Mislighetsområdet – en bekymring for internrevisor?

IIA standardene stiller en rekke krav til internrevisjoners arbeid for å forebygge og avdekke misligheter. Vi har ønsket å finne ut hvorvidt standardene etterleves i praksis. Resultatene viser at det gjøres mye godt arbeid, men også et klart forbedringspotensial.

Det er et potensial for å profesjonalisere praksisen når det gjelder en systematisk tilnærming til forebygging og avdekking av misligheter, vurdering av risiko for misligheter i det enkelte revisjonsoppdrag, bruk av nye digitale løsninger for å vurdere mislighetsrisiko og avdekke eventuelle misligheter, samt ikke minst når det gjelder rapportering av mislighetsrisiko til toppledelsen og styret.

AV VERONICA STORLID KVINGE
Prosjektleder internrevisjon, BKK AS
Medlem i IIA Norges mislighetsnettverk

AV HEGE SKJELBRED-ERIKSEN
Nestleder, internrevisjonen Norconsult AS

I forbindelse med studiet *Intern revisjon, governance, risikostyring, intern styring og kontroll* ved Handelshøyskolen BI, skrev vi våren 2018 en oppgave med tittelen *En studie av i hvilken grad norske internrevisjoner etterlever IIA standardenes krav til forebygging og avdekking av misligheter.* Formålet med oppgaven var å vurdere i hvilken grad norske internrevisjoner etterlever kravene i IIA standardene knyttet til forebygging og avdekking av misligheter. Dette har vi gjort ved å utføre en spørreundersøkelse blant ledere av internrevisjoner som er medlem av IIA Norge. Undersøkelsen ble sendt ut til 133 virksomheter, hvorav 50 besvarte undersøkelsen. Vi har ikke funnet at det tidligere er gjort tilsvarende undersøkelser i Norge, eller i Norden for øvrig.

Norge er fortsatt i stor grad et tillitsbasert samfunn. Dette er en viktig verdi i samfunnet vårt, men det kan også gi noen utfordringer med å få tilstrekkelig støtte til et aktivt arbeid for å forebygge og avdekke misligheter. Samtidig øker digitaliseringen av samfunnet risikoen for misligheter. Alle individer i en organisasjon har et ansvar for å forebygge og avdekke misligheter. Styret, toppledelsen og internrevisjonen har imidlertid et særlig ansvar for å forebygge misligheter i en virksomhet. Vi har i oppgaven fokusert på hvordan norske internrevisjoner ivaretar dette ansvaret.

Vår konklusjon er at de fleste internrevisjonene har et bevisst forhold til risikoen for misligheter, de jobber metodisk for å avdekke misligheter, om enn kun i en andel av revisjonsoppdragene sine, og de opplever å ha relativt god kompetanse til å revidere mislighetsområdet. Vi ser imidlertid også at ingen av IIA standardene vi har sett på (IIA standard 1210.A2, 1220.A1, 1220.A2, 2060 og 2120.A2), etterleves fullt ut av alle respondentene i undersøkelsen. Kun halvparten av internrevisjonene i undersøkelsen fortalte at de hadde etablert et metodeverk som beskriver hvordan de skal jobbe for å avdekke misligheter, og således kan sies å ha en strukturert tilnærming til dette arbeidet.

Under vil vi trekke frem funn innenfor fem temaer i undersøkelsen som vi vurderer som særlig interessante. Studien er i sin helhet tilgjengelig på følgende lenke: https://brage.bibsys.no/xmlui/handle/11250/2573426.

Vurdering av risiko for misligheter

Standard 2120.A2 stiller krav til at internrevisor skal vurdere muligheter for at misligheter kan forekomme, og hvordan organisasjonen håndterer risikoen for misligheter. Vanlige måter å følge opp dette kravet på, er gjennom risikoanalyser på mislighetsområdet, ved å se etter mislighetsindikatorer, dialog med medarbeidere og ledere i virksomheten, samt

> Kun en fjerdedel av respondenter forteller at de har dialog om risikoen for misligheter med revisjonsutvalget eller styret.

gjennomgang av eventuelle varslingssaker knyttet til misligheter. Kun en fjerdedel forteller at de har dialog om risikoen for misligheter med revisjonsutvalget eller styret. Dette gir en risiko for at internrevisjonen går glipp av nyttig informasjon ved ikke å diskutere dette med styret. Topplederе og eiere er oftere i en posisjon som gir mulighet til å begå misligheter av et større og alvorligere omfang enn øvrige medarbeidere i virksomheten. Styret vil i mange tilfeller ha et relativt tett samarbeid med toppledelsen, og kan ha interessante refleksjoner rundt risikoen for at topplederе kan begå misligheter.

