

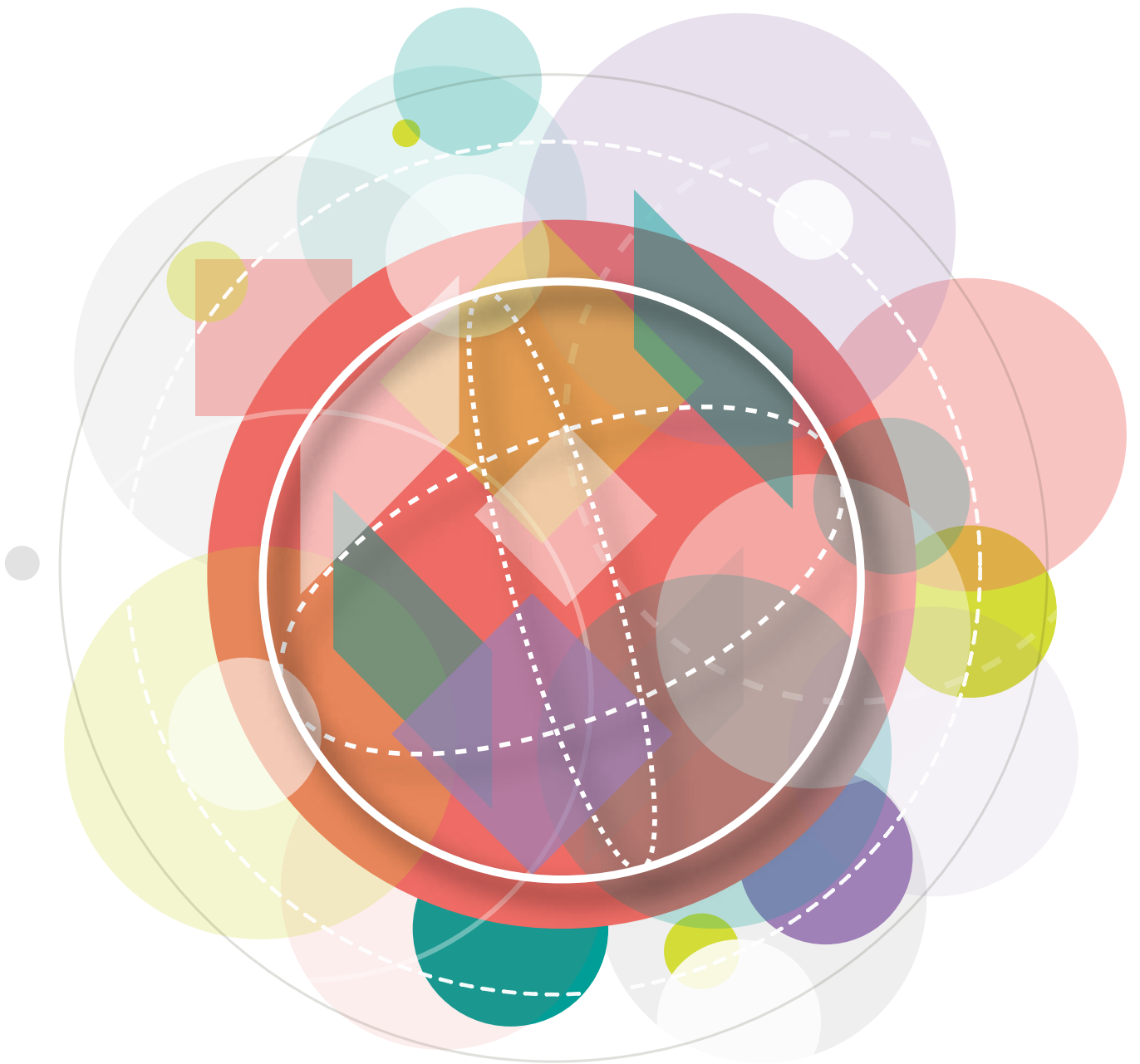


Committee of Sponsoring Organizations of the Treadway Commission

Helhetlig Risikostyring

Integrering med strategi og måloppnåelse

Sammendrag



Juni 2017

Dette prosjektet ble bestilt av the Committee of Sponsoring Organizations of the Treadway Commission (COSO), som er dedikert til å gi tankelederskap gjennom utvikling av helhetlige rammeverk og veiledning om intern kontroll, helhetlig risikostyring og mislighetsforebygging. Disse er utformet for å forbedre organisasjoners måloppnåelse og tilsyn med virksomheten samt for å redusere omfanget av misligheter i organisasjoner. COSO er et initiativ av private aktører, støttet og finansiert av:

- American Accounting Association
- American Institute of Certified Public Accountants
- Financial Executives International
- Institute of Management Accountants
- The Institute of Internal Auditors

Om den norske oversettelsen:

IIA Norges Fag- og metodekomite har oversatt dette sammendraget til norsk våren 2018. Enkelte steder er setninger omskrevet for å tilpasses norsk språkdrakt, uten at innholdet er endret. Der- som det skulle være avvik mellom den norske versjonen av sammendraget og den engelske, vil den originale versjonen være overordnet.

