

**Enterprise Risk Management integreret ramme
Resumé, september 2004**

Ophavsretligt beskyttet © 2004 af Committee of Sponsoring Organizations of the Treadway Commission. Alle rettigheder reserveret.

De er hermed berettiget til at downloade og distribuere et ubegrænset antal eksemplarer af dette resumé, som forekommer i et PDF-dokument. Resuméet må kun benyttes til personligt eller internt brug i Deres virksomhed.

Det er ikke tilladt at fjerne varemærker eller ophavsretlige symboler som ©, eller ® fra det downloadede eksemplar. I fald resuméet skal bruges til distribution i kommercielt øjemed, skal De anmode om ophavsretlig tilladelse. Dette skal ske som følger:

Den nuværende procedure for anmodning om AICPA-tilladelse er først og fremmest at besøge vores hjemmeside på adressen www.aicpa.org og derefter klikke på linket [privacy policies and copyright information](#), som findes i bunden af siden.

Derefter skal De klikke på det efterfølgende menu-link med titlen COPYRIGHT PERMISSION REQUEST FORM, udfylde alle relevante dele af online-skemaet og klikke på SUBMIT-knappen i bunden af siden. Der vil blive opkrævet en afgift for de anmodede reproduktionsprivilegier.

Forord

For mere end 10 år siden udgav the Committee of Sponsoring Organizations of the Treadway Commission (COSO) rapporten *Internal Control Integrated Framework* med henblik på at hjælpe virksomheder og andre enheder til at kunne overskue og forbedre deres interne kontrolsystemer. Rapportens ramme er lige siden blevet omdannet til politikker, regler og regulationer og benyttet af tusindvis af virksomheder til bedre at kunne kontrollere deres aktiviteter i forsøget på at opnå deres mål.

Der har i de seneste år været en forstærket interesse for og fokus på risk management, og det er blevet mere og mere indlysende, at der er behov for en bred ramme, via hvilken man effektivt kan identificere, vurdere og håndtere risici. I 2001 iværksatte COSO et projekt, hvor de bad PriceWaterhouseCoopers om at udvikle en ramme, som virksomhedsledelser på en let måde kunne anvende til at evaluere og forbedre deres organisations enterprise risk management.

Perioden, i hvilken rammen blev udviklet, var mærket af en række store erhvervsskandaler og fiaskoer, hvor investorer, virksomhedspersonale og andre interessenter led kolossale tab. Efterfølgende var der behov for forøget corporate governance og risk management med nye love, reglementer og standarder for listeføring. Behovet for en enterprise risk management-ramme, der kunne forsyne virksomhederne med nøgleprincipper og koncepter, et fælles sprog samt klar vejledning og rådgivning, blev endnu større. COSO er af den opfattelse, at *Enterprise Risk Management Integrated Framework* opfylder dette behov og forventer, at dokumentet vil blive bredt accepteret af virksomheder og andre organisationer, samt især ejere og interessenter.

Som følge af udviklingen findes i USA blandt andet Sarbanes-Oxley-loven fra 2002, og lignende lovgivning er blevet vedtaget eller overvejet i andre lande. Denne lov opfylder et gammelt krav til offentlige virksomheder om at have interne kontrolsystemer og påbyder ledelsen at bekræfte - og den uafhængige forfatter at attestere - effektiviteten af disse systemer. *Intern Kontrol Integrated Framework* fortsætter med at stå tidens test, og tjener som en bredt accepteret standard til at efterleve disse rapporteringskrav.

Rapporten *Enterprise Risk Management Integrated Framework* omhandler intern kontrol og indeholder et stærkere og mere omfattende fokus på bredere emner inden for enterprise risk management. Det er ikke er meningen, at rammen skal erstatte den interne kontrol-ramme men snarere inkludere den. Virksomheder kan således beslutte at benytte denne enterprise risk management-ramme både med henblik på at opfylde deres behov for intern kontrol og på at arbejde sig hen imod en mere omfattende risk management-proces.

Nogle af de mest kritiske udfordringer vil for ledelsen være at fastslå, hvor mange risici virksomheden kan udsættes for og acceptere i dens stræben efter at skabe værdi. Denne rapport vil ruste dem bedre til at møde denne udfordring.

