste side, som sammenfatter eksempler på vigtige risici, viser at nogle specifikke risici kan skyldes både eksterne og interne faktorer, og derfor overlapper hinanden. De kan yderligere inddeles i risikotyper som f.eks. strategiske, økonomiske, driftsmæssige, direkte faremomenter etc.

2.1 Eksempler på årsager til vigtige risici



2.2 Risikostyringsprocessen



Risikostyring beskytter virksomheden og tilføjer værdier til organisationen og dens interessenter ved at støtte virksomhedens mål på følgende måde:

- *skaber en ramme for en virksomhed, der sikrer, at fremtidige aktiviteter kan forløbe kontrolleret*
- *forbedrer beslutningstagningen, planlægningen og prioriteringen ved hjælp af en omfattende og struktureret forståelse af aktiviteter, usikkerhed og muligheder/trusler ved projekter*
- *bidrager til en mere effektiv brug/allokering af kapital og ressourcer i virksomheden*
- *reducerer usikkerheden i ikke-essentielle dele af virksomheden*
- *beskytter og øger aktiverne samt forbedrer virksomhedens image*
- *udvikler og understøtter medarbejderne og virksomhedens videnbase*
- *optimerer den driftsmæssige effektivitet*

3. Risikovurdering

Risikovurdering defineres af ISO/IEC Guide 73 som den samlede proces bestående af risikoanalyse og risikoevaluering.
(Se tillæg)

4. Risikoanalyse

4.1 Risikoidentifikation

Risikoidentifikation beskæftiger sig med at identificere, hvor eksponeret en virksomhed er for usikkerhed. Dette kræver et indgående kendskab til virksomheden, det marked, den opererer i, det juridiske, sociale, politiske og kulturelle miljø, den er omgivet af, samt udviklingen af dens strategiske og driftsmæssige mål, herunder faktorer, der er afgørende for dens succes, og de trusler og muligheder, der er forbundet med opnåelsen af disse mål.

Risikoidentifikation skal gribes metodisk an for at sikre, at alle betydningsfulde aktiviteter i virksomheden er blevet identificeret, og at alle risici fra disse aktiviteter er blevet defineret. Al usikkerhed i forbindelse med disse aktiviteter skal identificeres og kategoriseres.

Forretningsaktiviteter og beslutninger kan klassificeres på en lang række måder, og følgende er eksempler herpå:

- *Strategiske – Disse faktorer vedrører virksomhedens langsigtede strategiske mål. De kan påvirkes af faktorer som f.eks. tilgængelig kapital, risiko forbundet med statslige låntagere og politiske risici, juridiske og lovgivningsmæssige forandringer, omdømmet og ændringer i det fysiske miljø.*
- *Operationelle – Disse faktorer vedrører de daglige problemer, virksomheden konfronteres med i sit arbejde for at nå de strategiske mål.*
- *Økonomiske – Disse faktorer vedrører den effektive ledelse og kontrol af virksomhedens økonomi og påvirkningen fra eksterne faktorer som f.eks. kreditmuligheder, valutakurser, bevægelser i renteniveauet og andre påvirkninger fra markedet.*
- *Videnstyring – Disse faktorer vedrører den effektive ledelse og styring af videnressourcer samt produktion, beskyttelse og formidling af disse. Eksterne faktorer kan omfatte den uautoriserede brug eller misbrug af intellektuel ejendom, generelt strømsvigt og konkurrerende teknologi. Interne faktorer kan være systemfejl eller tab af dygtige medarbejdere.*
- *Overensstemmelse med markedskrav – Disse faktorer vedrører emner som f.eks. sundhed og sikkerhed, miljø, varebeskrivelser, forbrugerbeskyttelse, databeskyttelse, medarbejderpraksis og lovgivningsmæssige forhold.*

Selv om risikoidentifikation godt kan udføres af eksterne konsulenter, vil en intern fremgangsmåde med grundigt formidlede, konsistente og koordinerede processer og værktøjer (se tillæg, side 14) sandsynligvis være mere effektiv. Internt "ejerskab" af risikostyringsprocessen er af afgørende betydning.