IIA Norge retter en stor takk til følgende medlemmer i Fag- og metodekomiteen:

Tor Solbjørg, Helse Nord RHF
Trygve Sørli, Trygve Sørli Services EPF
Rune Johannessen, Nordea Bank Norge ASA
Martin W. Stevens, Gjensidige Forsikring ASA
Cecilie Thorberg, Universitetet i Oslo

Copyright © 2017 by Committee of Sponsoring Organizations of the Treadway Commission, (“COSO”) strictly reserved. No parts of this material may be reproduced in any form without the written permission of COSO.

Permission has been obtained from the copyright holder, COSO, to publish this translation, which is the same in all material respects, as the original unless approved as changed. No parts of this document may be reproduced, stored in any retrieval system, or transmitted in any form, or by any means electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of COSO.

Copyright © 2017 by Committee of Sponsoring Organizations of the Treadway Commission, (“COSO”) - alle rettigheter reservert. Ingen del av denne publikasjonen kan reproduseres uten skriftlig tillatelse fra COSO.

Rettigheter til å publisere oversettelsen er tildelt fra rettighetshaver, COSO. Oversettelsen sam- svarer i all hovedsak med originalen, men dersom avvik skulle forekomme vil den engelske tek- sten være overordnet den norske. Ingen deler av dette dokumentet kan gjengis eller kopieres uten skriftlig tillatelse fra COSO.

Forord

I tråd med sitt overordnede formål bestilte og publiserte COSO-styret i 2004 *Helhetlig Risikostyring – Et integrert rammeverk*. I løpet av det siste tiåret har rammeverket fått bred aksept og anvendelse av organisasjoner i deres arbeid med å styre risiko. I denne perioden har imidlertid også risikokompleksiteten endret seg, og nye risikoer har kommet til. Både styret og ledelse har styrket bevisstheten om den helhetlige risikostyringen og tilsynet med denne, samtidig som de etterspør forbedret risikorapportering. Denne oppdateringen av 2004-publikasjonen tar hensyn til denne utviklingen av helhetlig risikostyring og nødvendigheten av at organisasjonene forbedrer sin tilnærming til risikostyring for å møte utfordringene ved omgivelser i stadig endring.

Det oppdaterte rammeverket, som nå heter *Helhetlig Risikostyring - Integrering med strategi og måloppnåelse*, understreker viktigheten av å vurdere risiko både i strategisettingsprosessen og i arbeidet med å fremme måloppnåelse. Den første delen av den oppdaterte utgaven gir et overblikk over nåværende risikostyringskonsepter og slike konsepter under utvikling, samt bruken av helhetlig risikostyring. Den andre delen av rammeverket er delt inn i fem lettfattelige komponenter som ivaretar ulike perspektiv og driftsstrukturer og bidrar til forbedring av strategi- og beslutningsprosesser. Kort sagt, så innebærer denne oppdateringen:

- Større forståelse for verdien av helhetlig risikostyring ved utvikling og implementering av strategi.
- Klarere sammenheng mellom måloppnåelse og helhetlig risikostyring, som bidrar til bedre fastsettelse av mål og gir bedre forståelse for risikoers effekt på måloppnåelsen.
- At forventninger om virksomhetsstyring og tilsyn blir innfridd.
- Økt erkjennelse av globaliseringen av markeder og driftsprosesser samt behovet for å anvende en felles, men tilpasset, tilnærming på tvers av geografiske områder.
- Nye måter å betrakte risiko på knyttet til fastsettelse og oppnåelse av mål, på bakgrunn av økt forretningskompleksitet.
- Utvidet rapportering for å imøtekomme interessentenes forventninger om større åpenhet.
- At den teknologiske utviklingen og økt tilgang til data og analyser benyttes som støtte for beslutningstaking.
- Presentasjon av sentrale definisjoner, komponenter og prinsipper for alle ledelsesnivåer som er involvert i å utforme, iverksette og utøve helhetlig risikostyring.

Leserne kan også ha nytte av å sette seg inn i en annen publikasjon, *COSOs Intern Kontroll – Et integrert rammeverk*. Selv om de to rammeverkene har fellestrekk er det viktig å være oppmerksom på at dette er to publikasjoner med hvert sitt fokus; den ene erstatter ikke den andre. De henger imidlertid sammen. *Intern Kontroll – Et integrert rammeverk* handler om intern kontroll, som det delvis henvises til i denne oppdaterte publikasjonen. Det tidligere rammeverket er dermed fortsatt relevant og velegnet for å utforme, iverksette, utøve og evaluere intern kontroll og for å sikre konsistent rapportering.

COSOs styre vil gjerne takke PwC for deres betydelige bidrag i arbeidet med *Helhetlig Risikostyring - Integrering med strategi og måloppnåelse*. PwCs koordinering og vurdering av høringsinnspill fra mange interessenter, og deres gode innsikt, var avgjørende for å sikre at de sterke sidene i den opprinnelige publikasjonen er beholdt og at innholdet er tydeliggjort eller utvidet der dette har vært nødvendig. COSOs styre og PwC takker også "the Advisory Council and Observers" for deres bidrag med gjennomgang og tilbakemeldinger.