John J. Flaherty
Formand, COSO

Tony Maki
Formand, COSO Rådgivningsråd

Resumé

Enterprise risk management bygger på en grundlæggende forudsætning om, at enhver virksomhed har til formål at tilføre dens interessenter værdi. Alle virksomheder står over for usikkerhed, og ledelsens udfordring er derfor at afgøre, hvor meget usikkerhed den vil acceptere i dens stræben efter at øge interessentværdien. Usikkerhed repræsenterer både risici og muligheder, og begge aspekter har potentiale til henholdsvis at svække eller forøge virksomhedens værdi. Med enterprise risk management har ledelsen mulighed for på en effektiv måde at håndtere usikkerhed forbundet med risici og muligheder og forbedre evnen til værdiforøgelse.

Den største værdiforøgelse opnås, når ledelsen udarbejder strategier og mål for, hvordan den skaber en optimal balance mellem vækst, målopfyldelse og mulige risici. Desuden forøges værdien, når ledelsen på en effektiv og virkningsfuld måde udnytter ressourcer i dens bestræbelser på at opnå virksomhedens mål. Enterprise risk management gør det muligt at:

- *Skabe sammenhæng mellem risikoappetit og strategi* Ledelsen vurderer virksomhedens risikoappetit ved at evaluere strategiske alternativer, opstille mål og udvikle mekanismer til at håndtere mulige risici.
- *Understøtte beslutninger vedrørende risikoreaktion* Enterprise risk management gør det muligt at identificere og vælge mellem alternative risikoreaktioner at undgå, reducere, dele og acceptere risici.
- *Reducere operationelle overraskelser og tab* Virksomheder opnår en større mulighed for at identificere potentielle begivenheder og reagere herpå. Dermed kan de reducere overraskelser og komme efterfølgende udgifter eller tab i forkøbet.
- *Identificere og håndtere mangesidige og tværorganisatoriske risici* Enhver virksomhed står over for myriader af risici, der har indvirkning på forskellige dele af organisationen. Enterprise risk management gør det lettere at reagere effektivt på indbyrdes forbundne omstændigheder.
- *Gribe mulighederne* ved at overveje et bredt spektrum af potentielle begivenheder er ledelsen i stand til at identificere og udnytte muligheder på en proaktiv måde.
- *Forbedre spredning af kapital* Ved at tilegne sig håndfast risikoinformation kan ledelsen effektivt fastsætte det overordnede kapitalbehov og forøge kapitalfordelingen

Mulighederne forbundet med enterprise risk management hjælper ledelsen til at gennemføre virksomhedens drift, opnå dens rentabilitetsmål og afværge ressourcestab. Enterprise risk management hjælper med at sikre effektiv indberetning og overensstemmelse med love og regulativer og hjælper virksomheden med at afværge dårlig omtale og efterfølgende konsekvenser heraf. For at opsummere kan virksomheder, der prioriterer enterprise risk management, undgå faldgruber og overraskelser og i stedet blive hjulpet på rette vej.

Begivenheder risici og muligheder

Begivenheder kan have en negativ og en positiv effekt - eller begge dele. Begivenheder med negativ effekt repræsenterer risici, som kan forhindre værdiskabelse eller mindske eksisterende værdi. Begivenheder med positiv effekt kan udligne negative effekter eller repræsentere muligheder. Muligheder øger chancen for, at en begivenhed får en positiv indflydelse på opfyldelse af mål, der støtter værdiskabelse eller bevarelse. Ledelsen kan inkludere muligheder i dens strategier eller målsætningsprocesser og på den måde udarbejde en plan for udnyttelse af muligheder.

Definition på enterprise risk management

Enterprise risk management vedrører risici og muligheder, som har indflydelse på værdiskabelse og bevarelse, og enterprise risk management bliver defineret som følger:

Enterprise risk management er en proces, som en virksomheds bestyrelse, ledelse og andet personale bruger til at udvikle strategier på tværs af virksomheden og identificere potentielle begivenheder, som kan have indflydelse på virksomheden. Virksomheder anvender enterprise risk management til at håndtere risikoappetit og til på en fornuftig måde at forsikre, at virksomhedens mål bliver opfyldt.