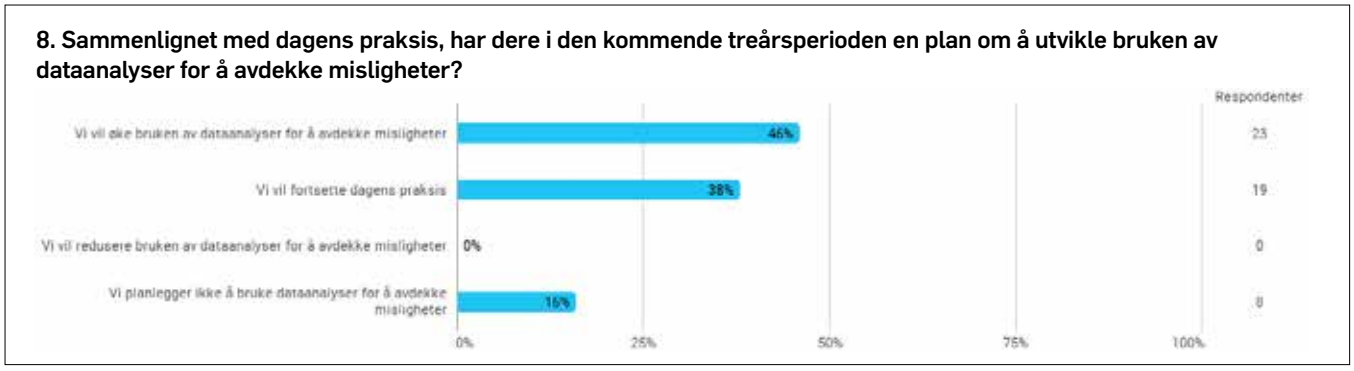
Teknologibasert revisjon (figur 1)

Standard 1220.A2 stiller krav om at internrevisjonen må vurdere å ta i bruk teknologibasert revisjon og andre dataanalyseteknikker. Dataanalyser er blant annet velegnet til raskt og effektivt avdekke avvik i transaksjoner i en database, og gir revisor et effektivt verktøy for å analysere identifiserte avvik. De siste årene er det lansert stadig flere og mer effektive digitale verktøy for å avdekke misligheter, og flere og flere internrevisjoner tar i bruk slike hjelpemidler. Likevel oppgir mindre enn halvparten at de har tatt i bruk dataanalyser for å vurdere risikoen for misligheter på ulike områder.

Det er positivt at nesten halvparten oppgir at de vil øke bruken av dataanalyser for å avdekke misligheter. Selv om det er en relativt liten prosentandel er det interessant at 16% av respondentene ikke planlegger å bruke dataanalyser for å avdekke misligheter i den kommende treårsperioden.

Risikovurdering av mislighetsrisiko i revisjonsoppdrag (figur 2)

Standard 1220.A1 stiller krav til at internrevisor vurderer risikoen for misligheter og feil i utførelse av revisjonsoppdrag. De fleste forteller at de vurderer mislighets-



Figur 1

Figur 2

risiko i en andel av gjennomførte revisjonsoppdrag, men det er stor variasjon i hvor stor andel av oppdragene dette gjøres. Så lenge mennesker har en rolle i eller kan påvirke en prosess, er det en risiko for at misligheter kan finne sted. Kun 18% sier at de vurderer slik risiko for alle revisjonsoppdrag.

Vi spurte også hvilke metoder internrevisjonene bruker for å avdekke misligheter i revisjonsoppdrag:

Internasjonale undersøkelser viser at oppfølging av varsler var hovedårsaken til avdekking av hele 40% av mislighetssaker globalt i 2017. Kun halvparten av respondentene forteller imidlertid at de følger opp indikasjoner på misligheter i varsel. Sett i sammenheng med at blant de 44% som oppga å ha avdekket misligheter, oppga hele 82% at informasjon i varsel var hovedårsak til avdekking av en eller flere misligheter, indikerer dette at internrevisjonene bør øke fokuset på oppfølging av varsel på mislighetsområdet.

IT-kontroller er kun oppgitt som viktigste kilde til at misligheter ble avdekket i 1% av tilfellene globalt. I vår undersøkelse oppgir 42% at de benytter dataanalyser for å avdekke misligheter i revisjonsoppdrag, og hele 32% av de som hadde avdekket misligheter oppga at dataanalyser hadde vært en viktig årsak til at misligheter ble avdekket. Det kan således synes som om norske internrevisjoner er kommet relativt langt når det gjelder bruk av IT-verktøy for å avdekke misligheter i et globalt perspektiv.