4.2 Risikobeskrivelse

Formålet med risikobeskrivelse er at vise de identificerede risici i et struktureret format ved for eksempel at bruge en tabel. Tabellen for risikobeskrivelse på næste side kan anvendes til at lette risikobeskrivelsen og -vurderingen. Det er nødvendigt at anvende en veldesignet struktur for at sikre en omfattende risikoidentifikations-, beskrivelses- og vurderingsproces. Ved at overveje hver enkelt risikos konsekvens og sandsynlighed, som de er opstillet i tabellen, skulle det være muligt at prioritere de vigtigste risici, der skal analyseres mere indgående. Identifikationen af de risici, der er forbundet med forretningsaktiviteter og beslutningstagning, kan kategoriseres som strategiske, projektmæssige/taktiske, driftsmæssige. Det er vigtigt at indarbejde risikostyring i den indledende fase af projekter og gennem et givet projekts levetid.

4.2.1 Tabel - Risikobeskrivelse

1. Risikoens navn	
2. Risikoens omfang	Kvalitativ beskrivelse af hændelserne, deres omfang, type, antal og afhængighedsforhold
3. Risikoens natur	For eksempel strategiske, driftsmæssige, økonomiske, viden- eller overensstemmelsesmæssige hændelser
4. Interessenter	Interessenterne og deres forventninger
5. Risikokvantificering	Betydning og sandsynlighed
6. Risikotolerance/-appetit	Potentielt tab og den økonomiske virkning Risikoens værdi Sandsynlighed for og størrelse af eventuelle tab/gevinster Mål for kontrol af risikoen og det ønskede præstationsniveau
7. Risikobehandling og kontrolmekanismer	De vigtigste midler, der for tiden bruges til risikostyring Tillid til eksisterende kontrol Identifikation af protokoller til overvågning og revision
8. Eventuelle tiltag til forbedring	Anbefalinger til reduktion af risici
9. Udvikling af strategi og politik	Identifikation af den funktion, der er ansvarlig for at udvikle strategi og politik

4.3 Risikokvantificering

Risikoskøn kan være kvantitativt, semikvantitativt eller kvalitativt, hvad angår sandsynligheden for forekomsten og dennes eventuelle konsekvens.

For eksempel kan konsekvenserne, både hvad angår trusler (risici med negative aspekter) og muligheder (risici med positive aspekter), være høje, middel eller lave (se tabel 4.3.1). Sandsynligheden kan være høj, middel eller lav, men det kræver forskellige definitioner af trusler og muligheder (se tabellerne 4.3.2 og 4.3.3).

I tabellerne på de næste sider gives der eksempler. Forskellige virksomheder vil opdage, at deres behov kræver forskellige målesystemer for konsekvens og sandsynlighed.

For eksempel er mange virksomheder af den opfattelse, at det er tilstrækkeligt for dem at vurdere konsekvens og sandsynlighed som stor, middel eller lav og at præsentere dette som en 3 x 3 matrix.

Andre virksomheder synes, at det giver dem en bedre vurdering, når konsekvens og sandsynlighed anslås ved hjælp af en 5 x 5 matrix.

Tabel 4.3.1 Konsekvenser – Både trusler og muligheder

Store	Den økonomiske afsmitning på virksomheden vil sandsynligvis overstige £x Betydelig indflydelse på virksomhedens strategi eller driftsmæssige aktiviteter Medfører betydelig bekymring for interessenterne
Middel	Den økonomiske afsmitning på virksomheden vil sandsynligvis ligge mellem £x og £y Moderat indflydelse på virksomhedens strategi eller driftsmæssige aktiviteter Medfører moderat bekymring for interessenterne
Små	Den økonomiske afsmitning på virksomheden vil sandsynligvis være under £y Ringe indflydelse på virksomhedens strategi eller driftsmæssige aktiviteter Medfører ringe bekymring for interessenterne.