Definitionen afspejler visse fundamentale begreber. Enterprise risk management er:

- En vedvarende proces, der strømmer gennem en virksomhed
- Benyttet af personer på alle niveauer af en organisation
- Anvendt til strategiudvikling
- Anvendt på tværs af virksomheden - på ethvert niveau og i enhver enhed - og inkluderer, at virksomheden definerer sin risikoportefølje
- Skabt til at identificere potentielle begivenheder der, hvis de opstår, kan påvirke virksomheden og til at håndtere risici ud fra virksomhedens risikoappetit
- Et redskab, der forsyner en virksomheds ledelse og bestyrelse med en vis sikkerhed
- Skabt til målopfyldelse i én eller flere separate men overlappende kategorier

Denne definition er forholdsvis bred. Den indeholder nøglebegreber, der er fundamentale for, hvordan virksomheder og andre organisationer håndterer risici, og den forsyner dem med et grundlag for, hvordan de bruger enterprise risk management på tværs af organisationer, industrier og sektorer. Definitionen fokuserer direkte på målopfyldelse, der er opstillet af en bestemt enhed, ligesom den danner grundlag for, hvordan man kan definere effektiviteten af enterprise risk management.

Målopfyldelse

I forbindelse med en virksomheds fastsatte mission eller vision opstiller ledelsen strategiske mål, udvælger strategier og sætter andre mål, der berører virksomheden. Nedenstående enterprise risk management-ramme, der er inddelt i fire kategorier, gør det muligt for en virksomhed at opfylde dens mål:

- *Strategi* overordnede mål, der støtter op om missionen
- *Drift* effektiv brug af ressourcer
- *Rapportering* rapporteringens pålidelighed
- *Overensstemmelse* overensstemmelse med gældende love og regulativer

Denne kategorisering af mål gør det muligt at fokusere på separate aspekter af enterprise risk management. Disse forskellige men dog alligevel overlappende kategorier et bestemt mål

kan høre under mere end en kategori - henvender sig til forskellige enheders behov og kan høre under forskellige lederes ansvarsområder. Denne kategorisering gør det ligeledes muligt at skelne mellem, hvad der kan forventes af de enkelte målkategorier. Kategorien ressourcebeskyttelse, som bruges af nogle virksomheder, er også beskrevet.

I forbindelse med en pålidelig rapportering og overensstemmelse med love og regulativer hører mål under virksomhedens kontrol. Og enterprise risk management kan hjælpe en virksomhed med en fornuftig målopfyldelse. Dog afhænger opfyldelse af strategiske og operationelle mål af eksterne begivenheder, og disse faktorer er derfor ikke udelukkende underlagt virksomhedens kontrol. Men en virksomhed, der anvender enterprise risk management, kan være sikker på, at ledelsen - og i overordnet forstand også bestyrelsen - i rette tid bliver gjort opmærksom på i hvilket omfang virksomheden styrer mod en opfyldelse af dens strategiske og operationelle mål.

Elementerne i Enterprise Risk Management

Enterprise risk management består af otte elementer, der er indbyrdes forbundet. Disse elementer er opstået via den måde, hvorpå en ledelse styrer en virksomhed, og elementerne er en del af ledelsesprocessen. Disse otte elementer udgør:

- *Internt miljø* Det interne miljø omfatter omgangstonen i en organisation, og det danner basis for, hvordan en virksomheds medarbejdere opfatter risici. Det interne miljø inkluderer risk management-filosofi og -risikoappetit, retskaffenhed, etiske værdier samt miljøet, i hvilket virksomheden opererer.
- *Målsætning* En virksomhed skal have opstillet en række mål, førend ledelsen kan identificere begivenheder, som kan påvirke disse mål. Enterprise risk management sikrer, at ledelsen er i stand til at opstille mål, og at de valgte mål støtter og bakker op om virksomhedens mission, samt at de er i overensstemmelse med virksomhedens risikoappetit.
- *Identificering af begivenheder* Interne og eksterne begivenheder, som har indflydelse på en virksomheds målopfyldelse, skal være identificeret og begivenhederne skal være opdelt i risici og muligheder. Muligheder ledes tilbage til processen vedrørende ledelsens udarbejdelse af strategier og opstilling af mål.
- *Risikovurdering* Risici bliver analyseret og deres sandsynlighed og konsekvenser vurderes. Dette danner basis for en beslutning om, hvordan de skal håndteres. Risici bliver vurderet ud fra et fast og fyldestgørende grundlag.
- *Risikoreaktion* Ledelsen vælger, hvordan den vil reagere på risici - undgå, acceptere, reducere eller dele risiciene - og udvikler et handlesæt til hvordan den vil forene risici med virksomhedens risikotolerance og -appetit.
- *Kontrolaktiviteter* Der bliver udarbejdet og iværksat politikker og procedurer til at sikre en effektiv risikoreaktion.
- *Information og kommunikation* Relevant information bliver identificeret, kortlagt og kommunikeret ud på en måde og med en tidsramme, som gør det muligt for personalet at udøve deres ansvar. Effektiv kommunikation bliver desuden en realitet på kryds og tværs af virksomheden.
- *Overvågning* Enterprise risk management bliver i sin helhed overvåget, og der laves modifikationer, når det er nødvendigt. Overvågning bliver gennemført via løbende aktiviteter fra ledelsens side, separate evalueringer eller begge dele.