Avdekking av misligheter (figur 3)

I overkant av halvparten av respondentene i undersøkelsen fortalte at de ikke har avdekket tilfeller av misligheter i løpet av de siste tre årene. På spørsmål om hva de trodde var viktigste årsak til at de ikke hadde avdekket misligheter svarte de som gjengitt i figur 3.

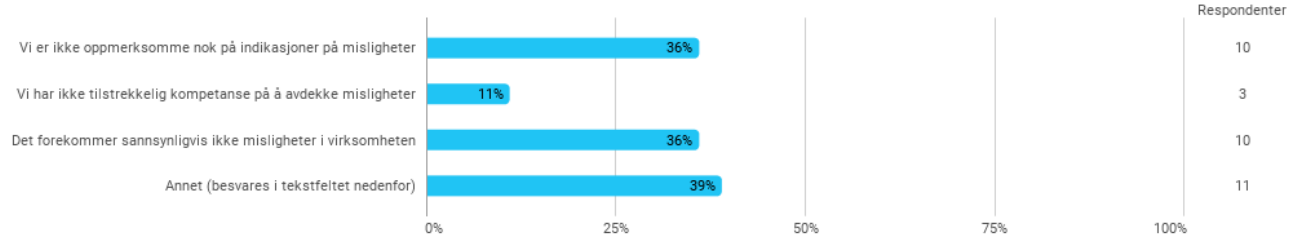
Det er interessant at hele 36% av respondentene som ikke hadde avdekket misligheter oppga at det sannsynligvis ikke forekommer misligheter i virksomheten. Eksperter på avdekking av misligheter anslår at kostnader knyttet til misligheter beløper seg til om lag 5 % av virksomheters omsetning globalt. Det er en risiko for misligheter i alle prosesser som involverer mennesker, og selv om mislighetsrisikoen varierer mellom bransjer, er ingen virksomheter uten slik risiko. Det er derfor overraskende at en så høy andel av respondentene ikke tror det forekommer misligheter internt i egen virksomhet. Her var det imidlertid stor forskjell mellom privat og offentlig virksomhet, ved at kun i overkant av 5% av de offentlige virksomhetene fortalte at de ikke trodde det forekom misligheter internt, hvilket indikerer at de er relativt oppmerksomme på risikoen for misligheter. Dette står imidlertid i kontrast til andre funn for offentlig virksomhet, derunder at de i mindre grad enn private virksomheter har tatt i bruk, og planlegger å ta i bruk, datanalyser for å forebygge og avdekke eventuelle misligheter, og at flere offentlige virksomheter oppgir at de ikke leter etter misligheter ved gjennomføring av revisjonsoppdrag.

> Hele 36% av respondentene som ikke hadde avdekket misligheter oppga at det sannsynligvis ikke forekommer misligheter i virksomheten.... anslag internasjonalt er at misligheter i snitt utgjør 5% av virksomheters omsetning

Rapportering til toppledelse og styret

Når det gjelder rapportering på mislighetsrisiko til toppledelsen og styret, har vi identifisert et stort forbedringspotensial. Selv om de fleste respondentene oppgir at de rapporterer minimum årlig på mislighetsrisiko til både toppledelsen og styret, er det en overraskende høy andel som oppgir at de ikke foretar slik rapportering til tross for at standard 2060 stiller krav til slik rapportering. 22% sier de aldri rapporterer på mislighetsrisiko til toppledelsen, mens tilsvarende tall for rapportering til styret er på hele 34%. Konklusjonen er således at et betydelig antall av respondentene ikke synes å etterleve kravet til rapportering på mislighetsrisiko til toppledelsen og styret.

18. Hva tror du er viktigste årsak til at dere ikke har avdekket noen misligheter? (velg et eller flere svaralternativer)



Figur 3

sendringer. Det viktigste, og kanskje det vanskeligste kan jeg tilføye for egen del, er å bygge kultur for GDPR forståelse og etterlevelse. Lillian Engebø tok oss deretter gjennom etableringen av en vellykket GDPR og hun delte villig med oss sin velprøvde oppskrift fra Konsernrevisjonen i DNB. De 7 personvernprinsippene er hovedingrediensene for et godt resultat. Et godt tips til alle var å tenke gjennom de persondata som du selv forvalter i din jobb og ta konkret stilling til oppbevaringstiden. Gjennom de tilbakemeldinger som kom fra deltakerne rundt bordet kunne det konstateres at det opereres med alt fra 3 til 10 års datostempling.