Tabel 4.3.2 Sandsynlighed for forekomst - Trusler

Vurdering	Beskrivelse	Indikatorer
Stor (Sandsynlig)	Vil sandsynligvis forekomme hvert år eller mere end 25 % risiko for forekomst.	Kan forekomme flere gange inden for tidsperioden (for eksempel ti år) Er forekommet for nylig.
Middel (Mulig)	Vil sandsynligvis forekomme i løbet af en tiårig periode eller mindre end 25 % risiko for forekomst.	Kan forekomme mere end én gang inden for en bestemt tidsperiode (for eksempel ti år). Kan være svær at kontrollere på grund af påvirkninger udefra Er den forekommet tidligere?
Lav (Usandsynlig)	Vil sandsynligvis ikke forekomme i en tiårig periode eller mindre end 2% risiko for forekomst.	Er ikke forekommet. Vil sandsynligvis ikke forekomme.

Tabel 4.3.3 Sandsynlighed for forekomst - Muligheder

Vurdering	Beskrivelse	Indikatorer
Stor (Sandsynlig)	Der vil kunne opnås et favorabelt resultat på et år eller mere end 75% chance for forekomst.	Entydig chance, som man med rimelig sikkerhed kan stole på vil kunne udnyttes på kort sigt baseret på de nuværende styringsprocesser.
Middel (Mulig)	Rimelige udsigter til gunstige resultater på et år eller 25% til 75% chance for forekomst.	Muligheder, der kan opnås, men som kræver omhyggelig styring. Muligheder, der kan opstå ud over planen.
Lav (Usandsynlig)	Nogen chance for gunstige resultater på mellemlangt sigt eller under 25 % chance for forekomst.	Mulig chance, der endnu mangler at blive fuldt undersøgt af ledelsen. Der er ringe chance for succes på basis af de styringsressourcer, der for tiden findes.

4.4 Metoder og teknikker til risikoanalyse
Der kan anvendes en række teknikker til risikoanalyse. Disse kan være specielt rettet mod positive- eller negative aspekter ved risici eller de kan anvendes på begge. ***(Se tillæg, side 14, vedrørende eksempler)***.

4.5 Risikoprofil
Resultatet af risikoanalyseprocessen kan anvendes til udarbejdelse af en risikoprofil, der vurderer hver enkelt risikos betydning og giver et værktøj til prioritering af arbejdet med risikobehandling. Dette klassificerer alle identificerede risici, så man får en oversigt over den relative betydning.

Denne proces, der gør det muligt at knytte risikoen til det berørte forretningsområde, beskriver de eksisterende primære kontrolprocedurer og angiver, i hvilke områder investeringsniveauet for risikokontrol kan øges eller omfordeles.

Ansvarlighed er med til at sikre, at risikoens 'ejerskab' anerkendes, og at den passende styringsressource tildeles.

5. Risikoevaluering

Når risikoanalyseprocessen er fuldført, er det nødvendigt at sammenligne de anslåede risikokriterier med de risikokriterier, virksomheden har opstillet. Risikokriterier kan omfatte tilknyttede omkostninger og udbytter, juridiske krav, socioøkonomiske og miljømæssige faktorer, interessenternes bekymringer etc. Risikoevaluering anvendes derfor til at træffe afgørelser vedrørende risikoens betydning for virksomheden og om, hvorvidt hver enkelt risiko skal accepteres eller behandles.

6. Risikostrategi

Risikobehandling er den proces, hvorved de tiltag, der skal til for at modificere risikoen, vælges og implementeres. Risikobehandling omfatter som vigtigste element risikokontrol/risikominimering, men den går videre end det og omfatter f.eks. også risikoafværgelse, risikooverførsel, risikofinansiering, etc.