Robert B. Hirth Jr.
COSO Chair



Dennis L. Chesley
PwC Project Lead Partner and Global
and APA Risk and Regulatory Leader

Committee of Sponsoring Organizations of the Treadway Commission

Styremedlemmer

Robert B. Hirth Jr.
COSO Chair

Richard F. Chambers
The Institute of Internal Auditors

Mitchell A. Danaher
Financial Executives International

Charles E. Landes
*American Institute of Certified Public
Accountants*

Douglas F. Prawitt
American Accounting Association

Sandra Richtermeyer
*Institute of Management
Accountants*

PwC—Author

Hovedbidragsyttere

Miles E.A. Everson
*Engagement Leader and Global
and Asia, Pacific, and Americas
(APA) Advisory Leader
New York, USA*

Dennis L. Chesley
*Project Lead Partner and Global
and APA Risk and Regulatory
Leader
Washington DC, USA*

Frank J. Martens
*Project Lead Director and Global
Risk Framework and Methodology
Leader
British Columbia, Canada*

Matthew Bagin
*Director
Washington DC, USA*

Hélène Katz
*Director
New York, USA*

Katie T. Sylvis
*Director
Washington DC, USA*

Sallie Jo Perraglia
*Manager
New York, USA*

Kathleen Crader Zelnik
*Manager
Washington DC, USA*

Maria Grimshaw
*Senior Associate
New York, USA*

Det endrende risikolandskapet

Vår forståelse av hva risiko er ligger i kjernen av vår moderne økonomi. Alle valg vi gjør for å nå målene våre har sine risikoer. Å håndtere risiko når disse valgene tas er en del av beslutningsprosessen, enten det gjelder de daglige driftsmessige beslutninger eller de grunnleggende avveiningene i styrerommet.

Når vi forsøker å optimalisere konsekvensen av en rekke mulige utfall er beslutningene sjelden binære, med ett riktig og ett galt svar. Derfor kan helhetlig risikostyring kalles både en kunst og en vitenskap, og når risiko vurderes ved formuleringen av en organisasjons strategi og målsettinger, vil helhetlig risikostyring bidra til å optimalisere utfallet.

Vår forståelse av risiko og vår praktisering av helhetlig risikostyring har blitt mye bedre de siste tiårene, men den tillatte feilmarginen er synkende. "The World Economic Forum" har omtalt den "økende volatiliteten, kompleksiteten og usikkerheten i verden."¹ Det er et fenomen vi alle er kjent med. Organisasjoner møter utfordringer som påvirker både pålitelighet, relevans og tillit. Interessentene er mer engasjert i dag og forventer mer åpenhet og ansvarlighet rundt risikohåndteringen, samtidig som de kritisk vurderer ledelsens evne til å utnytte muligheter. Selv suksess kan medføre risiko for uønskede utfall, som for eksempel risikoen for ikke å kunne oppfylle uventet høy etterspørsel eller opprettholde forventet fremdrift i forretningsutviklingen.

Organisasjonene må bli dyktigere til å tilpasse seg endringer. De må tenke strategisk på hvordan de skal håndtere den økende volatiliteten, kompleksiteten og usikkerheten i verden. Spesielt gjelder dette på toppledernivået i organisasjonen og i styrerommet, hvor konsekvensene av beslutningene er størst.

Helhetlig risikostyring - Integrering med strategi og måloppnåelse er et rammeverk for styret og ledelsen i organisasjoner av alle størrelser. Det bygger på hvordan risikostyringen gjennomføres i ordinær drift i dag. Videre viser det hvordan det å integrere helhetlig risikostyringspraksis i hele organisasjonen bidrar til å øke vekst og forbedre måloppnåelse. Det inneholder også prinsipper som kan benyttes, fra strategisk beslutningsprosess og helt frem til måloppnåelse.

Nedenfor gjør vi rede for hvorfor det er fornuftig for ledelse og styre å bruke det helhetlige risikostyringsrammeverket², hva organisasjoner har oppnådd ved å ta i bruk helhetlig risikostyring, og hvilke ytterligere fordeler som kan realiseres gjennom fortsatt bruk. Vi avslutter så med en titt inn i fremtiden.

Helhetlig risikostyring – veiledning for ledelsen

Ledelsen har det overordnede ansvaret for å styre foretakets risiko, men det er viktig at ledelsen går videre og inviterer til dialog med styret og interessentene om å bruke helhetlig risikostyring til å oppnå konkurransemessige fortrinn. Da starter man med å benytte helhetlig risikostyring som element ved fastsettelse og tilpassing av strategien.

Gjennom denne prosessen vil ledelsen først og fremst oppnå bedre forståelse for hvordan en eksplisitt vurdering av risiko kan påvirke valg av strategi. Helhetlig risikostyring bidrar til bedre ledelsesdialog ved å gi perspektiver på strategiske styrker og svakheter i takt med endrede rammebetingelser, og ved å gi innsikt i hvor godt en strategi er tilpasset organisasjonens formål og visjon. Ledelsen kan da føle seg tryggere på at alternative strategier er undersøkt, og at innspill fra de i organisasjonen som skal implementere den fastsatte strategien, er vurdert.

¹ The Global Risks Report 2016, 11th edition, World Economic Forum (2016).

² Rammeverket bruker begrepet "styret". Med styret menes det styrende organet, det vil si de som er ansvarlig for virksomhetsstyringen. Dette kan for eksempel være styret, supervisory board, board of trustees, general partners, direktøren i et direktorat, eller eiere.

Når strategien er fastsatt er helhetlig risikostyring en effektiv og hensiktsmessig metode som ledelsen kan bruke for å ivareta sin rolle, i visshet om at organisasjonen er tilpasset de risikoer som kan påvirke strategien og at disse styres på en god måte. Bruk av helhetlig risikostyring bidrar til å skape tillit og gi interessentene trygghet i nåværende situasjon. Dette krever større oppmerksomhet enn noen gang tidligere om hvordan risiko aktivt identifiseres og håndteres.