> Neste hovedrett kan betegnes som noe mer eksotisk, eller i hvert fall nyskapende ved at vi fikk en svært så interessant innføring i robotisering og automatisering.

Den neste hovedretten kan kanskje betegnes som noe mer eksotisk, eller i hvert fall nyskapende ved at vi fikk en svært så interessant innføring i robotisering og automatisering. Dette innlegget var det Gaute Brynildsen, revisjonssjef fra Gjensidige og Ida Kjær fra Konsernrevisjonen i DNB som var mester for. De dro oss gjennom digitalisering og trender. De hjalp oss å konstatere at dette med roboter egentlig har vært her ganske lenge, utviklingen går saktere enn vi går rundt og tror, og de er ikke så farlige som de kan synes ved første øyekast. Vi trodde eksempelvis i 2014 at bankene snart skulle bli irrelevante og at google skulle komme og ta oss. Hva har skjedd? Frykten er der men heller ikke så mye mer. Vi ble introdusert til de to AI-robotene Alexa og Sofia. Sistnevnte deltok endog på et amerikansk TV show. Etikk og teknologi er tema som forsamlingen tar med det største alvor, og i denne sammenheng byr det på ekstra utfordringer. Ta eksempelvis dette med selvkjørende biler. Det må programmeres i hvilken rekkefølge levende vesener skal dø i krisesituasjoner i trafikken, og noen må ta stilling til dette spørsmålet i forbindelse med programmeringen. Ingen tenker på at trafikksikkerheten gjerne kan bli bedre totalt sett med rasjonelle roboter i stedet for levende sjåfører. Det neste fenomen vi ble introdusert for var ansiktsgjenkjenning i Kina. Smartkameraer brukes til å finne igjen kidnappede barn. Her ville det vært noen svært store spørsmål knyttet til personvern hvis det hadde foregått på mer hjemlige arenaer. Nytten av AI er likevel stor for finansnæringen som i dag, ved å gjøre bruk av avansert logikk, spesialkompetanse og stor datakraft, kan drive effektiv fraud analytics. Vi ble til slutt presentert for noen risk cases som fikk oss til å rette litt ekstra opp i stolen. Disse omfattet en lite vellykket bruk av robotics i form av en rekrutteringsrobot som diskriminerte kvinner, tradingalgoritmer som gikk bananas og hundretalls millioner kroner i virtuell valuta som gikk tapt. Vi kunne konstatere at risikofritt er heller ikke dette.

Vi hadde flere små pauser med mingling og kaffe, så også før det var klart for desserten. Den besto av hvitvask og økonomisk kriminalitet og kokken var Thomas Nielsen fra BDO. Han ga oss først en innføring i det globale trusselbildet.

> Desserten besto av hvitvask og økonomisk kriminalitet og kokken var Thomas Nielsen fra BDO.

Meldingen til finansforetakene var at de må beskytte seg selv siden etterforskningskapasiteten er på et lavmål. Igjen kom buzzordet «risikovurdering» opp på bordet. Denne gang i sammenheng med hvitvasking. Det skal lages en virksomhetsrettet risikovurdering. Den skal være konkret og individuell.

Vidar Hansen, Intern revisjonssjef Sparebanken Sør.

Risikovurderingen skal dokumenteres og forankres hos øverste ledelse. På denne bakgrunn skal det vurderes å etablere en egen anonym varslingskanal. Vi merket oss at dette ikke er sammenfallende med den varslingskanal som etableres i tråd med Arbeidsmiljøloven. Riset bak speilet er som kjent store sanksjoner. Top down risikovurderinger er ikke godt nok siden man da risikerer å ikke få med seg risikoen som ligger ute i satellittene. Innlegget var dessuten smaksatt med fenomenet sosiale bedragerier. Det ble referert til at 286 kjærlighetshungrige og kanskje litt, i hvert fall forbigående, naive nordmenn er blitt lurt for til sammen 164 mill NOK. Hva vi skulle mene om dette er det ikke så godt å si, annet enn at risikoen for å finne på mye rart er større i ruspåvirket tilstand, uansett hva rusen består i. Seansen toppet seg når vi til slutt ble utfordret til å tenke som en kriminell. Hva ville vi gjort hvis oppdraget var å hvitvaske 5 millioner kroner. Det viste seg at det var vi ganske gode til alle sammen, bare vi ble varmet opp litt. Det ene kreative forslaget etter det andre kom opp på bordet, men disse oppskriftene var faktisk så gode at det ville det bli veldig feil å dele de. Nielsen viste avslutningsvis til Basel AML indexen hvor Danmark har falt ned på stigen som følge av AML saken, mens Norge fortsatt ligger blant topp 10. Måtte det bli slik lenge.