BEMÆRK: I denne standard henviser risikofinansiering til de mekanismer (f.eks. forsikringsprogrammer), der finansierer de økonomiske konsekvenser. Risikofinansiering anses ikke i almindelighed for at omfatte tilvejebringelse af økonomiske midler til imødegåelse af omkostningerne ved at gennemføre risikobehandling (som defineret af ISO/IEC Guide 73; se side 17).

Ethvert system til risikobehandling skal som minimum sørge for:

- *en effektiv og virkningsfuld drift af virksomheden*
- *effektive interne kontroller*
- *overensstemmelse med love og regulativer.*

Risikoanalyseprocessen er en hjælp til den effektive og dygtige drift af virksomheden, da den identificerer de risici, som kræver ledelsens opmærksomhed. Ledelsen skal så prioritere tiltagene til risikokontrol, alt efter i hvilken udstrækning de vil kunne gavne virksomheden.

Den interne kontrols effektivitet er afgørende for, om risikoen enten vil blive elimineret eller reduceret af de foreslåede kontroltiltag.

Omkostningsrentabiliteten ved den interne kontrol udregnes på baggrund af udgiften til implementering af kontrollen sammenlignet med den forventede gevinst ved risikoreduktionen.

Målingen af omkostningsrentabiliteten ved de foreslåede kontroller skal ske ved at sammenholde den potentielle økonomiske effekt, hvis der ikke foretages noget, med udgiften til de foreslåede tiltag og kræver mere detaljerede oplysninger og flere forudsætninger, end der umiddelbart er til rådighed.

Først skal man fastslå omkostningerne i forbindelse med implementeringen. Disse skal udregnes meget præcist, da det hurtigt bliver den basis, omkostningsrentabiliteten måles ud fra. Endvidere skal det forventede tab, hvis der ikke gennemføres tiltag, vurderes, hvorefter ledelsen kan sammenligne resultaterne og ud fra disse afgøre, hvorvidt tiltagene til risikokontrol skal implementeres.

Man kan ikke vælge, om man vil overholde love og regulativer. En virksomhed skal forstå gældende love og implementere et system af kontroller, der sikrer, at disse overholdes. Der vil kun en gang imellem forekomme nogen fleksibilitet, hvor udgiften til reduktion af en risiko kan stå i afgjort misforhold til den pågældende risiko.

En måde at opnå økonomisk beskyttelse mod risicienes påvirkning er gennem risikofinansiering, der omfatter forsikring. Det er imidlertid nødvendigt at indse, at visse tab eller elementer af et tab ikke vil kunne forsikres, dvs. de ikke forsikrede omkostninger i forbindelse med arbejds- og sundhedsskader eller miljøhændelser, der kan medføre skade på medarbejderes moral og virksomhedens rygte.

7. Risikorapportering

7.1 Intern rapportering

De forskellige niveauer i en virksomhed har brug for forskellige oplysninger fra risikostyringsprocessen.

Direktionen skal:

- *kende til de vigtigste risici, virksomheden står over for*
- *kende de mulige virkninger på aktionærværdien af afvigelser fra de forventede resultater*
- *sikre et tilfredsstillende bevidsthedsniveau i hele virksomheden*
- *vide, hvordan virksomheden vil klare en krise*
- *være klar over betydningen af interessenters tillid til virksomheden*
- *vide, hvordan kommunikationen med investormiljøet skal styres, hvor dette er relevant*
- *være sikker på, at risikostyringsprocessen arbejder effektivt*
- *offentliggøre retningslinjer for en klar risikostyringspolitik, der omfatter risikostyringsfilosofi og ansvar.*

Forretningsenhederne skal:

- *være opmærksomme på risici inden for deres ansvarsområde, den eventuelle indflydelse, disse kan have på andre områder, og de konsekvenser, andre områder kan have for dem*
- *have præstationsindikatorer, der gør det muligt at overvåge vigtige forretningsmæssige og økonomiske aktiviteter og følge fremskridtene i forhold til målene samt identificere udviklinger, hvor det kan være nødvendigt at gribe ind (f.eks. overslag og budgetter)*
- *have systemer, der med passende mellemrum underretter variationer i budgetter og overslag, så der kan gribes ind*
- *rapportere systematisk og hurtigt til topledelsen, hvis der dukker en ny risiko op, eller hvis de eksisterende kontroltiltag ikke fungerer.*

De enkelte medarbejdere skal:

- *forstå deres ansvar for individuelle risici*
- *forstå, hvordan de kan igangsætte kontinuerlig forbedring af responsen på risikostyringen*
- *forstå, at risikostyring og risikobevidsthed er en vigtig del af virksomhedens kultur*
- *rapportere systematisk og hurtigt til topledelsen, hvis der dukker en ny risiko op, eller hvis de eksisterende kontroltiltag ikke fungerer.*

7.2 Ekstern rapportering

En virksomhed skal regelmæssigt orientere sine interessenter om virksomhedens risikostyringspolitikker og om, hvor langt man er nået for at opnå målene.

Interessenter forlanger i stigende grad, at virksomheder beviser en effektiv styring af deres ikke-økonomiske præstationer, f.eks. inden for lokalsamfundet, menneskerettighederne, medarbejderpraksis, sundhed og sikkerhed på arbejdspladsen samt miljøet.

En god virksomhedsstyring forudsætter, at virksomheder anlægger en metodisk indfaldsvinkel til risikostyring, der:

- *beskytter deres interessenters interesser*
- *sikrer, at bestyrelsen opfylder sine forpligtelser til gennemførelse af en direkte strategi, opbygger værdier og overvåger virksomhedens præstationer*

- *sikrer, at styringsværktøjerne er til stede, og at de arbejder effektivt.*

Bestemmelserne vedrørende den formelle rapportering i forbindelse med risikostyringen skal være klart formulerede og være tilgængelige for interessenterne.

Den formelle rapportering skal behandle:

- *kontrolmetoderne – især ledelsens ansvar for risikostyringen*
- *de processer, der anvendes til identificering af risici, og hvordan de behandles af risikostyringssystemerne*
- *de eksisterende vigtigste kontrolsystemer til styring af betydningsfulde risici*
- *det eksisterende system til overvågning og revision.*

Alle betydningsfulde mangler, der registreres af systemet eller i selve systemet, skal meddeles sammen med de skridt, der er taget for at afhjælpe disse mangler.

8. Risikostyringens struktur og administration

8.1 Risikostyringspolitik

En virksomheds risikostyringspolitik skal vise virksomhedens holdning til og appetit på risiko og dens indstilling til risikostyring. Politikken skal endvidere fastlægge ansvaret for risikostyringen i hele virksomheden.

Desuden skal den tage hensyn til eventuelle juridiske krav til virksomhedspolitiske erklæringer, f.eks. vedrørende sikkerhed og sundhed på arbejdspladsen.

Til risikostyringsprocessen er der knyttet et integreret sæt værktøjer og teknikker, der kan bruges på de forskellige trin af forretningsprocessen. For at kunne arbejde effektivt kræver risikostyringsprocessen:

- *den administrerende direktørs og den øverste ledelses engagement*
- *fordeling af ansvar i virksomheden*
- *tildeling af passende ressourcer til uddannelse og udvikling af en øget risikobevidsthed hos alle interessenter.*

8.2 Bestyrelsens rolle

Bestyrelsen har ansvaret for at fastlægge virksomhedens strategiske retning og for at skabe det miljø og de strukturer, der gør, at risikostyringen kan arbejde effektivt.

Dette kan foregå gennem en gruppe med ledelsesbeføjelser, en komite uden ledelsesbeføjelser, en undersøgelseskomite eller en anden funktion, der passer til virksomhedens arbejdsmåde, og som er i stand til at optræde som 'sponsor' for risikostyringen.