Helhetlig risikostyring – veiledning for styret

Ethvert styre har en tilsynsrolle som skal bidra til å støtte verdiskapningen i enheten og hindre verdiforringelse. Tradisjonelt har helhetlig risikostyring vært til god støtte for styret. Nå forventes det i økende grad at styrene fører tilsyn med og nyttiggjør seg den helhetlige risikostyringen.

Rammeverket gir styret viktige momenter å vurdere og ta hensyn til når de skal definere og ivareta sitt ansvar for å føre tilsyn med risiko. Dette inkluderer virksomhetsstyring og kultur, fastsettelse av strategi og mål, gjennomføring, informasjon, kommunikasjon og rapportering, samt gjennomgang og evaluering av praksis for å styrke virksomhetens måloppnåelse.

Styrets ansvar for å føre tilsyn med risiko kan omfatte, men er ikke begrenset til:

- Å gjennomgå ledelsens arbeid, samt utfordre og komme til enighet med ledelsen om:
 - Foreslått strategi og risikoappetitt.
 - Tilpasning av strategi og forretningsmessige mål til foretakets formål, visjon og kjerneverdier.
 - Vesentlige forretningsmessige beslutninger, inkludert fusjoner, oppkjøp, kapitalallokeringer, finansiering og utbytte.
 - Håndtering av betydelige svingninger i foretakets måloppnåelse eller porteføljevurdering av risiko.
 - Håndtering av avvik fra kjerneverdier.
- Godkjenning av ledelsesinsentiver og godtgjørelser.
- Deltakelse i arbeid med investor- og interessentrelasjoner.

Spørsmål til ledelsen

Kan alle ledere - ikke bare den som har ansvar for risikostyringsfunksjonen – gjøre rede for hvordan risiko er evaluert ved valg av strategi eller forretningsmessige beslutninger? Kan lederne klart formulere enhetens risikoappetitt og hvordan den kan påvirke spesifikke beslutninger? Resultatet fra den dialogen kan kaste lys over hvordan man faktisk tenker rundt risikotaking i organisasjonen.

Styrene kan også be den øverste ledelsen om ikke å snakke utelukkende om risikoprosesser, men også om kultur. Hvordan fremmer eller hindrer kulturen ansvarlig risikotaking? Hvordan overvåker ledelsen risikokulturen, og hvordan har kulturen endret seg? Etter hvert som ting endres - og ting vil forandre seg enten de er på enhetens radar eller ikke - hvordan kan styret være trygg på at ledelsen har en egnet og rettidig håndtering av dette?

På lang sikt kan helhetlig risikostyring også forbedre virksomhetens fleksibilitet og motstandsdyktighet - evnen til å forutse og reagere på endringer. Den hjelper organisasjoner med å identifisere faktorer som ikke bare innebærer risiko, men også endring, samt se hvordan denne endringen kan påvirke måloppnåelsen og nødvendiggjøre omlegging av strategi. Ved en klarere forståelse av slike endringer kan organisasjonen utarbeide en tilpasset handlingsplan; f.eks. ta stilling til om den bør være defensiv og trekke seg tilbake, eller offensivt investere i et nytt forretningsområde. Helhetlig risikostyring er et egnet rammeverk som legger godt til rette for at styrene kan vurdere risiko og bidra til å styrke virksomhetens tilpasnings- evne og motstandsdyktighet.

Hva helhetlig risikostyring har oppnådd

COSO publiserte *Helhetlig risikostyring - Et integrert rammeverk* i 2004, og det kom i norsk versjon i 2005. Formålet med publikasjonen var å hjelpe virksomhetene til bedre å beskytte og styrke interessentenes verdier. Den underliggende filosofien var at "maksimal verdiskapning oppnås når ledelsen fastsetter strategi og målsettinger slik at det er optimal balanse mellom vekst- og lønnsomhetsmål og relaterte risikoer, og utnytter ressursene målrettet og kostnadseffektivt for å nå virksomhetens mål." ³

³ Helhetlig risikostyring – Et integrert rammeverk, Sammendrag, COSO (2004/2005).

Siden publiseringen har rammeverket blitt brukt med suksess rundt i verden, i ulike næringer og i organisasjoner av alle typer og størrelser, for å identifisere risikoer, håndtere disse innenfor en definert risikoappetitt og bidra til måloppnåelse. Selv om mange har anvendt rammeverket i praksis har det likevel potensial for mer omfattende bruk. Det kunne med fordel gått dypere og tydeligere inn i visse aspekter, og gitt større innsikt i sammenhengen mellom strategi, risiko og måloppnåelse. Derfor vil det oppdaterte rammeverket:

- Knytte helhetlig risikostyring bedre opp mot interessentenes mange forventninger.
- Se risiko i sammenheng med organisasjonens måloppnåelse, ikke som gjenstand for en isolert øvelse.
- Sette organisasjoner i stand til bedre å forutse risiko, slik at de kan komme den i forkjøpet, og forstå at forandring skaper muligheter, ikke bare potensielle kriser.

I denne oppdateringen legges det også sterkere vekt på hvordan helhetlig risikostyring påvirker strategien og effektueringen av denne.