Hele den lange dagen ble elegant anført under toastmaster Vidar Hansens kyndige veiledning. Han er avtroppende leder av nettverket og høstet stor applaus for sitt ukuelige engasjement til beste for alle.

Risikostyringsfunksjon i vekst og utvikling

AV KENNETH HANSEN
Senior prosjektleder, Konsernrevisjonen, Avinor

AV SIW-METTE THOMASSEN
Seniorrådgiver, avdeling for pensjon og forsikring, NHO

Selskapers fokus på helhetlig risikostyring har vært økende de siste 20 årene og spesielt etter Dot.com, Enron og senest finanskrisen. Store kriser har lagt grunnlaget for lovregulering på risikostyrings- og internkontrollområdet som f. eks Sarbanes-Oxley i 2002, men også flere rammeverk (COSO ERM fra 2004 og 2017 og ISO 2009).

I vår oppgave skrevet ved Handelshøyskolen BI, har vi gjennomført en spørreundersøkelse med formål å belyse organiseringen av helhetlig risikostyring i selskap notert på hovedlisten på Oslo Børs, samt gi mer kunnskap om risikostyringsfunksjonens involvering i strategiutviklingen.

Konklusjoner fra spørreundersøkelsen:

- Det å ha egen leder for risikostyringsfunksjon begynner å bli mer utbredt blant selskapene på Oslo Børs. De fleste av disse har en egen rapporteringslinje (formell/uformell) til styret.
- Det er stort fokus på rapportering og mindre på analyse av konsekvenser for selskapenes måloppnåelse og risikotiltak.
- Leder for risikostyringsfunksjonen opplever å bli hørt og deltar aktivt i strategiprosessen i større grad enn hva organiseringen av prosessene skulle tilsi, men brukes ikke som en aktiv rådgiver i strategiprosessene.

Flere bruker et rammeverk for helhetlig risikostyring (figur 1)

Selskapene svarer at nærmere 60 prosent har etablert helhetlig risikostyring. Flertallet anvender COSO-rammeverket (42 prosent), mange bruker egne modeller (35 prosent) og om lag 25 prosent bruker ISO. Andre modeller omfatter blant annet modeller som brukes i finansnæringen for å oppfylle kravene i kapitaldeknings- og solvensreguleringen.

Og en egen leder for risikostyring (CRO) er mer vanlig enn før

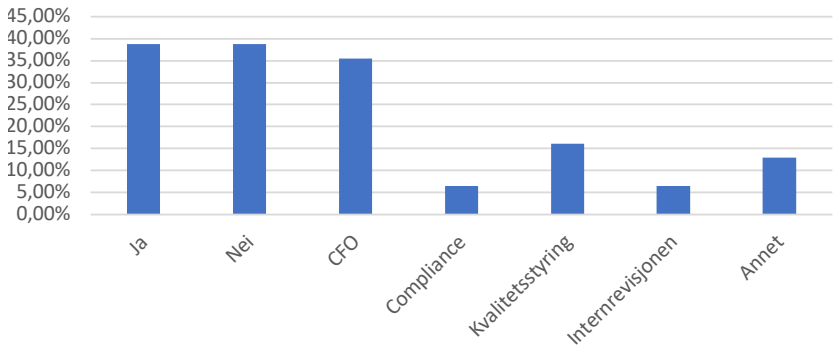
Av figur 2 ser vi at nesten 39 prosent svarer at de har organisert seg slik at risikostyringen ivaretas av en egen CRO-funksjon. Dette er en betydelig økning sammenlignet med en undersøkelse blant nordiske foretak i 2011, hvor 12 prosent svarte at de har en egen CRO-funksjon (Lundqvist, 2014).

> 39 % har egen CRO-funksjon kontra 12% i 2011

Av de som ikke har en egen CRO-funksjon svarer 35 prosent at dette ivaretas av CFO. Det er med andre ord fortsatt relativt vanlig at risikostyringen er et ansvar som

Figur 1

Figur 2



ligger hos CFO, enten faglig og/eller administrativt. Videre ser vi at 16 prosent svarer at dette ivaretas av egen kvalitetsstyringsfunksjon og 6,5 prosent svarer at ansvaret ligger hos Compliance. Et annet interessant funn er at 6,5 prosent svarer at internrevisjonen har ansvaret for risikostyringen, selv om dette er i strid med IIA sine anbefalinger. Dette er imidlertid ikke helt uvanlig. I en global undersøkelse gjennomført av IIA Research Foundation, fant man at internrevisor var ansvarlig for helhetlig risikostyring i 36 prosent av virksomhetene (de Zwaan et al., 2011).