Bestyrelsen skal som minimum overveje følgende, når virksomhedens system til intern kontrol evalueres:

- *natur og omfang af de risici med negative aspekter, virksomheden finder det acceptabelt at bære inden for dens særlige forretningsområde*
- *sandsynligheden for, at sådanne risici bliver til virkelighed*
- *hvordan uacceptable risici skal styres*
- *virksomhedens evne til at minimere sandsynligheden og påvirkningen af virksomheden*
- *omkostningerne og udbyttet ved den risiko- og kontrolaktivitet, der udføres*
- *risikostyringsprocessens effektivitet*
- *risiko som følge af beslutninger i bestyrelsen.*

8.3 Forretningsenhedernes rolle
Denne omfatter følgende:

- *forretningsenhederne har det primære ansvar for den daglige risikostyring*
- *forretningsenhedernes ledelse er ansvarlig for at fremme risikobevidstheden inden for deres område; skal introducere mål for risikostyring i deres forretningsenhed*
- *risikostyring skal regelmæssigt behandles på ledelsesmøder for at diskutere risikoeksponeringer og omprioritere arbejdet på baggrund af effektive risikoanalyser*
- *forretningsenhedens ledelse skal sikre, at risikostyring indarbejdes i den indledende fase af projekter og hele vejen igennem et givet projekts levetid.*

8.4 Risikostyringsfunktionens rolle
Afhængigt af virksomhedens størrelse kan risikostyringsfunktionen variere fra en enkelt risikoleder, en deltids risikodirektør, til en hel afdeling for risikostyring.

Risikostyringsfunktionens rolle skal omfatte følgende:

- *opstilling af politik og strategi for risikostyring*
- *primær leder af risikostyringen på strategisk og driftsmæssigt niveau*
- *opbygning af en risikobevidsthedskultur i virksomheden, herunder passende uddannelse*
- *etablering af en intern risikopolitik og risikostrukturer for forretningsenhederne*
- *etablering og revidering af processer til risikostyring*
- *koordinering af de forskellige funktionelle aktiviteter, der rådgiver om emner vedrørende risikostyring i virksomheden*
- *udvikling af risikoreaktionsprocesser, herunder nødplaner og programmer for fortsættelsen af forretningerne*
- *udarbejde rapporter om risiko til bestyrelsen og interessenterne.*

8.5 Den interne revisions rolle
Den interne revisions rolle varierer sandsynligvis fra virksomhed til virksomhed.

I praksis kan den interne revisions rolle inkludere nogle af eller alle følgende punkter:

- *fokusering af den interne revisions arbejde på betydelige risici, som identificeret af ledelsen, og revision af risikostyringsprocesserne i hele virksomheden*
- *skabe tillid og sikkerhed omkring risikostyringen*
- *sørge for aktiv støtte og engagement i risikostyringsprocessen*
- *forenkle risikoidentifikationen/-vurderingen og uddanne personalet i risikostyring og intern kontrol*
- *koordinering af risikorapportering til bestyrelsen, revisionsudvalget etc.*

Ved fastlæggelsen af den mest passende rolle for en bestemt organisation, skal den interne revision sikre, at de professionelle krav til uafhængighed og objektivitet overholdes.

8.6 Ressourcer og implementering
De ressourcer, der er nødvendige til implementeringen af virksomhedens risikostyringspolitik, skal tydeligt fremgå på hvert niveau af ledelsen og i hver enkelt forretningsenhed.

De, der er involveret i risikostyring, skal ud over andre driftsmæssige funktioner, de måtte have, klart have defineret deres roller i koordineringen af risikostyringspolitikken/-strategien. Den samme klare definition er desuden nødvendig for dem, der er involveret i revision og gennemgang af interne kontroller og forenkling af risikostyringsprocessen.