Fordeler ved hensiktsmessig og effektiv risikostyring

Alle organisasjoner trenger å fastsette en strategi som de jevnlig tilpasser. De må alltid være oppmerksomme både på de stadig skiftende mulighetene for å skape verdier, og utfordringer dette fører med seg. Dermed trenger organisasjonene et best mulig rammeverk for optimalisering av strategien og måloppnåelsen.

Det er her helhetlig risikostyring kommer til sin rett. Organisasjoner som integrerer helhetlig risikostyring i hele virksomheten kan oppnå mange fordeler, inkludert, men ikke begrenset til å:

- *Øke omfanget av muligheter:* Ved å vurdere alle mulige utfall – både de positive og de negative sider ved risiko – kan nye muligheter og spesielle utfordringer knyttet til kjente muligheter identifiseres.
- *Identifisere og håndtere risiko i virksomheten samlet sett:* Alle enheter står overfor utallige risikoer som kan påvirke mange deler av organisasjonen. Noen ganger kan en risiko stamme fra én del av virksomheten, men påvirke en annen del. Ledelsen vil derfor identifisere og styre disse risikoene helhetlig for å opprettholde og forbedre måloppnåelsen.
- *Forbedre positive resultater og fortrinn samtidig som negative overraskelser reduseres:* Gjennom bruk av helhetlig risikostyring kan virksomhetene forbedre evnen til å identifisere risikoer og håndtere dem på hensiktsmessig vis, redusere overraskelser med tilhørende kostnader eller tap, men samtidig dra nytte av fordelaktige utviklinger.

Oppklaring av noen misoppfatninger

Vi har hørt noen misoppfatninger om det opprinnelige rammeverket siden det ble introdusert i 2004. For å rydde opp i dette:

Helhetlig risikostyring er ikke en funksjon eller en avdeling. Det er den kulturen, de egenskapene og den praksisen som organisasjoner integrerer med strategi og som de benytter når strategien settes ut i praksis. Dette for å styre risikoen når verdier skapes, bevares og realiseres.

Helhetlig risikostyring er mer enn en risikoopplisting. Helhetlig risikostyring krever mer enn å utarbeide en oversikt over alle risikoene i organisasjonen. Det inkluderer også rutiner og retningslinjer som ledelsen har etablert for aktivt å håndtere risiko.

Helhetlig risikostyring omhandler mer enn intern kontroll. Det dreier seg også om andre tema, som fastsettelse av strategi, virksomhetsstyring, kommunikasjon med interessenter og resultatmåling. Prinsippene gjelder for alle nivåer og på tvers av alle funksjoner i organisasjonen.

Helhetlig risikostyring er ikke en sjekklister. Det er et sett prinsipper som rutiner og prosesser kan bygges på eller integreres i for en bestemt organisasjon, og det er et system for oppfølging og læring samt forbedring av måloppnåelse.

Helhetlig risikostyring kan brukes av organisasjoner av enhver størrelse. Hvis organisasjonen har et formål, en strategi og målsettinger – og behov for å ta avgjørelser som fullt ut tar hensyn til risiko – da kan helhetlig risikostyring benyttes. Helhetlig risikostyring kan og bør brukes av alle typer organisasjoner, fra små bedrifter til ideelle organisasjoner, statlige etater og de største børsnoterte selskapene.

- *Redusere variasjon i måloppnåelse:* For noen dreier utfordringene seg mindre om overraskelser og tap enn om variasjon i måloppnåelse. Å være i forkant av planen eller prestere utover forventningene kan gi like store bekymringer som det å være forsinket eller levere mindre enn forventet. Helhetlig risikostyring setter organisasjonene i stand til å forutse risiko som vil påvirke måloppnåelse, og gjøre det mulig å sette i gang de tiltak som trengs for å minimere avvik og maksimere muligheter.
- *Forbedre ressursutnyttelsen:* Hver risiko kan ses på som noe som krever bruk av ressurser. Med tilgang til solid informasjon om risiko kan ledelsen vurdere de samlede ressursbehovene, prioritere ressursene og forbedre ressursfordelingen.
- *Styrke bedriftens fleksibilitet og motstandsdyktighet:* En virksomhets levedyktighet over tid er avhengig av dens evne til å forutse og håndtere endringer, ikke bare for å overleve, men også for å utvikle seg videre. Dette blir stadig viktigere ettersom forandringstakten akselererer og forretningskompleksiteten øker. En hensiktsmessig og effektiv helhetlig risikostyring bidrar til slik økt fleksibilitet og motstandsdyktighet.

Disse fordelene viser at risiko ikke skal ses utelukkende som en mulig begrensning eller utfordring i enhetens fastsetting av en strategi og gjennomføring av den. Tvert om, forandringen som ligger til grunn for risikoen, og organisasjonens håndtering av denne, vil gi strategiske muligheter og åpne for at virksomheten utvikler viktige særpreg.

Risikoens rolle ved valg av strategi

Å velge strategi handler om å ta beslutninger som omfatter avveininger og tilpasninger. Dermed er det fornuftig å anvende helhetlig risikostyring når strategien velges, da det er den beste tilnærmingen for å gjøre velinformerte valg.

Risiko er tema i mange strategiprosesser, men ofte vurderes risikoen primært med tanke på dens mulige effekt på en allerede fastlagt strategi. Med andre ord fokuserer risikodiskusjoner på den eksisterende strategien: Hva kan påvirke denne strategiens relevans og levedyktighet?