I 6,5 % av tilfellene utføres risikostyring av internrevisjon

De fleste CROer har en egen rapporteringslinje (formell/uformell) til styret

Hele 60 prosent av respondentene svarer at risikostyringsfunksjonen rapporterer til CEO, om lag 13 prosent til CFO, om lag 7 prosent til styret mens 20 prosent rapporterer til andre.

Selv om leder av risikostyringsfunksjonen i Norge oftest rapporterer til CEO, er det viktig at det er formelle eller uformelle rapporteringslinjer til styret, slik at styremedlemmene kan ivareta sitt «påseansvar» på en hensiktsmessig måte. På spørsmål om CRO har en egen linje til styret (formelt eller uformelt), uavhengig av selve organiseringen/rapporteringen, svarer 47 prosent at de har en formell linje, mens 20 prosent har en uformell linje til styret. Dette vil si at vel 30% mener å ikke ha rapporteringslinje til styret. Et siste kvalitetstegn på uavhengighet er at man har et stillingsvern som innebærer at administrasjonen alene ikke kan si opp en CRO dersom det oppleves at rådene og risikoarbeidet ikke er det CEO eller CFO ser for seg. På denne bakgrunn har vi spurt om CRO kan avsettes uten styrets samtykke. Her deler selskapene seg i to like deler, som er noe overraskende basert på svar knyttet til organiseringen. Imidlertid burde dette legge til rette for CRO sin uavhengighet og evne til å opptre som en «uavhengig» rådgiver for styret og ledelsen.

Men fokus er på rapportering og mindre på analyse av konsekvenser for selskapenes måloppnåelse og risikotiltak

Uavhengig av hvilket rammeverk som benyttes vil forskjellige selskap ha ulik vektlegging av betydningen av rapportering og analyse. Skal organisering og gjennomføring av helhetlig risikostyring gi selskapet gode beslutningsgrunnlag, både operasjonelt og strategisk er det viktig at det legges tilstrekkelig vekt på å analysere og evaluere output fra rapportene. Vår undersøkelse (figur 3) viser at litt over 40 prosent av respondentene har gitt seg selv en skår på 5 (midt på treet) på spørsmålet om de har mest fokus på rapportering eller analyse/evaluere. Dette kan tolkes som at rapportering tar tiden/hovedfokus til risikostyringsfunksjonen og at det ikke anvendes mye tid på å se fremover og analysere konsekvenser for selskapenes måloppnåelse. Dette kan tyde på at risikostyringsfunksjonen fremdeles har et stykke igjen for å bli den gode sparringspartneren for toppledelsen, som vi mener den kan være.

Figur 3

Skala 1-10, der 1 er helt uenig og 10 er svært enig

Hensiktsmessig organisering

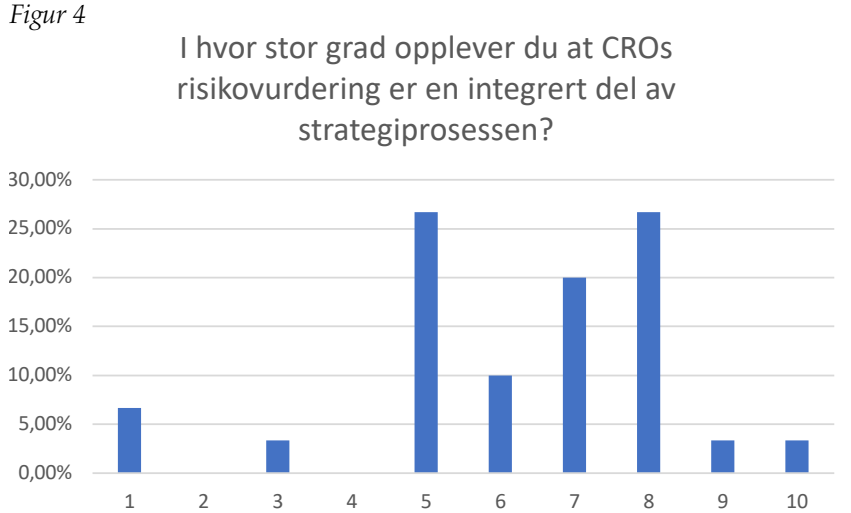
En ting er hvordan risikostyringsfunksjonen formelt er organisert, noe annet om den oppleves som hensiktsmessig av de som jobber med dette. Så hvordan opplever CRO og andre med CRO-lignende funksjon organiseringens hensiktsmessighet? Nærmere 75 prosent av respondentene har svart 7 eller høyere (ut av 10 som er best) på om de opplever at organiseringen er hensiktsmessig. I underkant av 35 prosent har svart 8 eller høyere. Det er verdt å merke seg at få respondenter ligger i nedre del, selv om dette klart indikerer at det er enkelte som er misfornøyd med dagens organisering av risikostyringen. Gjennomsnittet for alle respondentene er 5,6. Oppsummert tilsier dette at selskapene mener de relativt godt organisert i forhold til å løse sine oppgaver.