Risikostyring skal inkorporeres i hele virksomheden gennem strategi- og budgetprocessen. Den skal fremhæves ved oplæring og al anden uddannelse og udvikling samt i driftsprocesser som f.eks. udviklingsprojekter inden for produkt/service.

9. Overvågning og revision af risikostyringsprocessen

En effektiv risikostyring kræver en rapporterings- og revisionsstruktur for at sikre, at risiciene identificeres og vurderes effektivt, og at passende kontroller og reaktioner findes.

Der skal gennemføres regelmæssige revisioner af overensstemmelsen med politik og standarder, og standardernes effektivitet skal gennemgås for at identificere muligheder for forbedring. Man skal huske på, at virksomheder er dynamiske og arbejder i et dynamisk miljø. Forandringer i virksomheden og det miljø, den arbejder i, skal identificeres og systemerne ændres tilsvarende.

Overvågningsprocessen skal garantere, at der findes passende kontroller i forbindelse med virksomhedens aktiviteter, og at procedurerne forstås og følges. Ændringer i virksomheden og det miljø, den arbejder i, skal identificeres, og systemerne skal ændres tilsvarende.

Alle overvågnings- og revisionsprocesser skal fastslå, om:

- *de anvendte tiltag har givet det ønskede resultat*
- *de indførte procedurer og indsamlede oplysninger til grundlag for vurderingen har været egnede*
- *en forbedret viden ville have hjulpet med at træffe bedre beslutninger og identificere, hvad man kan lære til brug for vurderinger og styring af risici i fremtiden.*

10. Appendiks

Risikoidentifikationsteknikker - eksempler

- *Brainstorming*
- *Spørgeskemaer*
- *Undersøgelser af forretningerne, der ser på hver enkelt forretningsproces og beskriver både de interne processer og de eksterne faktorer, der kan påvirke disse processer*
- *Benchmarking inden for branchen*
- *Scenarieanalyse*
- *Workshops om risikovurdering*
- *Undersøgelse af hændelser*
- *Revision og kontrol*
- *HAZOP (Hazard & Operability Studies – Studier i risikomomenter og gennemførlighed).*

Metoder og teknikker til risikoanalyse - eksempler

Rsiko med positive aspekter

- *Markedsundersøgelse*
- *Bearbejdelse af kundeemner*
- *Testmarketing*
- *Forskning og udvikling*
- *Analyse af påvirkning af virksomheden.*

Begge

- *Opstilling af afhængighedsforhold*
- *SWOT-analyse (styrker, svagheder, muligheder, trusler)*
- *Hændelsesanalyse*
- *Planlægning for fortsættelse af forretningen*
- *BPEST-analyse (forretningsmæssigt, politisk, økonomisk, socialt, teknologisk)*
- *Opstilling af reelle valgmuligheder*
- *Beslutningstagning med risiko og usikkerhed*
- *Statistiske slutninger*
- *Middelværdi og spredning*
- *PESTLE (politisk, økonomisk, socialt, teknisk, juridisk, miljømæssigt).*

Risiko med negative aspekter

- *Trusselsanalyse*
- *Fejltræsanalyse*
- *FMEA (Failure Mode & Effect Analysis - Analyse over art og virkning af fejl).*

FOR LOCAL INFORMATION, PLEASE CONTACT THE OFFICE OF THE NATIONAL ASSOCIATION

AGERS - Asociacion Española de Gerencia de Riesgos y Seguros
Príncipe de Vergara, 86 - 1ª Esc., 2º Izda.– 28006 Madrid - SPAIN
Tel: + 34-91-562.84.25– Fax: + 34-91-561.54.05– Email: gerencia@agers.es

AIRMIC - The association of Insurance and Risk Managers
Lloyd's Avenue, 6 – London EC3N3AX - UK
Tel: + 44-207-480.76.10 – Fax: + 44-207-702.37.52 – Email: enquiries@airmic.co.uk
Web: www.airmic.com