Det er likevel også andre spørsmål som bør stilles knyttet til strategi, og som organisasjonene er blitt bedre til å stille: Har vi tilpasset oss kundens behov korrekt? Vil vår forsyningskjede levere i tide og innenfor budsjett? Vil nye konkurrenter dukke opp? Er vår teknologiske infrastruktur tilpasset oppgaven? Dette er den type spørsmål ledelsen bryner seg på hver dag, og for at strategien skal la seg gjennomføre er det avgjørende at slike spørsmål blir besvart og fulgt opp.

Risikoen for den valgte strategien er imidlertid bare ett av aspektene som vurderes. Som dette rammeverket understreker, er det ytterligere to aspekter ved helhetlig risikostyring som kan ha langt større innvirkning på en virksomhets verdi: muligheten for at strategien ikke er tilpasset, og konsekvensene av den strategien som er valgt.

Det første aspektet, **muligheten for at strategien ikke er i samsvar med organisasjonens formål, visjon og kjerneverdier**, er sentralt for beslutningene ved valg av strategi. Enhver enhet har et formål, en visjon og kjerneverdier som definerer hva organisasjonen prøver å oppnå og hvordan virksomheten drives. Noen organisasjoner er skeptiske til virkelig å ta inn over seg innholdet i disse formuleringene. Men formål, visjon og kjerneverdier har vist seg å ha stor betydning, og de har mest betydning når det gjelder å håndtere risiko og forbli motstandsdyktig og fleksibel i endringstider.

En valgt strategi må støtte opp under organisasjonens formål og visjon. En feiljustert strategi øker muligheten for at organisasjonen ikke realiserer formålet og visjonen, eller den kan kompromittere organisasjonens verdier, selv om strategien er gjennomført på en vellykket måte. I helhetlig risikostyring vurderes derfor muligheten for at strategien ikke er i samsvar med organisasjonens formål og visjon.

Konsekvensene av den valgte strategien er det andre aspektet som kommer i tillegg. Når ledelsen utvikler en strategi og går gjennom alternativer med styret, tas det beslutninger om de avveininger og tilpasninger strategien fører med seg. Hver alternative strategi har sin egen risikoprofil som omhandler konsekvenser av strategien. Styret og ledelsen må avgjøre om strategien fungerer i samsvar med organisasjonens risikoappetitt, og hvordan strategien hjelper virksomheten å nå sine målsettinger og fordele ressursene hensiktsmessig og effektivt.

Kort oppsummert: Helhetlig risikostyring handler like mye om å forstå konsekvensene av strategien og muligheten for at strategiske valg ikke er tilpasset, som om å styre risikoen for ikke å nå fastsatte mål. Figuren under illustrerer disse betraktningene sett i forhold til formål, visjon, kjerneverdier, og som en pådriver for virksomhetens overordnede retning og måloppnåelse.



Helhetlig risikostyring, slik den vanligvis har blitt praktisert, har hjulpet mange organisasjoner med å identifisere, vurdere og håndtere risiko forbundet med strategien. Men de viktigste årsakene til verdiforringelse ligger i risikoen for at strategien ikke støtter opp under enhetens formål og visjon, og konsekvensene av den valgte strategi.

Helhetlig risikostyring forbedrer prosessen når strategien velges. Å velge en strategi krever en strukturert beslutningsprosess som analyserer risiko og tilpasser ressursene til organisasjonens formål og visjon.

Et fokusert rammeverk

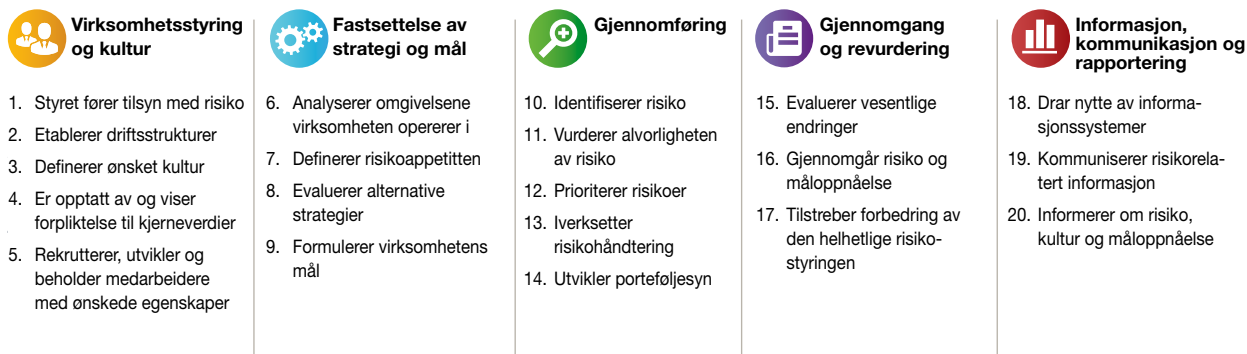
Helhetlig risikostyring—Integrering med strategi og måloppnåelse klargjør betydningen av helhetlig risikostyring i strategisk planlegging samt innføring av helhetlig risikostyring i hele organisasjonen. Risiko påvirker og samordner strategi og måloppnåelse på tvers av alle avdelinger og funksjoner.