Leder for risikostyringsfunksjonen opplever å bli hørt og deltar aktivt i strategiprosessen i større grad enn hva organiseringen av prosessene skulle tilsi

Rammeverkene legger i stadig sterkere grad vekt på at helhetlig risikostyring bør være en integrert del av foretakets strategiprosesser og at dette vil styrke foretakets strategi og mulighet til å nå sine mål.

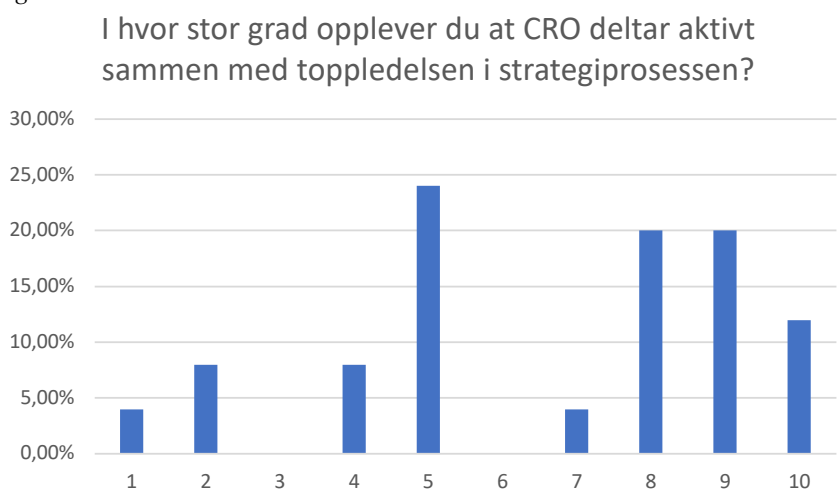
I gjennomsnitt ligger våre svar i figur 4 med feilmargin i et intervall mellom [5,0 – 6,9]. Dette tyder på at risikostyringsfunksjonen er relativt godt involvert i selskapenes strategiprosesser. Bare om lag 10 prosent av respondentene svarer at de i liten grad er en integrert del av strategiprosessen (3 eller mindre). 1 av 3 svarer at de i er involvert i stor grad (8 eller mer). Ser vi dette funnet i sammenheng med spørsmålet om hvor hensiktsmessig respondentene synes organiseringen av risikostyringen er, kan dette tolkes som om at deres opplevelse av hensiktsmessighet i organisering ikke nødvendigvis er et tegn på at de har tatt på seg rollen som strategisk rådgiver i strategiprosessene.

Figur 4



Skala 1-10, der 1 er helt integrert og 10 er svært integrert

Figur 5



Skala 1-10, der 1 er svært liten grad og 10 er svært stor grad

..Men brukes ikke som en aktiv rådgiver i strategiprosessene

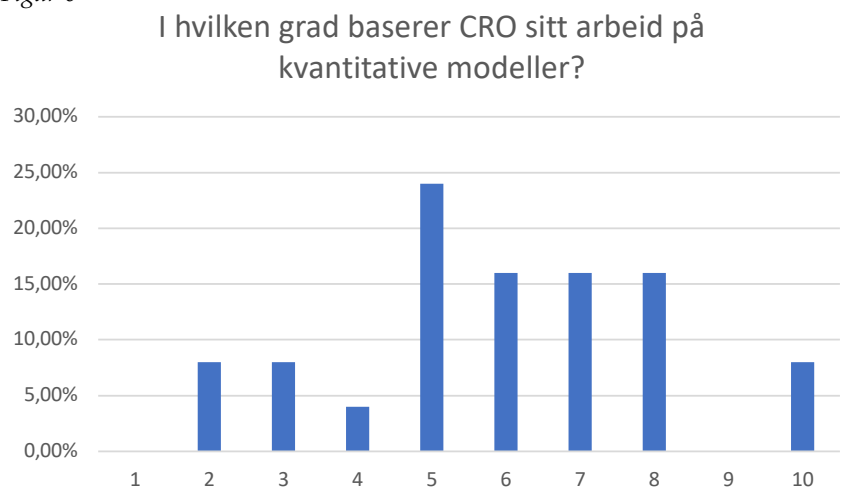
Når vi spør om de opplever at CRO deltar aktivt sammen med toppledelsen i strategiarbeidet ligger gjennomsnittet blant våre respondenter på 5,5 (se figur 5). Dette tyder på at CRO/leder for risikostyringsfunksjonen synes å bli hørt og deltar aktivt i strategiprosessen i større grad enn hva organiseringen av prosessene skulle tilsi. På den andre siden synes vi det er urovekkende at omlag 10 prosent av CRO'er i selskap notert på Oslo Børs ikke opplever å få delta aktivt.