AMRAE - Association pour le Management des Risques et des Assurances de l'Entreprise
Avenue Franklin Roosevelt, 9-11 – 75008 Paris - FRANCE
Tel: + 33-1-42.89.33.16 – Fax: + 33-1-42.89.33.14 – Email: amrae@amrae.asso.fr
Web: www.amrae.asso.fr

ANRA - Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali
Viale Coni Zugna, 53 – 20144 Milano - ITALY
Tel: + 39-02-58.10.33.00 – Fax: + 39-02-58.10.32.33 – Email: anra@betam.it – Web: www.anra.it

APOGERIS - Associação Portuguesa de Gestão de Riscos e Seguros
Avenida da Boavista, 1245, 3a Esq. – 4100-130 Porto – Portugal
Tel: (+351) 22 608 24 62 – Fax: (+351) 22 608 24 73 – E-mail: anfernandes@sonae.pt

BELRIM - Belgian Risk Management Association
Rue Gatti de Gamond, 254 – 1180 Bruxelles - BELGIUM
Tel: + 32-2-380.03.94 – Fax: + 32-2-370.34.93 – Email: info@belrim.com – Web: www.belrim.com

BfV - Bundesverband firmenverbundener Versicherungsvermittler und -Gesellschaften E. V.
Hattenbergstrasse 10, 55122 Mainz - D
Tel: + 49 - 6131 – 662226 - Fax: + 49 - 6131 – 662059 - Email: johannes.fischer@schott.com
Web: www.bfv-fvv.de

DARIM - Dansk Industris Risk Management Forening
DK-1787 Copenhagen – DENMARK
Tel: + 45-33-77.33.77 – Fax: + 45-33-77.33.00 – Email: bg@di.dk

DVS - Deutscher Versicherungs-Schutzverband e.V.
Breite Strasse 98 - D 53111 Bonn - Germany
Tel: + 49-228-98.22.30 - Fax: + 49-228-63.16.51- Email: info@dvs-schutzverband.de
Web: www.dvs-schutzverband.de

NARIM - Nederlandse Associatie van Risk en Insurance Managers
Postbus 65707 – 2506 EA Den Haag – THE NETHERLANDS
Tel: + 31-70-345.74.26 – Fax: + 31-70-427.32.63 – Email: info@narim.com – Web: www.narim.com

RUSRISK - Russian Risk Management Society
Address Expert Institute, Staraya Ploshchad 10/4, Moscow, 103070, Russia
Phone: +7 (095) 748-4313 - Fax: +7 (095) 748-4316 - Email: sh.tatiana@relcom

SIRM - Swiss Association of Insurance and Risk Managers
Route du Jura, 37- Case Postale, 74 – 1706 Fribourg - SWITZERLAND
Tel: + 41-26-347.12.20 – Fax: + 41-26-347.12.39 – Email: sirm@cfcis.ch – Web: www.sirm.ch

SWERMA - Swedish Risk Management Association
Gränsvägen 15 ˆ SE-135 47 Tyresö - Sweden
Phone: +468 742 13 07 - Fax: + 468 798 83 11- E-mail: lani.rcrd@swipnet.se

ALARM - The National Forum for Risk Management in the Public Sector
Queens Drive, Exmouth - Devon, EX8 2AY
Tel: 01395 223399 - Fax: 01395 223304 - Email admin@alarm.uk.com - www.alarm-uk.com

IRM - The Institute of Risk Management
6 Lloyd's Avenue - London EC3N 3AX
Tel: 020 7709 9808 - Facsimile 020 7709 0716 - Email enquiries@theIRM.org - www.theirm.org

FOR MORE INFORMATION ABOUT FERMA

FERMA - RUE DE LA PRESSE 4
1000 BRUSSELS - BELGIUM
PHONE: + 32 2 227.11.44
FAX: + 32 2 227.11.48
EMAIL: info@ferma-asso.org
WEB: www.ferma-asso.org