Rammeverket består av et sett med prinsipper organisert i fem komponenter som henger nært sammen:

- 1. Virksomhetsstyring og kultur:** Virksomhetsstyring bidrar til etablering av organisasjonskultur, styrker betydningen av helhetlig risikostyring og fastsetter ansvaret for oppfølging av den. Kultur omhandler etiske verdier, ønsket atferd og forståelse for risiko i enheten.
- 2. Fastsettelse av strategi og mål:** Helhetlig risikostyring, strategi og fastsettelse av mål er elementer som virker sammen i strategiplanprosessen. Risikoappetitt blir fastsatt og avstemt mot strategien; virksomhetens mål setter strategien ut i praksis og danner samtidig grunnlag for å identifisere, evaluere og respondere på risiko.
- 3. Gjennomføring:** Risiko som kan påvirke oppnåelsen av strategiske og operasjonelle mål må identifiseres og evalueres. Risikoer prioriteres ut fra alvorlighetsgrad i forhold til risikoappetitt. Organisasjonen velger deretter risikohåndtering og benytter et porteføljesyn på hvor mye risiko den kan pådra seg. Resultatene av denne prosessen rapporteres til relevante interessenter.
- 4. Gjennomgang og revurdering:** Ved å gjennomgå enhetens måloppnåelse kan en organisasjon ta stilling til hvor godt komponentene i den helhetlige risikostyringen virker over tid og ved betydelige endringer, samt identifisere behov for revurderinger.
- 5. Informasjon, kommunikasjon og rapportering:** Helhetlig risikostyring krever en kontinuerlig prosess for å innhente og dele nødvendig informasjon, både fra interne og eksterne kilder, som kommuniseres i hele organisasjonen.

De fem komponentene i det oppdaterte rammeverket støttes av et sett prinsipper.⁴ Disse prinsippene dekker alt fra virksomhetsstyring til oppfølging. De er håndterbare i omfang, og de beskriver forskjellige fremgangsmåter som kan brukes på ulike organisasjoner uansett størrelse, type eller sektor. Overholdelse av prinsippene kan gi ledelsen og styret rimelig grunn til å forvente at organisasjonen forstår risikoer knyttet til strategien og virksomhetens mål, og søker å styre disse.



En titt inn i fremtiden

Det er ingen tvil om at organisasjonene fortsatt står overfor en fremtid preget av volatilitet, kompleksitet og usikkerhet. Helhetlig risikostyring vil da være viktig for organisasjonens evne til å overleve og lykkes. Uavhengig av type og størrelse på en enhet, må strategiene samsvare med organisasjonens formål. Alle enheter må ha egenskaper som bidrar til effektiv og hensiktsmessig endringshåndtering, herunder en smidig beslutningsprosess, evnen til å reagere på en koordinert måte, og omstillingsevne som gjør det mulig å forandre og reposisjonere seg samtidig som man opprettholder høy grad av tillit fra interessentene.

Flere trender vil påvirke den helhetlige risikostyringen i fremtiden. Vi nevner fire av disse:

- *Håndtering av rask spredning av data:* Etter hvert som stadig mer data blir tilgjengelig og hastigheten ved analyse av nye data øker, må den helhetlige risikostyringen tilpasses. Dataene vil være både interne og eksterne, og de vil være strukturert på nye måter. Avanserte analyser og datavisualiseringsverktøy vil bli tilgjengelige og til stor hjelp for å forstå risiko og risikoens betydning, både den positive og den negative.
- *Bruk av kunstig intelligens og automatisering:* Mange mener at vi nå er inne i de automatiserte prosessers og den kunstige intelligensens tid. Uavhengig av individuelle oppfatninger er det viktig at man i den helhetlige risikostyringen vurderer effekten av disse og fremtidige teknologier, og utnytter mulighetene de gir. Sammenhenger, trender og mønstre som det tidligere ikke var mulig å identifisere, kan avdekkes og bli en rik kilde til informasjon som er avgjørende for virksomhetens håndtering av risiko.
- *Styring av kostnadene ved risikostyring:* Mange bedriftsledere er bekymret for kostnadene ved risikostyring, complianceprosesser og kontrollaktiviteter, sett opp mot verdien dette gir. Etter hvert som helhetlig risikostyring utvikles er det viktig at aktivitetene knyttet til risiko, compliance, kontroll og til og med virksomhetsstyring, samordnes effektivt, slik at organisasjonen får maksimal nytte av disse. Dette aspektet kan bli en av de beste mulighetene for å redefinere betydningen av helhetlig risikostyring i organisasjonen.

⁴ En mer utfyllende beskrivelse av disse 20 prinsippene er gjengitt på slutten av dette dokumentet.

- *Bygge sterkere organisasjoner:* Etter hvert som organisasjoner blir bedre til å integrere helhetlig risikostyring med strategi og måloppnåelse, vil det åpne seg muligheter for å styrke deres fleksibilitet og motstandsdyktighet. Ved å vite hvilke risikoer som vil ha størst innvirkning på enheten, kan organisasjoner dra nytte av helhetlig risikostyring for å bli i stand til å respondere tidlig. Dette vil åpne opp for nye muligheter.

Kort oppsummert: helhetlig risikostyring vil måtte endres og tilpasses til fremtiden for til enhver tid å tilby de fordelene som er beskrevet i rammeverket. Med riktig fokus vil fordelene som oppnås ved helhetlig risikostyring klart overstige kostnadene og gi organisasjoner trygghet på egen evne til å håndtere fremtiden.