Enterprise risk management er ikke en bestemt fortløbende proces, hvor et element med sikkerhed påvirker det næste element. Det er tværtimod en gentagelsesproces, som kan gå i mange retninger, og som er præget af, at alle elementer har indflydelse på hinanden.

Forbindelse mellem mål og komponenter

Der er en direkte forbindelse mellem mål, som udgør det, som virksomheden stræber efter at nå, og enterprise risk management, som repræsenterer, hvad virksomheden behøver, for at kunne opfylde sine mål. Forbindelsen er skildret i en tredimensional matrix, der har form af en kubus.

De fire målkategorier strategi, drift, beretning og overensstemmelse er repræsenteret i de vertikale kolonner, de otte komponenter er repræsenteret i horisontale rækker og virksomhedens enheder er repræsenteret i den tredje dimension. Denne skildring viser evnen til at fokusere på alt ved en virksomheds enterprise risk management eller dens målkategorier, komponenter, enheder eller dele deraf.

Effektivitet

At fastslå om en virksomheds enterprise risk management er effektiv er en bedømmelse, der afhænger af en vurdering af, hvorvidt de otte komponenter er til stede og fungerer effektivt. Komponenterne er således alle kriterier, der skal indgå i effektiv enterprise risk management. En forudsætning for, at komponenterne er til stede og fungerer rigtigt, er, at der ikke er nogle materielle svagheder. Desuden skal risici indgå som en del af virksomhedens risikoappetit.

Bestyrelsen og ledelsen kan være sikker på at have forstået, i hvilket omfang virksomhedens strategiske og operationelle mål opnås, når enterprise risk management indgår effektivt i hver af de fire målkategorier, når virksomhedens indberetning er pålidelig, og når gældende love og reguleringer bliver efterlevet.

De otte komponenter fungerer ikke på samme måde i enhver virksomhed. Anvendelsen i for eksempel små og mellemstore virksomheder kan være mindre formel og mindre struktureret. Ikke desto mindre kan små virksomheder stadig have effektiv enterprise risk management, så længe hver komponent er til stede og fungerer rigtigt.

Begrænsninger

Selvom enterprise risk management giver virksomheden vigtige fordele, eksisterer der også begrænsninger. I forlængelse af de ovenfor diskuterede faktorer kan begrænsninger opstå som følge af, at menneskelig dømmekraft i forbindelse med beslutningstagning kan være mangelfuld. Desuden er virksomheden, når den tager beslutninger om risikohåndtering og etablering af kontrolforanstaltninger, nødt til at tage relative omkostninger og udbytte i betragtning. Ligeledes kan sammenbrud opstå som følge af menneskelige fejl - såsom simple fejltagelser eller misforståelser - og kontrollen kan blive hindret af sammenstød mellem to eller flere personer. Endelig kan ledelsen vælge at sætte sig ud over enterprise risk management-beslutninger. Disse begrænsninger afskærer en bestyrelse og en ledelse fra at have en total forsikring om, at virksomhedens mål kan opnås.

Omfatter intern kontrol

Intern kontrol er en integreret del af enterprise risk management. Denne enterprise risk management-ramme omfatter intern kontrol, som former en mere bred begrebsdannelse og et redskab for ledelsen. Intern kontrol er defineret og beskrevet i rapporten *Internal Control Integrated Framework*. Da denne ramme har været udsat for tidens tests og indeholder

grundlaget for eksisterende regler, reguleringer og love, forbliver dette dokument definitionen på og rammen om intern kontrol. Det er kun dele af teksten *Internal Control Integrated Framework*, der er gengivet i rammen. Dette resumé refererer dog til rammen i sin helhed.