> «Det er urovekkende at omlag 10 prosent av CRO'er i selskap notert på Oslo Børs ikke opplever å få delta aktivt i strategiprosessene.»

Banker og forsikringsselskap er underlagt kapitalkrav som følge av Basel II/Solvency II og har som følge av dette etablert kvantitative modeller for å beregne effekter for egen virksomhet.

Andre bransjer er ikke underlagt tilsvarende regulering og har dermed ikke samme insentiv for å kvantifisere arbeidet til risikostyringsfunksjonen. På denne bakgrunn ønsket vi å undersøke i hvor stor grad risikostyringsfunksjonen arbeider kvantitativt og/eller kvalitativt. I gjennomsnitt plasserer respondentene seg sånn midt på treet, 5,2 på en skala fra 1-10 (se figur 6). Vi konkluderer derfor med at selskapene på Oslo Børs baserer sitt arbeid på en miks av kvalitative og kvantitative modeller. Dette samsvarer godt med funn blant 15 finansinstitusjoner i Storbritannia (Mikes 2008).

Figur 6



Skala 1-10, der 1 er svært liten grad og 10 er svært stor grad

Anbefalinger for videre undersøkelser

For å fange opp utviklingstrekk og trender innenfor helhetlig risikostyring, hadde det vært interessant å kjøre en tilsvarende undersøkelse på nytt om 5 år og om 10 år.

Et annet interessant tema for videre forskning, er å undersøke om regulering av foretak og helhetlig risikostyring har effekt på foretakenes måloppnåelse og bunnlinje, samt på innovasjon og nyskapning. Den norske banksektoren er for eksempel sterkt regulert, men har likevel klart å lansere Vipps som har snudd opp ned på betalingsformidlingen i Norge, både sett fra et markeds- og forbrukerperspektiv. Å undersøke om man finner systematiske forskjeller mellom bransjer og størrelse på foretak, er derfor svært interessant.

Konklusjon

Risikostyringsfunksjonen basert på ERM er i vekst og utvikling. Våre funn indikerer at en egen leder for risikostyringsfunksjon er utbredt. Videre at de fleste CROer rapporterer administrativt til CEO, men har egen kanal til styret og de har godt stillingsvern. Vi finner også at det er mest fokus på rapportering og mindre på analyse av konsekvenser for selskapenes måloppnåelse og risikotiltak. Leder for risikostyringsfunksjonen opplever å bli hørt og deltar aktivt i strategiprosessen, men brukes ikke som aktiv rådgiver i strategiprosessene. CROene baserer sitt arbeid på en miks av kvalitative og kvantitative modeller.

Oppdatert veileder for risikostyringsfunksjonen

Veilederen for risikostyringsfunksjonen ble gitt ut i mars 2017. Målet var å lage en kortfattet og enkel veileder, som pekte på sentrale elementer og god praksis ved etablering av en risikostyringsfunksjon. Det har kommet mange gode tilbakemeldinger, og arbeidsutvalget har jevnlig tatt imot og vurdert innspill som er kommet siden den første versjonen.

For å sikre at veilederen holdes relevant, er det utarbeidet en oppdatert versjon som ble utgitt i oktober 2018. Oppdateringen endrer ikke vesentlig på innholdet, men det er gjort mindre endringer som blant annet tar hensyn til oppdateringer i COSO-rammeverket og ISO 31000. I tillegg er det gjort enkelte justeringer for å støtte sterkere opp om at veilederen skal være «allmenngyldig», og ikke bygge på bransjespesifikke regulatoriske krav eller utfordringer. Herunder skal den være like relevant for virksomhet som forvalter et offentlig samfunnsoppdrag, som for en rent finansielt motivert virksomhet.

Arbeidsutvalget setter pris på at det kommer innspill til veilederen, og vil løpende vurdere endringer til senere versjoner. Gjerne send email til risikostyring@iia.no.