Komponenter og prinsipper

1. **Styret fører tilsyn med risiko** — Styret fører tilsyn med strategien og utøver sine virksomhetsstyringsforpliktelser som støtte for ledelsen i arbeidet med å gjennomføre strategien og nå virksomhetens mål.
2. **Etablerer driftsstrukturer** — Organisasjonen etablerer driftsstrukturer i arbeidet med å gjennomføre strategien og nå virksomhetens mål.
3. **Definerer ønsket kultur** — Organisasjonen definerer den atferd som karakteriserer enhetens ønskede kultur.
4. **Er opptatt av og viser forpliktelse til kjerneverdier** — Organisasjonen er opptatt av og viser forpliktelse til enhetens kjerneverdier.
5. **Rekrutterer, utvikler og beholder medarbeidere med ønskede egenskaper** — Organisasjonen er opptatt av å bygge menneskelig kapital som er i samsvar med strategien og virksomhetens mål.
6. **Analyserer omgivelsene virksomheten opererer i** — Organisasjonen vurderer potensielle virkninger omgivelsene kan ha på risikoprofilen.
7. **Definerer risikoappetitten** — Organisasjonen definerer risikoappetitten som en del av prosessen med å skape, bevare og realisere verdi.
8. **Evaluerer alternative strategier** — Organisasjonen evaluerer alternative strategier og den potensielle innvirkning disse kan ha på risikoprofilen.
9. **Formulerer virksomhetens mål** — Organisasjonen vurderer risiko når den på ulike nivåer etablerer virksomhetens mål, som er i samsvar med strategien og støtter opp om den.
10. **Identifiserer risiko** — Organisasjonen identifiserer risiko som påvirker gjennomføringen av strategien og oppnåelse av virksomhetens mål.
11. **Vurderer alvorligheten av risiko** — Organisasjonen vurderer hvor alvorlig risikoen er.
12. **Prioriterer risikoer** — Organisasjonen prioriterer risikoer som grunnlag for beslutninger om hvordan disse skal håndteres.
13. **Iverksetter risikohåndtering** — Organisasjonen identifiserer og velger hvordan risikoen skal håndteres.
14. **Utvikler porteføljesyn** — Organisasjonen utvikler og evaluerer et porteføljesyn på risiko.
15. **Evaluerer vesentlige endringer** — Organisasjonen identifiserer og evaluerer endringer som i vesentlig grad kan påvirke strategien og virksomhetens mål.
16. **Gjennomgår risiko og måloppnåelse** — Organisasjonen gjennomgår enhetens måloppnåelse og vurderer risiko.
17. **Tilstreber forbedring av den helhetlige risikostyringen** — Organisasjonen tilstreber kontinuerlig forbedring av den helhetlige risikostyringen.
18. **Drar nytte av informasjonssystemer** — Organisasjonen drar nytte av enhetens informasjons- og teknologisystemer for å understøtte den helhetlige risikostyringen.
19. **Kommuniserer risikorelatert informasjon** — Organisasjonen bruker kommunikasjonskanaler til å understøtte den helhetlige risikostyringen.
20. **Informerer om risiko, kultur og måloppnåelse** — Organisasjonen informerer om risiko, kultur og måloppnåelse på flere nivåer og på tvers av enheten.

Anerkjennelser

En spesiell takk til følgende selskaper og organisasjoner for deres tillatelse til at medlemmer av Advisory Council og observatørene kunne delta.

Medlemmer av Advisory Council

Selskaper og organisasjoner

- Athene USA (Jane Karli)
- Edison International (David J. Heller)
- First Data Corporation (Lee Marks)
- Georgia-Pacific LLC (Paul Sobel)
- Invesco Ltd. (Suzanne Christensen)
- Microsoft (Jeff Pratt)
- US Department of Commerce (Karen Hardy)
- United Technologies Corporation (Margaret Boissoneau)
- Zurich Insurance Company (James Davenport)

Høyere utdanning og foreninger

- North Carolina State University (Mark Beasley)
- St. John's University (Paul Walker)
- The Institute of Internal Auditors (Douglas J. Anderson)

Profesjonelle konsulentselskaper

- Crowe Horwath LLP (William Watts)
- Deloitte & Touche LLP (Henry Ristuccia)
- Ernst & Young (Anthony J. Carmello)
- James Lam & Associates (James Lam)
- Grant Thornton LLP (Bailey Jordan)
- KPMG LLP Americas (Deon Minnaar)
- Mercury Business Advisors Inc. (Patrick Stroh)
- Protiviti Inc. (James DeLoach)

Tidligere COSO-styremedlem

- COSO Chair, 2009-2013 (David Landsittel)

Observatører

- Federal Deposit Insurance Corporation (Harrison Greene)
- Government Accountability Office (James Dalkin)
- Institute of Management Accountants (Jeff Thompson)
- Institut der Wirtschaftsprüfer (Horst Kreisel)
- International Federation of Accountants (Vincent Tophoff)
- ISACA (Jennifer Bayuk)
- Risk Management Society (Carol Fox)



En komplett versjon av

Helhetlig risikostyring – Integrering med strategi og måloppnåelse

på engelsk, kan kjøpes ved å besøke websiden www.coso.org.