Roller og ansvar

Alle personer i en virksomhed har et vist ansvar for enterprise risk management. Den øverste leder er i sidste instans ansvarlig og skal påtage sig dette ansvar. Andre ledere støtter virksomhedens enterprise risk management-filosofi, fremhjælper overensstemmelse med virksomhedens risikoappetit og håndterer risici inden for deres respektive ansvarsområder i overensstemmelse med risikotolerance. Det er som regel blandt andre risikoledere, økonomiledere og interne revisorer, der har ansvaret for at yde den største støtte. Virksomhedens resterende personale er ansvarlig for at udføre enterprise risk management i overensstemmelse med etablerede direktiver og protokoller. Bestyrelsen har det nødvendige opsyn med enterprise risk management og er bevidst om og enig i virksomhedens risikoappetit. En række eksterne interessenter, så som kunder, forhandlere, forretningspartnere, eksterne revisorer, regulatorer og finansielle analytikere, forsyner ofte virksomheden med nyttige oplysninger til at udføre enterprise risk management, men de er hverken ansvarlige for effektiviteten eller en del af virksomhedens enterprise risk management.

Rapports disposition

Denne rapport falder i to dele. Den første del indeholder selve rammen og dette resumé. Rammen definerer enterprise risk management og beskriver principper og koncepter, der kan forsyne ledelsen på alle niveauer af erhvervsvirksomheder og andre organisationer med vejledninger til at evaluere og forøge effektiviteten af enterprise risk management. Resuméet udgør en omfattende oversigt, der henvender sig til udøvende ledere, andre seniorledere, bestyrelsesmedlemmer og regulatorer. Den anden del, *Application Techniques*, giver tekniske illustrationer, der kan være nyttige, når man skal bruge elementer af rammen.

Anvendelsen af denne rapport

De handlinger, som kan udledes af denne rapport, afhænger af de involverede parter position og rolle.

- *Bestyrelsen* - Bestyrelsen bør diskutere tilstanden af virksomhedens enterprise risk management med seniorledelsen og bidrage med det nødvendige opsyn. Bestyrelsen bør forsikre, at den bliver underrettet om de mest markante risici, ledelsens handlinger og dennes sikring af effektiv enterprise risk management. Bestyrelsen bør overveje at søge oplysninger fra interne revisorer, eksterne revisorer, med flere.
- *Seniorledelsen* Denne rapport foreslår, at den øverste leder vurderer organisationens evner inden for enterprise risk management. Den øverste leder skal på én gang samle lederne af virksomhedens enheder samt det vigtige funktionspersonel og sammen foretage en første vurdering af virksomhedens evner og effektivitet hvad angår enterprise risk management. En første vurdering bør, lige meget hvordan den falder ud, afgøre, hvad der er behov for, og hvordan man kan gå videre med en bredere og mere dybtgående evaluering.
- *Andet virksomhedspersonale* Ledere og andet personel bør overveje, hvordan de på baggrund af denne rapport skal håndtere deres ansvar, og de bør sammen med seniorpersonel diskutere deres idéer omkring styrkelsen af enterprise risk management. Interne revisorer bør overveje omfanget af deres fokus på enterprise risk management.
- *Regulatorer* Denne struktur kan give et delt syn på enterprise risk management, der inkluderer, hvad enterprise risk management kan gøre, og hvad dets begrænsninger er. Regulatorer bør henvise til denne struktur, når de opstiller forventninger til virksomheder,

som de fører tilsyn med. Dette gælder hvad enten det drejer sig om regler, vejledninger eller udførelse af undersøgelser.

- *Professionelle organisationer* Regelskabende og andre professionelle organisationer, der skaber retningslinier for finansiel ledelse, revision og andre lignende områder, bør overveje deres standarder og vejledning i lyset af denne struktur. I det omfang hvor uensartethed i koncepter og terminologi bliver mindre, har det været til gavn for alle parter.
- *Undervisere* Denne ramme kan tjene som objekt for akademisk forskning og analyse med det formål at afgøre, hvor fremtidige forbedringer kan foretages. Med formodningen om, at denne rapport bliver accepteret som en fælles forståelsesramme, vil rapportens koncepter og termer også kunne blive en del af universitære studieordninger.

Med dette grundlag for gensidig forståelse kan alle parter i fremtiden være i stand til at tale et fælles sprog og kommunikere på en mere effektiv måde. Udøvende erhvervsledere vil være i stand til at vurdere deres virksomheds enterprise risk management-proces og holde den op mod en standard. De kan således styrke denne proces og styre deres virksomhed mod fastsatte mål. Fremtidig forskning kan vægtes mod et etableret grundlag. Lovgivere og regulatorer vil kunne opnå øget forståelse for enterprise risk management, og det inkluderer forståelse for dets fordele og begrænsninger. Disse fordele bliver realiseret, når alle parter anvender en fælles ramme for enterprise risk management.